МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДЕНО
Ученым советом МГТУ им. Г.И. Носова
Протокол № 4 от « 26 » февраля 2020 г

Ректор МГТУ им. Г.И. Носова,
председатель ученого совета
_____ М.В. Чукин

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Специальность
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Направленность (специализация) программы
Обеспечение информационной безопасности распределенных информационных систем

Магнитогорск, 2020

ОП-АИБ-20-1,2

7.1 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ			
ОК-1 способностью использовать основы философских знаний для формирования мировоззренческой позиции			
Знать	Основные философские категории и специфику их понимания в различных исторических типах философии и авторских подходах. Основные направления философии и различия философских школ в контексте истории. Основные направления и проблематику современной философии.	***Перечень теоретических вопросов к экзамену:*** 1. Философские концепции человека. Особенности взаимодействия человека с миром. Мировоззрение. 2. Разумность человека. Космоцентризм античной философии. 3. Религиозное мировоззрение. Особенности средневековой философии. Конечность существования человека и проблема бессмертия души. 4. Материализм и идеализм в философии как способы объяснения мира. Механистическая картина мира. 5. Возникновение диалектической проблемы развития из метафизического понимания мира. Основные законы диалектики. 6. Проблема пространства и времени в философии. Отличие от научного подхода. Специфика философии Нового времени. 7. Человек как производящее существо. Марксизм и материалистическое понимание истории. 8. Свобода как альтернатива природной детерминации. Иррациональная философия как способ объяснения мира. 9. Экзистенциализм как направление современной философии. Проблема экзистенции и бытия человека. 10. Проблема бытия в философии. 11. Проблема субстанции в философии. Философские картины материального единства мира. 12. Познание как путь движения к истине и основа ориентации в мире. Проблема истины. 13. Природа сознания. Идеальное как форма информационного отражения. 14. Проблема биосоциальной природы человека. Проблема социального в философии. Общество. 15. Экологические риски глобализированного мира. Социальные риски коммуникационного общества. 16. Философская концепция культуры. Культура и цивилизация.	Б1.Б.03 Философия
Уметь	Раскрывать смысл выдвигаемых идей,	**Примерные практические задания для экзамена:**	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	корректно выражать и аргументировано обосновывать положения предметной области знания. Представлять рассматриваемые философские проблемы в развитии. Сравнивать различные философские концепции по конкретной проблеме. Уметь отметить практическую ценность определенных философских положений и выявить основания на которых строится философская концепция или система;	Прочитайте и прокомментируйте высказывания, аргументируйте свой ответ. 1. «Из ничего ничто не может возникнуть, ни одна вещь не может превратиться в ничто» (Демокрит). Сталкивается ли современный человек с проблемой бытия? Обладает ли виртуальность бытием? 2. Абсолютное большинство историков считает, что присоединение Новгорода к Московской Руси являлось прогрессивным явлением: создавалось централизованное русское государство, и все славянские земли надо было объединить. С этим можно согласиться. Но ведь одновременно с тем была похоронена республиканская модель правления – важнейшее демократическое достижение в русских княжествах и землях. Как соотносится общее и уникальное в жизни современного человека? 3. «Чтобы не говорили пессимисты, земля все же совершенно прекрасна, а под луною и просто неповторима» (М.Булгаков). Разум – это величайшее благо или величайшее проклятие человека? 4. «Всякий трудящийся находится в состоянии войны с массой и неблагожелателен к ней в силу личного интереса. Врач желает своим согражданам добрых лихорадок, а поверенный добрых тяжб в каждой семье. Архитектору нужен добрый пожар, который превратил бы в пепел добрую часть города, а стекольщик желает доброго града, который разбил бы все стекла. Портной, сапожник желают публике только материй непрочной окраски и обуви из плохой кожи с тем, чтобы их изнашивали втрое больше, ради блага торговли» (Ш.Фурье) О какой общественно-экономической формации идет речь? Изменились ли намерения современного человека? Чем вызваны эти намерения – «дурной» природой человека или объективными законами истории? 5. «Хромой спутник может обогнать скакуна на лошади, если знает куда идти» (Ф.Бэкон) Что это означает? Какие проблемы в жизни современного человека возникают при определении такого пути? 6. «Если бы материя нее была бы вечной, давно бы весь существующий мир совершенно в ничто превратился (сгорают дрова)» (Лукреций Кар). Свободен ли современный человек от	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		субстанции? Может ли незнание о ее существовании служить аргументом ее ненужности? 7. «Иногда лучший способ погубить человека – это предоставить ему самому выбрать судьбу» (М. Булгаков). В чем сложность свободы для современного человека? 8. «Знание есть только путь к силе» (Т.Гоббс). В чем сила философского знания?	
Владеть	Навыками работы с философскими источниками и критической литературой. Приемами поиска, систематизации и свободного изложения философского материала и методами сравнения философских идей, концепций и эпох. Способами обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации. Владеть навыками выражения и обоснования собственной позиции относительно современных социогуманитарных проблем и конкретных философских позиций	***Примерный перечень тем письменных индивидуальных заданий (эссе):*** 1. Отношение к бытию современного человека. 2. Роль эпистемологии в жизни современного человека. 3. Вопросы этики в деятельности современного человека. 4. Роль философии в современном обществе 5. Софистика в современном мире. 6. Идеализм Платона в современном мировоззрении. 7. Телеология Аристотеля в современной теории развития. 8. Принципы стоицизма в жизни современного человека. 9. Принципы эпикуреизма в жизни современного человека. 10. Принципы скептицизма в жизни современного человека. 11. Вера и разум в мировоззрении современного человека. 12. Принцип «бритвы Оккама» в современной философии и науке. 13. Гедонизм как основа современного мировоззрения. 14. Конфуцианство и индивидуализм. 15. Философия буддизма и общество потребления. 16. Рационализм и здравый смысл в поведении современного человека. 17. Идеи прагматизма и утилитаризма в современном обществе. 18. Влияние русской философии на развитие	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		российского менталитета. 19. Влияние идей экзистенциализма на развитие современного человека. 20. Рациональная и иррациональная составляющие поведения современного че-ловека. 21. Интуиция и здравый смысл в условиях постмодерна. 22. Свобода и ответственность личности. 23. Проблема человека в современном обществе. 24. Проблема определения смысла жизни. 25. Смысл существования человека. 26. Этические проблемы развития науки и техники. 27. Проблема самоактуализации человека в обществе потребления. 28. Социальные проблемы развития науки и техники. 29. Проблема развития и использования технологий. 30. Социальное и биологическое время жизни человека. 31. Концепция успеха в современном обществе. 32. Культура и цивилизация. 33. Доверие и сотрудничество в современном обществе. 34. Мифологичность мировоззрения современного человека. 35. Роль порядка и хаоса в жизни современного человека. 36. Онтология современного человека. 37. Эпистемология современного человека. 38. Этика современного человека. 39. Аксиология современного общества. 40. Проблема феномена инновации.	
Знать	-культурологические концепции и теории, формирующие представление о различных мировоззренческих позициях их авторов; -сущность понятия культурная картина мира, отражающего особенности мировоззрения личности; -причины формирования различных мировоззренческих позиций, основанных на философских знаниях представителей различных	**Перечень теоретических вопросов к зачету:** 1. Структура и состав культурологического знания. 2. Структура современной культурологии: теория культуры, история культуры, философия культуры, социология культуры. 3. Культурантропология. 4. Теоретическая и прикладная культурология. 5. Методы культурологического исследования. 6. Понятие культуры и её функции. 7. Культурогенез.	Б1.Б.06Культурология и межкультурное взаимодействие

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	культурных систем	8. Культура, природа и цивилизация. 9. Культура как мир смыслов и знаков. Язык и коды культуры. 10. Формы культуры: мифология, религия, искусство, наука. 11. Культурная картина мира. 12. Морфология культуры: материальная и духовная культуры. 13. Субкультура и контркультура. 14. Массовая и элитарная культура. 15. Функции, ценности и нормы культуры. 16. Типология культуры: дихотомия «Восток – Запад». 17. Общественно-историческая школа (Н.Я. Данилевский, О. Шпенглер, А. Тойнби и др.). 18. Натуралистическая школа (Ф. Ницше, З. Фрейд, К.Г. Юнг, Б.К. Малиновский и др.). 19. Социологическая школа (Т. Элиот, П. Сорокин, А. Вебер, Т. Парсонс и др.). 20. Структурно-символическая школа (Ф. Соссюр, Э. Кассирер, К. Леви-Стросс и др.). 21. Антропологическая школа (Э. Тэйлор, А. Ланг, Дж. Фрейзер, А.Н. Веселовский и др.). 22. Концепция «игровых культур» (Й. Хейзинга, Х. Ортега-и-Гассет, Е. Финки др.). 23. Межкультурные коммуникации. 24. Культура, личность и общество: аккультурация и ассимиляция. 25. Социальные институты культуры. 26. Инкультурация и социализация. 27. Модели культурной универсализации. 28. Место и роль России в диалоге культур и мировой культуре. 29. Национальное своеобразие русской культуры: мессианское сознание. 30. Становление и развитие культуры на Руси в IX – XVIII веках: из культурной изоляции к интеграции с европейской культурой. 31. Роль личности в русской культуре XIX века.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		32. Диалог культур в русском искусстве «Серебряного века». 33. Культурная модернизация. 34. Глобальные проблемы современности. 35. Культура в современном мире. **Тест:** 1.Что характерно во взглядах на культуру в античности **а)космоцентризм** б)теоцентризм в)антропоцентризм 2. Что характерно во взглядах на культуру в средневековье а)космоцентризм **б)теоцентризм** в)антропоцентризм 3. Что характерно во взглядах на культуру в Новое время а)космоцентризм б)теоцентризм **в)антропоцентризм** 4. Согласно О. Шпенглеру, цикл каждой культуры укладывается в один и тот же временной интервал. Он включает в себя четыре периода, назовете их **а) зарождение; расцвет; старение; смерть** б)смерть, зарождение, расцвет, старение в)младенчество, отрочество, юность, смерть 5. Кто из философов выдвинул идею о моральном превосходстве «естественного человека», не испорченного культурой и цивилизацией, а также лозунг о «возврате в природу» а)Гегель б)Сократ **в)Руссо** 6. Кто из ученых смотрит на жизнь человека через призму двух основных, по его мнению, инстинктов - сексуального (инстинкт Эроса, или продолжения жизни) и разрушительного (инстинкт Танатоса, или смерти)? а)Юнг **б)Фрейд** в)Ницше	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		7. Как называется сочинение немецкого философа и историка О. Шпенглера, в котором он излагает свои взгляды на культуру? а) «Феномен человека» б) «Идеи к философии истории человечества» **в) «Закат Европы»** 8. Философ, создавший концепцию «Осевого времени»: **а) В. К. Ясперс** б) В.Ф. Гегель в) Ф.В. Ницше 9. Основоположник учения о культурных архетипах как коллективном бессознательном а) Сократ б) З. Фрейд **в) К. Юнг** 10. Представители одного из направлений русской общественной мысли, выступавшие за принципиально отличный от западного путь развития России на основе самобытности а) Гуманисты б) Декабристы **в) Славянофилы** 11. Назовите самых первых древнегреческих мыслителей, давших начало древнегреческой философии **а) Демокрит, Сократ** б) Фалес, Солон в) Гераклит, Пифагор	
Уметь	-выстраивать собственную мировоззренческую позицию на основе имеющихся культурно-философских знаний; -обосновывать собственную мировоззренческую позицию; -формировать новые взгляды и представления, основанные на существующих мировоззренческих позициях представителей различных культурных систем	**Практические задания**: Установите, кому из теоретиков культуры принадлежат данные высказывания. 1. Человек создан, чтобы усвоить дух гуманности и религии. Мне хотелось бы вместить в одно слово – «человечность» – все сказанное о благородном складе человеческого существа, ведь, чтобы говорить о своем предназначении нет слова более благородного, чем «человек», в коем запечатлен образ Творца.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Великий закон справедливости стал путеводною нитью для человека: и как не хотите того, чтобы сделали вам люди, так не делайте того и им; и как хотите, чтобы с вами поступали люди, так и вы поступайте с ними. Закон справедливости и правды превращает людей в верных помощников и братьев друг другу, а когда он утвердится совершенно, то и врагов обратит в друзей. Религия – вот высшая гуманность человека. Это упражнение сердца, поклонение Богу, подражание самому высшему и прекрасному, запечатление его в образе человеческом, а вместе с тем наидеятельнейшая доброта и человеколюбие. 2. Совокупность производственных отношений составляет экономическую структуру общества, реальный базис, на котором возвышается юридическая и экономическая надстройка и которому соответствуют определенные формы общественного сознания. Способ производства материальной жизни обусловливает социальный, политический и духовный процессы жизни вообще. 3. Ход развития культурно-исторических типов всего ближе уподобляется тем многолетним одноплодным растениям, у которых период роста бывает неопределенно продолжителен, но период цветения и плодоношения – относительно короток и истощает раз и навсегда их жизненную силу. 4. Культура как совокупность выражения души в жертвах и трудах, как тело ее, смертное, преходящее; культура как историческое зрелище, как образ в общей картине мировой истории; культура как совокупность великих символов жизни, чувствования и понимания: таков язык, которым только и может поведать душа, как она страждет. 5. Общие разряды культурной деятельности таковы: 1) деятельность религиозная, объемлющая собою отношения человека к Богу; 2) деятельность культурная, в тесном значении этого слова, объемлющая отношения человека к внешнему миру, во-первых, теоретическое – научное, во-вторых, эстетическое – художественное; 3) деятельность политическая, объемлющая	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		отношения людей между собою; 4) деятельность общественно-экономическая, объемлющая отношения людей применительно к условиям пользования предметами внешнего мира, добывания и обработки их. 6. Рассмотрим истоки двадцати одной цивилизации, обращая внимание на вызовы, которые делала среда, и на ответы на них. Не будем постулировать никакого единства и не будем пытаться обнаружить какой бы то ни было всеобщий закон, наша задача – исследовать феномены Вызова и Ответа применительно к частным случаям. 7. Мы достаточно определенно установили истину, согласно которой благоприятные условия враждебны цивилизации, и показали, что чем благоприятнее окружение, тем слабее стимул для зарождения цивилизации. Допустимо, что стимул, побуждающий к строительству цивилизации, возрастает по мере того, как условия проживания становятся все более трудными. Для удобства разделим интересующие нас исторические примеры на две группы. К первой группе отнесем те случаи, когда цивилизация зарождалась под воздействием природной среды, ко второй – те цивилизации, где бóльшее влияние оказывало человеческое окружение. **Ключ к заданию** И.-Г. Гердер (1744-1803) – немецкий философ эпохи Просвещения, интересовался вопросами философии истории и эстетики. Состоял пастором в Риге и Веймаре. Был другом Гете и одним из теоретиков художественного движения «Буря и натиск», ратовал за национальную самобытность искусства. Автор сочинения «Идеи к философии истории человечества», в котором история трактуется как осуществление идеалов гуманности. Ж.-А.-Н. (де) Кондорсе (1743-1794) – французский философ эпохи Просвещения, математик, социолог, политический деятель. Сотрудничал в «Энциклопедии» Д. Дидро и Д’Аламбера. В годы Великой французской революции был избран в Законодательное собрание, затем стал членом Конвента. Как философ Кондорсе	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		является создателем концепции исторического прогресса, в основе которого, по его мнению, лежат достижения человеческого разума в области науки, техники и социальной жизни. Свои идеи Кондорсе изложил в работе «Эскиз исторической картины прогресса человеческого разума» (1794). К. Маркс (1818-1883) и Ф. Энгельс (1820-1895) – немецкие мыслители и общественные деятели. Организаторы и идейные вдохновители первого «Союза коммунистов», авторы «Манифеста Коммунистической партии». Общественно-политическая деятельность К. Маркса и Ф. Энгельса в своей основе имела социально-экономическую доктрину, наиболее полно изложенную ими в «Капитале» (1867-1894). Теоретики марксизма разработали принципы материалистического понимания истории: по их мнению, побудительные мотивы исторического развития определяются материальными условиями общественного производства. Производственные отношения представляют собой тот «базис», по отношению к которому все прочие аспекты культуры выступают в качестве идеологизированной «надстройки». Соответственно, исторический процесс рассматривается как закономерная смена общественно-исторических формаций, в результате которой должен утвердиться коммунизм. Н.Я. Данилевский (1822-1885) – российский публицист и социолог, разделял взгляды славянофилов. В сочинении «Россия и Европа» (1869) выдвинул идею обособленных «культурно-исторических типов» (локальных цивилизаций), каждый из которых должен, подобно живому организму, пройти через периоды становления, расцвета и угасания. Своеобразие культурно-исторических типов Данилевский видел в характерном для каждого из них сочетании доминирующих видов деятельности. Особые надежды возлагал на «славянский» культурно-исторический тип, поскольку считал его «четырехосновным». О. Шпенглер (1880-1936) – немецкий математик, историк и философ. Развил учение о культуре как множестве замкнутых	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		«организмов», проходящих определенный жизненный цикл и выражающих «душу» разных народов. Ключ к пониманию своеобразия культуры – «первосимвол», хранящийся в ее «душе» и воплощаемый во всех значимых культурных формах. Когда творческий потенциал культуры иссякает, она в преддверии своей гибели перерождается в «цивилизацию», в которой господствует голый техницизм, лишенный духовного содержания. Главное произведение О. Шпенглера – «Закат Европы» (1918-1922). А.Дж. Тойнби (1889-1975) – английский историк и социолог, дипломат и общественный деятель. В культурологическом исследовании «Постижение истории» (1934-1961) обобщил факты из прошлого более чем двадцати разнообразных культур и выдвинул теорию круговорота сменяющих друг друга локальных цивилизаций, каждая из которых проходит аналогичные стадии роста, развития, надлома и разложения. Развитию цивилизаций, по мнению Тойнби, способствуют неблагоприятные обстоятельства, природные или исторические. Именно они становятся стимулом для активизации потенциала «творческой элиты», которая затем увлекает за собой «инертное большинство» – так в ответ на внешний вызов рождается новый тип культуры.	
Владеть	- методом критического анализа в области основ философских знаний с целью формирования собственной мировоззренческой позиции; - приемами убеждения в верности собственной мировоззренческой позиции; - навыком отбора значимых философских знаний для формирования мировоззренческой позиции	**Блок творческих заданий для выявления уровня креативного показателя личности:** 1. С. Л. Франк в известной работе «Смысл жизни» пишет, что этот «проклятый вопрос» «о смысле жизни» волнует и мучает в глубине души каждого человека. Человек может на время, даже на очень долгое время, совсем забыть о нем, погрузиться с головой в будничные интересы сегодняшнего дня, в материальные заботы о сохранении жизни, о богатстве, довольстве и земных успехах…. но жизнь уже так устроена, что совсем и навсегда отмахнуться от него не может и самый тупой, заплывший жиром или духовно спящий человек … Этот вопрос - не теоретический, не предмет праздной умственной игры; этот вопрос есть вопрос о смысле самой жизни, он даже страшен – и, собственно, говоря еще гораздо более страшнее, чем при тяжкой нужде вопрос о куске хлеба для	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		утоления голода…». • Что же такое «смысл жизни»? Какие мнения есть по этому вопросу среди философов, теологов, ученых? • Зачем человеку нужно прояснить его для себя? Почему С. Л. Франк называет его практическим вопросом, вопросом всей жизни? • В чем Вы видите смысл своей жизни. Ответ аргументируйте. 2. Высшей подлинной сущностью человека является свобода. Человек всегда стремится к свободе. «Без свободы нет человека», - говорил, Ф.М. Достоевский. В то же время он отмечал, что свобода может привести к эгоизму, неблаговидности и даже безобразию. Тогда она превращается в несвободу. Современный немецкий философ, социолог и психолог Э. Фромм («Бегство от свободы») пишет, что процесс развития человеческой свободы носит диалектический характер. С одной стороны, это «процесс развития человека, овладения природой, возрастания роли разума, укрепления человеческой солидарности. Но, с другой, это – усиление индивидуализации, которая означает усиление изоляции, неуверенности… Вместе с этим растет и чувство бессилия, ничтожности отдельного человека». «Люди утрачивают первичные связи, давшие им осуществление уверенности. Такой разрыв превращает свободу в невыносимое бремя: она становится источником сомнений, влечет за собой жизнь, лишенную цели и смысла. И тогда возникает сильная тенденция избавиться от такой свободы, уйти в подчинение или найти иной способ связаться с людьми и миром, чтобы спастись от неуверенности даже ценой свободы». Что такое свобода человека? Какие есть точки зрения по этому вопросу? •	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Когда и при каких условиях она превращается в свою противоположность. Подтвердите примерами. • Что необходимо, чтобы осуществить подлинную свободу, избежать ее превращения в несвободу или «бегство от свободы 3. «Ценности упорядочивают действительность, вносят в ее осмысление оценочные моменты, отражают иные по сравнению с наукой аспекты окружающей действительности… Ценности придают смысл человеческой жизни». (П. С. Гуревич). • Что такое ценность? Какие бывают ценности? • Как соотносятся «ценность» и «оценка», «ценность» и «истина», «ценность» и «норма»? • Что такое «святыня»? • Назовите святыни человека. Какую роль они играют в его жизни?	
ОК-2	**способностью использовать основы экономических знаний в различных сферах деятельности**		
Знать	– основные термины, определения, экономические законы и взаимозависимости на уровне экономики в целом и на уровне отдельного предприятия; – методы исследования экономических отношений на уровне экономики в целом и на уровне отдельного предприятия; – методики расчета важнейших экономических показателей и коэффициентов на уровне экономики в целом и на уровне отдельного предприятия; – теоретические принципы выработки экономической политики на уровне государства и на уровне отдельного предприятия.	**Перечень теоретических вопросов к зачету:** 1. Определение экономики, основные понятия и определения. 2. Факторы производства. 3. Структура экономики. 4. Границы производственных возможностей общества. 5. Спрос и предложение. Равновесная цена. Государственное вмешательство в рыночное ценообразование и его формы. 6. Эластичность спроса и предложения. 7. Основы потребительского поведения. 8. Основы теории производства. Производственная функция. 9. Издержки производства: понятие, виды. Выручка. Прибыль. Рентабельность. 10. Определение цены и объема производства.	Б1.Б.04Экономика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		11. Рынок ресурсов: особенности их экономического анализа. 12. Особенности рынка совершенной конкуренции. 13. Три типа рынков несовершенной конкуренции. Антимонопольное регулирование. 14. Система национальных счетов (СНС) как способ единообразного о писания различных сторон макроэкономики. 15. Основные макроэкономические показатели. 16. Совокупный спрос, совокупное предложение. 17. Модели макроэкономического равновесия. 18. Циклическое развитие экономики. 19. Инфляция: сущность, оценка, причины возникновения, формы, социально-экономические последствия. Антиинфляционное регулирование. 20. Безработица: сущность, формы, оценка. 21. Финансовая система и финансовая политика государства. Налоги: сущность, функции. 22. Кредитно-денежная система государства. Теоретические основы кредитно-денежной политики. 23. Предприятие в рыночной среде. Классификация предприятий. Формы объединения предприятий. 24. Основные средства предприятия. Состав и виды основных средств. Оценка и учет основных средств. 25. Износ и амортизация основных средств. Нормы амортизации. Способы начисления амортизации. 26. Показатели эффективности использования основных средств предприятия и пути их повышения. 27. Оборотные средства. Состав и структура оборотных средств предприятия. 28. Показатели эффективности использования оборотных средств и пути ускорения их оборачиваемости. 29. Трудовые ресурсы предприятия: количественная и качественная характеристика. 30. Фонды рабочего времени. Показатели их использования	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		31. Показатели эффективности использования трудовых ресурсов. Производительность труда. 32. Оплата труда на предприятии: сущность, функции. Системы сдельной и повременной оплаты труда. 33. Расходы и затраты предприятия. Экономические элементы затрат и калькуляционные статьи. 34. Расходы и затраты предприятия. Постоянные и переменные, прямые и косвенные, основные и накладные затраты. 35. Себестоимость продукции предприятия и структура затрат. Калькулирование себестоимости продукции предприятия. 36. Цены и ценообразование на предприятии. Состав и структура цены. 37. Прибыль как основной показатель деятельности предприятия. Виды прибыли и методы ее расчета. 38. Рентабельность продукции и общая рентабельность предприятия: показатели и пути их повышения. 39. Точка безубыточности и запас финансовой прочности. 40. Основные экономические школы **Задания в тестовой форме «выбор одного ответа из предложенных».** Задание 1 (укажите один вариант ответа). Невозможность удовлетворения потребностей всех членов общества одновременно и в полном объеме определяется в экономической теории как … Варианты ответов: 1) ограниченность ресурсов 2) чрезмерность потребностей 3) доминирование псевдопотребностей 4) отсутствие природных ресурсов Задание 2 (укажите один вариант ответа). Исходной стадией процесса общественного воспроизводства является … Варианты ответов: 1) производство	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		2) распределение 3) обмен 4) потребление Задание 3 (укажите один вариант ответа). Взаимосвязь экономических интересов продавцов и покупателей обеспечивается выполнением рынком _____ функции. Варианты ответов: 1) посреднической 2) стимулирующей 3) ценообразующей 4) информационной Задание 4 (укажите один вариант ответа). Рыночные барьеры на рынке совершенной конкуренции … Варианты ответов: 1) отсутствуют 2) низкие 3) высокие 4) непреодолимые Задание 5 (укажите один вариант ответа). К физическому капиталу относятся … Варианты ответов: 1) здания, сооружения, машины и оборудование 2) денежные средства, акции, облигации 3) предметы труда, которые ранее не подвергались обработке 4) нематериальные активы (торговые марки, патенты и др.) Задание 6 (укажите один вариант ответа). Суммарная стоимость всех рыночных и нерыночных продуктов и услуг, произведенных в стране в отчетном периоде, в системе национальных счетов получила название … Варианты ответов: 1) валового выпуска 2) валового внутреннего продукта 3) чистого внутреннего продукта 4) валовой добавленной стоимости Задание 7 (укажите один вариант ответа). Инвестиции, осуществляемые с целью восстановления изношенного капитала, называют …	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Варианты ответов: 1) инвестициями в модернизацию (реновацию) 2) портфельными инвестициями 3) индуцированными инвестициями 4) инвестициями в жилищное строительство Задание 8 (укажите один вариант ответа). Инфляция приведет к … Варианты ответов: 1) росту цен 2) увеличению реальных доходов кредиторов 3) увеличению денежных сбережений населения в банках 4) росту реальных доходов населения Задание 9 (укажите один вариант ответа). К безработным **не относят** … Варианты ответов: 1) недееспособных граждан старше 16 лет 2) дееспособных граждан старше 16 лет 3) не имеющих работы 4) ищущих работу Задание 10 (укажите один вариант ответа). Бюджет государства представляет собой … Варианты ответов: 1) финансовый план, в котором представлены доходы и расходы государства 2) организацию бюджетных отношений на различных уровнях государственного устройства 3) совокупность экономических отношений по образованию и распределению денежных фондов государства 4) государственное имущество, принадлежащее государству на праве собственности, не закрепленное за государственными предприятиями и учреждениями Задание 11 (укажите один вариант ответа). Фактором спроса на деньги является … Варианты ответов: 1) скорость обращения денег в экономике 2) состояние баланса центрального банка страны 3) поступление налогов и сборов	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4) экспортно-импортное сальдо торгового баланса страны Задание 12 (укажите один вариант ответа). Для прогнозирования динамики изменения денежной массы вследствие изменения нормы резервирования, устанавливаемой для коммерческих банков центральными банками, требуется расчет такого показателя, как мультипликатор … Варианты ответов: 1) денежный 2) инвестиционный 3) совокупных расходов 4) «цена/выручка»	
Уметь	– ориентироваться в типовых экономических ситуациях, основных вопросах экономической политики; – использовать элементы экономического анализа в своей профессиональной деятельности; – рационально организовать свое экономическое поведение в качестве агента рыночных отношений, – анализировать и объективно оценивать процессы и явления, осуществляющиеся в рамках национальной экономики в целом и отдельного предприятия в частности. – ориентироваться в учебной, справочной и научной литературе.	**Практические задания** 1. Марья Ивановна – домработница. Она тратит по 15 мин. на стирку рубашки и по 45 мин. – на мытье окна. Нарисуйте линию производственных возможностей Марьи Ивановны в рамках 9-ти часового рабочего дня. Как изменится график, если в результате совершенствования технологии на мытье окна Марья Ивановна станет тратить 20 мин.? 2. В экономике производится 200 тыс. т молока и 300 тыс. т пшеницы. Альтернативные издержки производства молока = 5. Найти максимально возможный выпуск пшеницы после увеличения выпуска молока на 10%. 3. Функция спроса на благо Qd = 15 – P, функция предложения Qs = –9 + 3P. Определите равновесие на рынке данного блага. Что произойдет с равновесием, если объем спроса уменьшится на 1 единицу при любом уровне цен? 4. Зависимость спроса и предложения выражена формулами Qd = 94 – 7P, Qs = 15P – 38. Найти равновесную цену и равновесный объём продаж. Чему равен дефицит или избыток товара при цене 4 рубля за единицу товара? 5. В результате роста цены с 4 до 7 долл., объем спроса на товар X упал с 1000 до 800 штук. Определите коэффициент эластичности спроса по цене. 6. Цена на товар А выросла со 100 до 200 ден. ед. Спрос на этот товар упал с 3000 до 1000 штук. Спрос на товар В вырос с 500 до 1000. Определите коэффициенты эластичности товара А и В. О	

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>каких коэффициентах идет речь?
7. Коэффициент перекрестной эластичности Ex/y = (–2). Цена товара Y равна 100 у. е. Определите спрос на товар X, если цена товара Y увеличится на 10 %, а первоначальный спрос на товар X равен 80 т.
8. Владелец небольшого магазина ежегодно платит 3 тыс. у. е. аренды, 20 тыс. у. е. заработной платы, 100 тыс. у. е. за сырье, 10 тыс. у. е. за электроэнергию. Стоимость установленного оборудования составляет 200 тыс. у. е., срок его службы 10 лет. Если бы эти средства он положил в банк, то ежегодно получал бы 16 тыс. у. е. дохода. Определите бухгалтерские и экономические издержки.
9. Известно, что при L = 30 достигается максимум среднего продукта труда, и такое количество ресурса позволяет фирме произвести 120 единиц продукции. Каким будет предельный продукт труда, если занято 29 единиц труда?
10. Фирма платит 200 тыс. руб. в месяц за аренду оборудования и 100 тыс. руб. заработной платы. При этом она использует такое количество труда и капитала, что их предельные продукты соответственно равны 0,5 и 1. Использует ли фирма оптимальное сочетание факторов производства с точки зрения максимизации прибыли?
11. Фирма работает по технологии, характеризующейся производственной функцией . Во сколько раз увеличится выпуск продукции фирмой, если она в 4 раза увеличит использование обоих ресурсов?
12. Функция общих издержек фирмы имеет вид TC=30Q – Q2. Эта фирма реализует продукцию на рынке совершенной конкуренции по цене 90 руб. Подсчитайте, какую она получает прибыль?
13. Определите, какой объем лучше выпускать предприятию, продающему товар по цене, равной 15 у. е., и имеющему следующие затраты на производство и реализацию продукции (см. таблицу). Определите максимальную прибыль.
<table>
<tr><td>Q</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td></tr>
<tr><td>TC</td><td>50</td><td>65</td><td>75</td><td>84</td><td>92</td><td>102</td><td>114</td><td>129</td><td>148</td><td>172</td><td>202</td><td>252</td></tr>
</table>
</td><td></td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		14. Спрос на продукцию конкурентной отрасли $Q_d = 50 - P$, а предложение $Q_S = 2P - 1$. Если у одной фирмы отрасли восходящий участок кривой предельных издержек MC = 3Q + 5, то при каких цене и объеме производства фирма будет максимизировать прибыль? 15. Фирма по производству автомобилей приобрела прокат у сталелитейной фирмы на сумму 1500 тыс. долл., покрышки у шинного завода на сумму 600 тыс. долл., комплектующие у различных фирм на сумму 1200 тыс. долл., выплатила заработную плату своим рабочим в размере 1000 тыс. долл., потратила 300 тыс. долл., на замену изношенного оборудования и продала изготовленные 200 автомобилей нпо 30 тыс. долл. каждый, при этом прибыль фирмы составила 400 тыс. долл. Определить величину добавленной стоимости автомобильной фирмы. 16. Если в экономике страны располагаемый личный доход составляет 550 млрд. долл., чистые инвестиции – 70 млрд. долл., государственные закупки товаров и услуг – 93 млрд. долл., косвенные налоги – 22 млрд. долл., личные сбережения – 13 млрд. долл., амортизация – 48 млрд. долл., экспорт – 27 млрд. долл., импорт – 15 млрд. долл. Определить ВВП. 17. В результате роста совокупных расходов номинальный ВВП страны в 2009 г. стал равен 5250 млрд. долл., и темп изменения ВВП по сравнению с 2008 г. составил 5%. Известно, что в 2008 г. номинальный ВВП был равен 4600 млрд. долл., а дефлятор ВВП – 1,15. Определите фазу цикла и темп инфляции 2009 г. 18. Потенциальный ВВП составляет 500 млрд. долл., фактический ВВП – 455 млрд. долл., а фактический уровень безработицы – 10%. Когда фактический ВВП сократился на 20%, уровень безработицы вырос на 9,1%. Определите величину коэффициента Оукена и естественный уровень безработицы. 19. Функция сбережений имеет вид S = -50 + 0.1Y, автономные инвестиции I = 25. Каким будет равновесный уровень национального производства и дохода Y? а) На основе этой функции составьте функцию потребления. б) Поясните	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		взаимосвязь двух методов определения равновесия логически, аналитически и графически 20. Объем производства в цехе в прошлом месяце составил 6500 т. Вся произведенная продукция была продана в том же месяце. Цех выпускает только один вид продукции. Цена единицы выпускаемой цехом продукции составляет 14 000 руб. Среднесписочная численность работников цеха за прошлый месяц составила 524 человека. Определите производительность труда в денежном и натуральном выражении. 21. Среднегодовая стоимость основных производственных фондов составила 1200 тыс. руб. в том числе здания и сооружения 337 тыс. руб., оборудование и машины 743 тыс. руб., прочие фонды 120 тыс. руб. Норма амортизации соответственно определены в 2,5%, 8% и 5%. Рассчитать структуру основных производственных фондов и годовые амортизационные отчисления. По зданиям и прочим фондом амортизация начислялась линейным методом, а по оборудованию и машинам методом уменьшаемого остатка (коэффициент ускорения взять равным 2). 22. Скорость оборота оборотных средств составляет 6 оборотов за год, объем реализованной продукции предприятия за год составил 854 тыс. руб. Определить сумму денежных средств, находящихся в обороте фирмы. 23. В результате реконструкции на предприятии увеличится объем производства на 20% и составит 25600 ед. Рассчитать, как изменится себестоимость единицы продукции, если до реконструкции она составляла 1050 руб., условно-постоянные расходы в себестоимости составляют 60%. 24. Рассчитать чистую прибыль организации, если цена реализации единицы продукции – 267 руб., в т.ч. НДС, общая сумма затрат за месяц – 15000 руб. Объем производства – 100 единиц продукции. 25. Выручка от реализации продукции составила 219 млн. руб. Полная себестоимость – 168 млн. руб. Определите рентабельность реализованной продукции	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Задания как закрытой, так и открытой тестовой формы. Задание 1 (укажите один вариант ответа). Предоставляя обществу знания о социально-экономическом поведении людей и их групп, экономика выполняет _____ функцию. Варианты ответов: 1) теоретическую 2) практическую 3) методологическую 4) идеологическую Задание 2 (укажите один вариант ответа). На ранних этапах экономического развития общества, когда человек полностью зависит от окружающей среды, имел место _____ технологический способ производства. Варианты ответов: 1) присваивающий 2) простой 3) производящий 4) постоянный Задание 3 (укажите один вариант ответа). Больше всего условиям совершенной конкуренции соответствует рынок … Варианты ответов: 1) пшеницы 2) стали 3) услуг парикмахерских 4) автомобилей Задание 4 (выберите не менее двух вариантов). Особенностями рынка с монополистической конкуренцией являются … Варианты ответов: 1) наличие множества продавцов и покупателей 2) влияние на уровень цен в довольно узких рамках 3) отсутствие товаров-заменителей 4) несовершенная информированность продавцов и покупателей об условиях рынка	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Задание 5 (выберите не менее двух вариантов). На графике показана модель «AD–AS» (совокупный спрос – совокупное предложение). Если кривая совокупного спроса пересекает кривую совокупного предложения на горизонтальном участке, то увеличение совокупного спроса … Варианты ответов: 1) увеличит реальный объем производства 2) не изменит уровня цен 3) не изменит реального объема производства 4) повысит цены Задание 6 (выберите не менее двух вариантов). Инвестиции в запасы … Варианты ответов: 1) осуществляются с целью сглаживания колебаний объемов производства при неизменном объеме продаж 2) осуществляются в связи с технологическими особенностями производства 3) связаны с расходами домашних хозяйств на приобретение домов, квартир 4) связаны с расширением применяемого основного капитала	
Владеть	– методами и приемами анализа экономических явлений и процессов на уровне экономики в целом и на уровне отдельного предприятия; – практическими навыками использования экономических знаний на других дисциплинах, на занятиях в аудитории и на практике; – на основании теоретических знаний принимать решения на уровне экономики в целом и на уровне отдельного предприятия; – самостоятельно приобретать, усваивать и применять экономические знания, наблюдать, анализировать и объяснять экономические явления, события, ситуации.	**Кейс-задания, состоящие из описания ситуации и вопросов к ней.** **Кейс 1** В государстве Ардения уровень инфляции за последние три года составил соответственно: 100 %, 130 % и по итогам текущего года – 150 %. Реальный уровень объема производства за рассматриваемый период снизился в пять раз и стабилизировался в этой точке. Величина государственного долга на начало последнего в рассматриваемом периоде года равна 200 аграм, номинальная ставка процента по которому равна 35 %. Состояние бюджета характеризуется также тем, что номинальные государственные расходы без платежей по обслуживанию долга выросли на 100% и по итогам последнего года составили 50 агров, номинальные налоговые поступления снизились и составили за последний год 80 агров. **Задание 1:**	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Номинальная величина сальдо государственного бюджета данной страны в текущем году равна _____ агров. **Задание 2:** Экономическая ситуация, сложившаяся в Ардении, называется … 1) стагфляцией 2) стагнацией 3) спадом 4) естественной инфляцией **Задание 3:** В измерении итогов экономической деятельности за тот или иной период времени существуют номинальные и реальные стоимостные величины. К последним относятся … Укажите один вариант ответа 1) уровень безработицы, темп инфляции, значение коэффициенты Оукена 2) общая величина доходов государственного бюджета, величина процентов, идущих на обслуживание внешнего долга, изменение заработной платы наемных работников без учета изменения уровня цен 3) доходы государственного бюджета от таможенных пошлин, уплачиваемые по внешнему долгу проценты, выплаты материнского капитала в будущем, на период трех лет 4) общие расходы государственного бюджета, поступления от уплаты косвенных налогов, изменение пенсий и социальных пособий относительно прошлых периодов с учетом индекса инфляции ***Кейс* 2** Спрос и предложение на сигареты описываются уравнениями: $P_d = 50 - Q_d$ и $P_s = 10 + Q_s$, где Pd – цена спроса, Ps – цена предложения, Qd – объем спроса, Qs – объем предложения. Государство, имея возможность регулирования рыночного ценообразования, решило использовать косвенный метод регулирования – ввести налог в размере 2 ден. единицы с каждой единицы проданного товара. ***Задание 1:***	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Подобное вмешательство государства в процесс рыночного ценообразования преследует цель … Укажите один вариант ответа 1) увеличения производства и потребления сигарет 2) снижения производства и потребления сигарет 3) поддержать потребителей сигарет 4) поддержать производителей сигарет ***Задание 2:*** Подобное вмешательство государства в рыночное ценообразование приведет к сдвигу кривой _____ и _____ равновесного объема продаж. Выберите не менее двух вариантов 1) сокращению 2) предложения вправо вниз 3) увеличению 4) предложения влево вверх **Задание 3:** В результате государственного вмешательства в процесс рыночного ценообразования путем введения налога бюджет будет пополнен на сумму ____ ден. единиц. **Кейс 3.** Известно, что в общественной жизни экономические отношения занимают особое место, формируя своим содержанием, в том числе, тип экономической системы. Экономика как хозяйственная деятельность общества имеет свои причины и особенности, являющиеся предметом изучения многих ученых на протяжении последних тысячелетий. Задание 1 (укажите один вариант ответа). Основной причиной возникновения и развития экономических отношений является _____ большей части благ, называемых экономическими. Варианты ответов: 1) редкость 2) неограниченность 3) исчерпаемость 4) материальная форма	

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>
Задание 2 (выберите не менее двух вариантов).
Примерами экономических благ, которые отличаются свойством редкости, могут служить …
Варианты ответов:
1) лесные ресурсы
2) кондиционер
3) солнечный свет
4) воздух
Задание 3 (установите соответствие между объектами задания и вариантами ответа).
Установите соответствие между названиями стадий общественного производства и их содержанием.
1. Производство
2. Распределение
3. Потребление
Варианты ответов:
1) процесс создания полезного продукта
2) определение доли каждого человека в произведенном продукте
3) использование созданных материальных и духовных благ и услуг для удовлетворения человеческих потребностей
4) процесс обмена одних продуктов на другие

Кейс 4
Средняя стоимость основных средств предприятия по группа в текущем году составляла (в млн. руб.): здания – 25, сооружения – 5, машины и оборудование 50, в том числе установленное в начале года - 10.
Норма амортизации для пассивной части составляет 5%, для активной – 15%. Метод амортизации – линейный. Для нового. Работающего 1 год оборудования, применяется метод суммы числе лет.
Численность работающих на предприятии приведена в таблице:
<table>
<tr><td></td><td>Численность, чел.</td><td>Среднемесячная заработная</td></tr>
<tr><td>очие</td><td>50</td><td>25000</td></tr>
<tr><td>ные рабочие</td><td>30</td><td>22000</td></tr>
<tr><td></td><td>10</td><td>40000</td></tr>
</table>
</td><td></td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Специалисты | 12 | 35000 Служащие | 2 | 20000 Страховые взносу в государственные внебюджетные социальные фонды – 30%. Годовой объем производства составляет 1000000 единиц продукции. На производство единицы продукции затрачено сырья, материалов в и энергетических ресурсов на сумму 152 руб. прочие затраты – в структуре себестоимости составляют 20%. Вся продукция была реализована по средней цене 250 руб. за единицу. Рассчитайте фондоотдачу, производительность труда, себестоимость единицы продукции, прибыль предприятия, критический выпуск (доля условно-постоянных расходов – 25%), рентабельность продукции.	
Знать	– систему финансирования инновационной деятельности в различных сферах жизнедеятельности; – принципы, формы и методы финансирования научно-технической продукции. – средства и методы стимулирования сбыта продукции.	*Теоретические вопросы:* 1. Система финансирования инновационной деятельности в различных сферах жизнедеятельности. 2. Принципы, формы и методы финансирования научно-технической продукции. 3. Понятие и экономическое содержание результатов научной и научно-технической деятельности. 2. Экономические показатели, характеризующие научную деятельность. 3. Классификация научно-технической продукции по экономическим критериям. 4. Источники финансирования инновационных проектов. 5. Формы финансирования инновационной деятельности. 6. Формы государственной поддержки инновационной деятельности. 7. Средства и методы стимулирования сбыта продукции.	Б1.Б.40Продвижение научной продукции
Уметь	– анализировать экономическую и научную литературу; – анализировать рынок научно-технической продукции – рассчитывать экономические показатели структурного подразделения организации;	*Практические задания:* Подготовка (написание) рефератов на предложенные или самостоятельные тематики: 1. Понятие научной деятельности, показатели ее характеризующие, источники финансирования. 2. Проблемы анализа рынка научно-технической	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	– анализировать существующие и потенциальные запросы потребителей, возможностей создания ценностей для потребителя с учетом особенностей жизненного цикла продукции и технологий; – выделять основные этапы продвижения научного товара и пути его совершенствования в условиях Российского рынка научной продукции; – определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий, глобальный информационный ресурсов.	продукции. 3. Научно-техническая продукция как товар особого рода. 4. Процесс производства, реализации и использования научно-технической продукции. 5. Классификация научно-технической продукции по экономическим критериям. 6. Организация и планирование продвижения товара и пути его совершенствования. 7. Средства и методы стимулирования сбыта продукции. 8. Принципы, формы и методы финансирования научно-технической продукции. 9. Основные этапы продвижения научного товара и пути его совершенствования в условиях Российского рынка научной продукции. 10. Формы государственной поддержки инновационной деятельности в России. 11. Производственный процесс и основные принципы его организации. 12. Порядок и особенности выполнения научно-исследовательских работ по государственным контрактам.	
Владеть	– способами оценивания значимости и практической пригодности инновационной продукции; – методами стимулирования сбыта продукции; – расчетом цен инновационного продукта; – современными методиками расчета и анализа показателей и индикаторов, характеризующие инновационную деятельность предприятия и возможности реализации инновационного проекта.	*Творческие задания:* 1. Разработать концепцию (методику) стимулирования сбыта конкретной научно-технической продукции. 2. Разработать концепцию (методику) оценивания значимости и практической пригодности конкретной инновационной продукции.	
Знать	основы экономических знаний, составляющих категориальный аппарат технологического предпринимательства, специфику и возможности их применения в различных сферах профессиональной деятельности;	**Перечень теоретических вопросов к зачету:** 1. Сущность и свойства инноваций. 2. Модели инновационного процесса и их характеристика. 3. Роль предпринимателя в инновационном процессе. 4. Классификация инноваций и их характеристика.	ФТД.03 Технологическое предпринимательство

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		5. Формирование и развитие команды. 6. Командный лидер, типы командного лидерства. 7. Бизнес-идея, основные методы ее генерирования. 8. Бизнес модель, элементы бизнес-модели. 9. Понятие и общая структура эффективных презентаций. 10. Виды презентаций и их характеристика. 11. Понятие и особенности питч-сессии. Сущность и основные разделы бизнес-плана. 12. Основные виды маркетинговых исследований, их характеристика. 13. Методы маркетинговых исследований. 14. Оценка рынка и целевой сегмент.	
Уметь	оперировать основами экономических знаний, составляющих категориальный аппарат технологического предпринимательства; использовать основы экономических знаний, составляющих категориальный аппарат технологического предпринимательства в различных сферах профессиональной деятельности;	**Перечень теоретических вопросов к зачету:** 1. Особенности продаж инновационных продуктов. 2. Методы разработки и жизненный цикл продукта. 3. Концепция Customer development. 4. Методы моделирования потребностей потребителей. 5. Понятие, методики и этапы развития стартапа. 6. Понятие и особенности коммерческого НИОКР. 7. Источники и инструменты финансирования предпринимательских проектов. 8. Понятие и критерии оценки инвестиционной привлекательности предпринимательских проектов. 9. Денежные потоки предпринимательского проекта. 10. Понятие и типология рисков предпринимательского проекта. 11. Методы количественного анализа рисков предпринимательского проекта. 12. Инновационная среда и ее структура. 13. Инновационный потенциал предпринимательского проекта (компании). 14. Сущность и структура национальных инновационных систем. 15. Понятие и элементы инновационной инфраструктуры. 16. Государственная инновационная политика.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	профессиональным языком предметной области знания; категориальным аппаратом технологического предпринимательства в различных сферах деятельности;	Разработанный и защищенный групповой и, или индивидуальный проект, выполненный в соответствии со всеми требованиями.	
ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма			
Знать	Основные проблемы, периоды, тенденции и особенности исторического процесса, -Осознавать место истории России во всемирно-историческом процессе	Экзаменационные вопросы: 1. История в системе социально-гуманитарных наук. Основы методологии исторической науки. 2. Государство и общество в Древнем мире 3. Средневековье как стадия всемирного исторического процесса 4. Раннее новое время: переход к индустриальному обществу 5. Мир в XVIII – XIX веках: попытки модернизации и промышленный переворот. 6. Мир в начале XX века. Первая мировая война. 7. Мир между двумя мировыми войнами. Вторая мировая война 8. Послевоенное устройство мира в 1946 – 1991 гг. 9. Мировое сообщество на рубеже XX - XXI веков. 10. Древнерусское государство в IX – XII вв. 11. Русские земли в период раздробленности. Борьба русских земель с иноземными захватчиками. 12. Образование и становление русского централизованного государства в XIV– первой трети XVI вв. 13. Иван Грозный: реформы и опричнина. 14. Смутное время в России. 15. Россия в XVII в. 16. Русская культура в IX – XVII вв. 17. Преобразования традиционного общества при Петре I.	Б1.Б.01История

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		18. Дворцовые перевороты. Правление Екатерины II. 19. Россия в первой половине XIX в. 20. Россия во второй половине XIX в. 21. Русская культура в XVIII – начале XX вв. 22. Первая российская революция 1905-1907 гг. и ее последствия. 23. Россия в 1917 г. 24. Социалистическая революция и становление советской власти (октябрь 1917 – май 1918 гг.). 25. Гражданская война и интервенция в России. Военный коммунизм. 26. Образование СССР 1922-1941 гг. 27. Внутренняя политика СССР в 1920 – 1930-е гг. 28. СССР в годы Великой Отечественной войны. 29. СССР в 1945-1964 гг.: послевоенное восстановление народного хозяйства и попытки реформирования. 30. СССР в 1965 – 1991 гг. 31. Особенности развития советской культуры. 32. Внутренняя политика Российской Федерации (1991 – 2000-е гг.) Тесты: 1. Куликовская битва: 1. 1237 г.; 2. 1480 г.; 3. 1223 г.; 4. 1380 г. 2. Опричнина: 1. 1565-1572 гг.; 2. 1598-1605 гг.; 3. 1550-1572 гг.; 4. 1556-1582 гг.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		3. Созыв первого Земского собора: 1. 1549 г.; 2. 1497 г.; 3. 1613 г.; 4. 1649 г. 4. Третьиюньская монархия: 1. 1905-1907 гг.; 2. 1894-1917 гг.; 3. 1907-1914 гг.; 4. 1914-1917 гг. 5. Брестский мир: 1. 1917 г.; 2. 1918 г.; 3. 1919 г.; 4. 1920 г. 6. В 1721 г.: 1. отмена крепостного права; 2. провозглашение России империей; 3. присоединением к России Крыма; 4. принятие «Соборного уложения». 7. Год царствования Екатерины II: 1. 1721 г.; 2. 1755 г.; 3. 1785 г.; 4. 1801 г. 8. Замена коллегий министерствами: 1. 1718 г.; 2. 1802 г.; 3. 1874 г.; 4. 1881 г.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		9. Полтавское сражение: 1. 1702 г. 2. 1709 г.; 3. 1711 г.; 4. 1714 г. 10. Реформа управления государственными крестьянами П.Д. Киселева: 1. 1801-1803 гг.; 2. 1837-1841 гг.; 3. 1861-1863 гг.; 4. 1881-1894 гг. 11. Начало «хождения в народ»: 1. 1863 г.; 2. 1873 г.; 3. 1883 г.; 4. 1895 г. 12. В 1700 г.: 1. Северная война; 2. городские восстания; 3. русско-турецкая война; 4. церковный раскол. 13. Декрет о земле: 1. 1917 г.; 2. 1918 г.; 3. 1921 г.; 4. 1924 г. 14. Полное прекращение выкупных платежей крестьянами: 1. 1803 г.; 2. 1861 г.; 3. 1894 г.; 4. 1907 г.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		15. Переход к нэпу: 1. 1919 г.; 2. 1921 г.; 3. 1924 г.; 4. 1927 г. 16. Период 1700-1721 гг.: 1. Двадцатилетняя война; 2. Северная война; 3. Отечественная война; 4. русско-турецкая война. 17. Крестьянская война под предводительством Е.И. Пугачева: 1. 1606-1607 гг.; 2. 1670-1671 гг.; 3. 1707-1708 гг.; 4. 1773-1775 гг. 18. Москва – столица РСФСР: 1. 1917 г.; 2. 1918 г.; 3. 1920 г.; 4. 1922 г. 19. 1922 г. – год образования: 1. РСФСР; 2. СССР; 3. УССР; 4. БССР. 20. Восстание в Кронштадте: 1. 1918 г.; 2. 1920 г.; 3. 1921 г.; 4. 1922 г.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		21. Испытание первой атомной бомбы в СССР: 1. 1945 г.; 2. 1949 г.; 3. 1952 г.; 4. 1954 г. 22. Избрание Н.С. Хрущева Первым секретарем ЦК КПСС: 1. 1953 г.; 2. 1956 г.; 3. 1964 г.; 4. 1972 г. 23. Принятие первой Конституции РСФСР: 1. 1917 г.; 2. 1918 г.; 3. 1924 г.; 4. 1936 г. 24. Первый секретарь (Генеральный секретарь) ЦК партии в 1964-1982 гг.: 1.Ю.В. Андропов; 2. И.В. Сталин; 3. Н.С. Хрущев; 4. Л.И. Брежнев. 25. Принятие христианства на Руси: 1. 962 г.; 2. 988 г.; 3. 989 г.; 4. 991 г. 26. Введение в России нового летоисчисления: 1. 1700 г.; 2. 1721 г.; 3. 1725 г.;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4. 1800 г. 27. Принятие Указа о «вольных хлебопашцах»: 1. 1803 г.; 2. 1861 г.; 3. 1883 г.; 4. 1894 г. 28. Созыв Учредительного собрания: 1. 1917 г.; 2. 1918 г.; 3. 1919 г.; 4. 1921 г. 29. Съезд князей в Любече: 1. 1097 г.; 2. 1136 г.; 3. 1147 г.; 4. 1199 г. 30. Ливонская война: 1. 1558-1583 гг.; 2. 1565-1572 гг.; 3. 1609-1612 гг.; 4. 1700-1721 гг.	
Уметь	обнаруживать причинно-следственные связи и использовать принцип историзма в характеристике социальных явлений	Практические задания:: Запишите цифры согласно хронологической последовательности событий: 1. издание Манифеста «О даровании вольности и свободы всему российскому дворянству»**;** **2. проведение губной реформы;** 3. строительство белокаменного Московского Кремля; 4. царствование Бориса Федоровича Годунова. Ответ: _____	

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>2. Распределите события по периодам согласно хронологической последовательности: в группу А – события, связанные с правлением Павла I; в группу Б – события, связанные с правлением Александра I:
1. ограничение свободы книгопечатания;
2. издание Манифеста «О трехдневной барщине»;
3. образование в Санкт-Петербурге тайного общества «Союз спасения»;
4. принятие университетского устава, предоставившего автономию университетам;
5. упразднение дворянских собраний в губерниях.
6. начало создания военных поселений.
<table>
<tr><td colspan="3">Группа А</td><td>Группа Б</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
3. Установите соответствие между датами и событиями:
1. 1989; А) объявление СССР войны Японии;
2. 1945; Б) издание Указа об отмене телесных наказаний;
3. 1857; В) начало ликвидации военных поселений;
4. 1863. Г) проведение I съезда народных депутатов СССР;
Д) принятие СССР в Лигу Наций.
Ответ: _____

4. Запишите цифры согласно хронологической последовательности событий:
1. принятие Конституции «развитого социализма»;
2. издание Постановлений ЦК ВКП(б), ЦИК и СНК СССР о борьбе с кулаками;
3. издание Постановления ЦК ВКП(б) «О преодолении культа личности и его последствий»;
4. издание Декрета об установлении 8-часового рабочего дня;
5. проведение XIX Всесоюзной партконференции.
Ответ: _____

5. Распределите события по периодам согласно хронологической</td><td></td></tr>
</table>

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>последовательности: в группу А – события, связанные с правлением Ивана IV; в группу Б – события, связанные с правлением Петра I:
1. основание Петербурга;
2. проведение опричнины;
3. издание Указа о престолонаследии;
4. учреждение Синода;
5. разгром Ливонского ордена;
6. образование «Избранной рады».
<table>
<tr><td colspan="3">Группа А</td><td>Группа Б</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
6. Установите соответствие между датами и событиями:
1. 1912 г. А) издание Манифеста о веротерпимости и свободе вероисповедания;
2. 1905 г. Б) проведение Второго съезда РСДРП;
3. 1903 г. В) Ленский расстрел;
4. 1907 г. Г) аграрная реформа П.А. Столыпина;
Д) отмена подушной подати.
Ответ: _____

7. Ранее других произошло:
1. начало возведения Берлинской стены;
2. Карибский кризис;
3. запуск первой в мире атомной электростанции;
4. проведение XXVI съезда КПСС.

8. Укажите ответ с правильным соотношением события и года:
1. 1841 – издание «Городового положения»;
2. 1919 – издание Декрета о ликвидации неграмотности;
3. 1918 – создание ВЧК;
4. 1917 – проведение V Всероссийского съезда Советов;
5. 1870 – запрещение продажи крестьян в розницу.

9. Распределите события по периодам согласно хронологической последовательности: в группу А – события, связанные с</td><td></td></tr>
</table>

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>правлением Ивана III; в группу Б – события, связанные с правлением Ивана IV:
1. путешествие Афанасия Никитина в Индию;
2. проведение Стоглавого собора;
3. создание приказной системы;
4. созыв первого Земского собора;
5. «Стояние на реке Угре»;
6. присоединение к Москве юго-западных русских земель.
<table><tr><td colspan="3">Группа А</td><td>Группа Б</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>
10. Соотнесите события и годы:
1. 1917; А) создание Временного правительства;
2. 1918; Б) конфликт на КВЖД;
3. 1922; В) начало первой пятилетки;
4. 1928. Г) созыв Учредительного собрания;
Д) образование СССР.
Ответ: _____

11. В XV веке княжил:
1. Дмитрий (Донской);
2. Василий II (Темный);
3. Иван II (Красный);
4. Василий III.

12. Укажите событие, произошедшее 29 апреля 1881 года:
1. учреждение Крестьянского поземельного банка;
2. возобновление Союза трех императоров.
3. издание Манифеста «О незыблемости самодержавия»;
4. принятие Положения об обязательном выкупе крестьянских наделов.

13. Событие, произошедшее ранее других в 1917 году:
1. подписание Николаем II в Пскове акта об отречении от престола;
2. открытие Предпарламента;
3. проведение Первого Всероссийского съезда Советов рабочих и</td><td></td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		солдатских депутатов в Петрограде; 4. начало «хлебных бунтов» в Петрограде; 5. отмена смертной казни на фронте. 14. Укажите вариант ответа с правильным соотношением фамилии и года руководства страной: 1. Брежнев Л.И. 1966 г.; 2. Горбачев М.С. 1974 г.; 3. Сталин И.В. 1954 г.; 4. Хрущев Н.С. 1969 г. 15. Соотнесите имя и год княжения: 1. Игорь А) 970; 2. Владимир Мономах Б) 977; 3. Святослав I В) 1113; 4. Ярополк I Д) 912. Ответ: _____ 16. Запишите цифры согласно хронологической последовательности событий: 1. учреждение Непременного совета; 2. *сражение* под Аустерлицем; 3. заключение Тильзитского мира; 4. преобразование «Союза спасения» в «Союз благоденствия». 5. замена Конституции Царства Польского «Органическим статутом». Ответ: _____ 17. Распределите события по периодам согласно хронологической последовательности: в группу А – события, связанные с правлением Павла I; в группу Б – события, связанные с правлением Екатерины II: 1. издание Указа о запрещении ввоза всех иностранных книг; 2. издание Жалованной грамоты дворянству; 3. запрет продавать крестьян без земли с аукционов; 4. восстание Е.И. Пугачева;	

<table>
<tr><td>Структурный элемент компетенции</td><td>Планируемые результаты обучения</td><td>Оценочные средства</td><td>Структурный элемент образовательной программы</td></tr>
<tr><td></td><td></td><td>5. секуляризация церковных и монастырских земель;
6. запрет отсутствия на службе дворян, приписанных к гвардейским полкам.
<table><tr><td colspan="3">Группа А</td><td>Группа Б</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>
18. Соотнесите событие и год:
1. издание Указа Президента РСФСР о приостановлении деятельности КПСС на территории России; А) 1990;
2. проведение выборов в Совет Федерации и Государственную Думу первого созыва; Б) 1996;
3. избрание М.С. Горбачева Президентом СССР; В) 1989;
4. принятие России в члены Совета Европы; Г) 1991;
Д) 1993.
Ответ: _____

19. Организация, созданная ранее других:
1. «Союз борьбы за освобождение рабочего класса»;
2. «Северный союз русских рабочих»;
3. «Земля и воля»;
4. «Освобождение труда».

20. Запишите цифры согласно хронологической последовательности событий:
1. «Ледовое побоище» на Чудском озере;
2. строительство белокаменного Московского Кремля;
3. княжение Василия I Дмитриевича;
4. княжение Андрея Юрьевича (Боголюбского);
5. съезд князей в Любече.
Ответ: _____</td><td></td></tr>
<tr><td>Владеть</td><td>Навыками работы с историческими документами и анализа исторических событий и явлений.</td><td>Вопросы для самопроверки:

1. В какие годы правила династия Рюриковичей?</td><td></td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		2. Кто из князей, и в какие годы правил в Киеве в X в.? Расскажите об их деятельности. 3. Какие главные события происходили на Руси в IX-начале XII вв.? 4. Какими событиями отмечено правление князя Владимира I? 5. Когда и какие правовые акты были приняты в IX-XII вв.? 6. Какие достижения культуры Древней Руси можете назвать? 7. Кто из князей, и в какие годы правил в Киеве в XI в.? Расскажите о их деятельности. 8. Чем прославился князь Ярослав (Мудрый)? 9. Какие важные события происходили в период правления Владимира (Мономаха)? 10. Каковы основные этапы борьбы русских земель с монгольским завоеванием? 11. Каковы особенности правления Ивана (Калиты)? 12. Какими важными событиями отмечен период завершения объединения русских земель вокруг Москвы в конце XV-начале XVI вв.? 13. Чем знаменателен период правления Ивана IV? 14. Какие события происходили в Смутное время? 15. Каковы были взаимоотношения России с Речью Посполитой в XVII в.? 16. Какими событиями отмечено царствование Михаила Федоровича и Алексея Михайловича Романовых? 17. Чем были вызваны народные выступления в XVII в.? 18. В чем состояла особенность русско-шведских отношений в XVII-XVIII вв.? 19. Когда и какие основные реформы были проведены Петром I? 20. Какие даты войн России с другими странами в XVIII в. можно назвать? 21. Какие международные договоры заключила Россия в XVIII в.? 22. Какие российские правители пришли к власти путем дворцового переворота в XVIII в.? Расскажите о их деятельности. 23. Какие реформы провела Екатерина II? 24. Каковы достижения российской культуры и науки в XVII-XVIII вв.? 25. Каково содержание мирных договоров России с Османской	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		империей в XVII-XIX вв.? 26. Когда и какие реформы проводили Александр I и Александр II? 27. Какие меры были осуществлены по отмене крепостного права? 28. Какие общественно-политические организации появились в России во второй половине XIX в.? 29. Какие международные договоры были заключены Россией в XIX в.? Расскажите об их содержании. 30. Какие основные события происходили в период царствования Александра III? 31. Какие политические партии, и в какие годы образовались в России в конце XIX-начале XX вв.? 32. Какие важные военные операции были проведены в ходе Первой мировой войны? 33. Каковы временные рамки деятельности Государственных Дум Российской империи и их состав по партийной принадлежности? 34. Как развивались события в стране в 1905-1907 гг.? 35. Какие основные события происходили во время Февральской революции 1917 г.? 36. В течение какого периода действовало каждое из Временных правительств в 1917 г.? 37. Какие правовые акты были приняты в первые годы советской власти? 38. Какие внешнеполитические акции характерны для советского государства в 1920-1930-е гг.? 39. Какие события, связанные с репрессиями 1930-1950-х гг., можете назвать? 40. Какие изменения в экономике СССР произошли в годы первых пятилеток? 41. Когда и какие наиболее значимые битвы происходили в годы Великой Отечественной войны? 42. Какие знаменательные даты времени хрущевской «оттепели» можно назвать? 43. Какие Постановления руководства СССР второй половины 1960-х – первой половины 1980-х гг. посвящались экономическим проблемам? 44. Когда были приняты Конституции СССР? 45. Какова роль СССР в послевоенном развитии мира?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		46. Каковы основные вехи развития российской культуры в XX вв.? 47. Какие изменения происходили в стране в ходе перестройки? 46. Какие основные события произошли в России в 1990-е гг.? 48. Как изменялись предпочтения избирателей в ходе президентских и думских выборов в 1990-е – 2000-е гг.? 49. Какие научные достижения XX в. прославили Россию? 50. Кто из россиян являлся лауреатом Нобелевской премии? 51. Какие важные события в стране произошли в начале 2000-х гг.?	
Знать	Процесс историко-культурного развития человека и человечества; всемирную и отечественную историю и культуру; особенности национальных традиций, текстов; движущие силы и закономерности исторического процесса; место человека в историческом процессе; политическую организацию общества.	Теоретические вопросы к зачету a. В каком году состоялись первые Олимпийские Игры современности? b. В каком году наша страна принимала летние Олимпийские игры? c. В каком году и в каком городе российский спортсмен впервые победил на Олимпийских играх? d. Как называется традиционный ритуал с участием спортсмена и судьи? e. Какие цвета используют для Олимпийских колец? f. Какого цвета полотнище Олимпийского флага? g. Где проходили первые Олимпийские Игры современности? h. В 1956 году во время Олимпийских игр в г. Мельбурне, в Австралию нельзя было привезти лошадей. i. В каком европейском городе прошли Олимпийские состязания по конному спорту? j. К каком городе проходили Олимпийские игры 1980 года? k. Что сделал Олимпийский мишка на закрытии Олимпийские игры 1980 года? l. Как себя повели кольца на открытии Сочинской Олимпиады? m. В каком порядке приносят клятву участники	Б1.Б.41 Физическая культура и спорт

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Олимпийских игр? n. Кто из спортсменов нашей страны завоевал боль всех золотых Олимпийских медалей?	
Уметь	Определять ценность того или иного исторического или культурного факта или явления; уметь соотносить факты и явления с исторической эпохой и принадлежностью к культурной традиции; проявлять и транслировать уважительное и бережное отношение к историческому наследию и культурным традициям; анализировать многообразие культур и цивилизаций; оценивать роль цивилизаций в их взаимодействии.	*Перечень заданий для зачета:* 1. Физическая культура и спорт как социальный феномен современного общества. 2. Средства физической культуры. 3. Основные составляющие физической культуры. 4. Социальные функции физической культуры. 5. Формирование физической культуры личности. 6. Физическая культура в структуре высшего профессионального образования. 7. Организационно-правовые основы физической культуры и спорта студенческой молодѐ жи России.	
Владеть	ками исторического, историко-типологического, сравнительно-типологического анализа для определения места профессиональной деятельности в культурно-исторической парадигме; навыками бережного отношения к культурному наследию и человеку; информацией о движущих силах исторического процесса; приемами анализа сложных социальных проблем в контексте событий мировой истории и современного социума.	*Задания на решение задач из профессиональной области, комплексные задания* 1. Физическая культура как часть культуры общества. 2. Физическая культура как особая сфера человеческой деятельности. 3. Уровни физической культуры личности. 4. Функции физической культуры. 5. Цель и задачи физической культуры. 6. Структура физической культуры. 7. Виды и разновидности физической культуры. 8. Дать характеристику принципа всестороннего гармоничного развития личности. 9. Дать характеристику принципа связи физической культуры с практической жизнью общества. 10. Дать характеристику принципа оздоровительной направленности. 11. Педагогическая направленность, цель и задачи физического воспитания. 12. Система физического воспитания. 13. Основы системы физического воспитания (социально-экономические, правовые основы).	
ОК-4	**способностью использовать основы правовых знаний в различных сферах деятельности**		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Знать	– основные правовые понятия; – основные источники права; – принципы применения юридической ответственности.	**Перечень вопросов для подготовки к зачету:** 1. Понятие, признаки государства 2. Форма правления: понятие, виды 3. Форма государственного устройства: понятие, виды 4. Государственный режим: понятие, виды. 5. Конституция Российской Федерации – основной закон государства. 6. Форма правления Российской Федерации. 7. Система органов государственной власти в Российской Федерации. 8. Президент Российской Федерации. 9. Федеральное Собрание Российской Федерации. 10. Правительство Российской Федерации. 11. Система судов в Российской Федерации. 12. Особенности федеративного устройства России. 13. Понятие и сущность права. 14. Источники права. 15. Система законодательства Российской Федерации. Нормативно-правовые акты, их виды. 16. Отрасли российского права. 17. Правонарушение: понятие, признаки, виды. 18. Юридическая ответственность, понятие и виды. 19. Предмет и метод гражданского права. 20. Субъекты и объекты гражданского права. 21. Правоспособность и дееспособность физических лиц. 22. Юридические лица: понятие, виды, особенности создания и прекращения деятельности. 23. Гражданско-правовые сделки, их виды, формы и условия действительности. 24. Понятие права собственности. Вещные права лица, не являющегося собственником. 25. Основания приобретения права собственности. 26. Основания прекращения права собственности. 27. Виды гражданско-правовых договоров и способы обеспечения их исполнения.	Б1.Б.05Правоведение

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		28. Наследование по закону и по завещанию. 29. Заключение брака. 30. Прекращение брака. Признание брака недействительным. 31. Имущественные права супругов. 32. Права и обязанности родителей и детей. 33. Алиментные обязательства (субъекты, условия и порядок выплаты). 34. Лишение родительских прав. 35. Предмет трудового права. 36. Трудовой договор: условия, стороны, порядок заключения. 37. Порядок приема на работу. Испытательный срок. 38. Понятие и виды рабочего времени 39. Время отдыха 40. Трудовая дисциплина и ответственность за ее нарушение. 41. Материальная ответственность работника: понятие, основания и порядок применения. 42. Материальная ответственность работодателя: понятие, основания и порядок применения. 43. Прекращение трудового договора. 44. Предмет и метод административного права. 45. Субъекты административного права. 46. Государственная служба. 47. Административные правонарушения и административная ответственность. Состав административного проступка. 48. Административные взыскания. Наложение административного взыскания. 49. Определение государственной тайны. 50. Предмет и метод уголовного права. 51. Понятие преступления. Категории преступлений. 52. Состав преступления. 53. Уголовная ответственность за совершение преступлений. 54. Предмет и метод экологического права. 55. Источники экологического права. 56. Право общего и специального природопользования.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	– ориентироваться в системе законодательства; – определять соотношение юридического содержания норм с реальными событиями общественной жизни; – разрабатывать документы правового характера; – приобретать знания в области права; – корректно выражать и аргументированно обосновывать свою юридическую позицию.	**Примерные практические задания** Используя статьи Конституции Российской Федерации, сосчитайте количество субъектов Российской Федерации: республик, краёв, областей, автономных округов, автономных областей, городов федерального значения. Укажите, какие новые субъекты Российской Федерации появились за последнее время. **Аргументируйте свой ответ со ссылкой на статьи Конституции РФ.**	
Владеть	– практическими навыками анализа и разрешения юридических ситуаций; – практическими навыками совершения юридических действий в соответствии с законом; – навыками составления претензий, заявлений, жалоб по факту неисполнения или ненадлежащего исполнения прав; – способами совершенствования правовых знаний и умений путем использования возможностей информационной среды.	**Примерные практические задания:** Составьте текст завещания, включив следующие условия: - несколько наследников - одного наследника по закону лишить наследства - определить завещательное возложение - определить завещательный отказ	
Знать	– основные виды охранных документов интеллектуальной собственности; – ключевые этапы и правила государственной системы регистрации результатов научной деятельности; – формы государственной поддержки инновационной деятельности в России.	*Теоретические вопросы:* 1. Понятие и правовое содержание результатов научной и научно-технической деятельности. 2. Виды охранных документов интеллектуальной собственности. 3. Виды научно-технических услуг. 4. Изобретательство. Изобретение. 5. Изобретательство. Полезная модель. 6. Государственная регистрация научных результатов. 7. Основные цели и принципы государственной научно-технической политики. 8. Формы государственной поддержки инновационной деятельности. 9. Нетрадиционные меры государственной поддержки.	Б1.Б.40 Продвижение научной продукции
Уметь	– анализировать социально-политическую и научную литературу;	*Практические задания:*	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	– оформлять документацию; – использовать основные правовые знания при закреплении основных результатов экспериментальной и исследовательской работы; – составлять пакет документов для регистрации изобретения или полезной модели; – составлять пакет документов для регистрации программы ЭВМ;	Подготовка докладов-презентаций на предложенные или самостоятельные тематики: 1) Пример составления пакета документов для регистрации программы ЭВМ. 2) Пример составления пакета документов для регистрации изобретения. 3) Пример составления пакета документов для регистрации полезной модели. 4) Организация и планирование продвижения товара и пути его совершенствования. 5) Формы государственной поддержки инновационной деятельности в России. 6) Научно-техническая политика России. 7) Порядок и особенности выполнения научно-исследовательских работ по государственным контрактам.	
Владеть	– вопросами правового регулирования деятельности предприятия; – знаниями о научно-технической политики России – навыками составления конкурсной документации.	*Творческие задания:* 1. Аналитический обзор научно-технической политики России. 2. Оформление методики анализа патентной документации и проведения патентного поиска.	
Знать	основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	Теоретические вопросы 1. Основы законодательства Российской федерации в области информационной безопасности. 2. Понятие и виды защищаемой информации. 3. Основы международного законодательства в области защиты информации. 4. Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. 5. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. 6. Понятие лицензирования. Нормативные правовые акты	Б1.Б.31Организационное и правовое обеспечение информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. 7. Понятие сертификации. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации. 8. Регуляторы в области информационной безопасности. 9. Сущность организационных методов защиты информации.	
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности - владения юридической терминологией; -навыками работы с правовыми актами; навыками реализации правовых норм; навыками принятия необходимых мер правового регулирования и (или) защиты интересов субъектов правовых отношений	1. Определить регуляторы и мероприятия по контролю и надзору за деятельностью аккредитованных испытательных лабораторий и органов по сертификации средств защиты информации в системе сертификации средств защиты информации по требованиям безопасности информации.	
Владеть	-навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике	1. Обосновать необходимость проведения лицензирования выбранного вида деятельности по защите информации. Указать порядок и необходимость (обязательная или добровольная) аккредитации выбранного вида деятельности по защите информации.	
Знать	- основы законодательства Российской Федерации; - нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации;	**Теоретические вопросы** **1.** Перечислить стандарты, относящиеся к управлению информационной безопасностью. **2.** Основные положения стандарта управления информационной безопасностью BS 7799. **3.** Основные положения стандарта управления информационной безопасностью ISO/IEC 17799. **4.** Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности.	Б1.Б.34Управление информационной безопасностью

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- меры правовой и дисциплинарной ответственности за разглашение защищаемой информации.	Требования.»	
Уметь	- обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей; - предпринимать необходимые меры по восстановлению нарушенных прав.	Сформулировать цели внедрения ISO 27001/17799 в организации. Провести сертификацию заданной СУИБ на соответствие ISO 27001.	
Владеть	- навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов.	Описать этапы разработки и внедрения системы управления ИБ	
Знать	правовые основы технологического предпринимательства;	*«Нематериальные активы. Охрана интеллектуальной собственности»* №1. При проведении опытно-конструкторской работы в лаборатории научно-исследовательского института научный сотрудник Матвеев изобрел новое устройство. Заведующий этой лабораторией Карпов потребовал указать в качестве авторов изобретения не только Матвеева, но и его, Карпова, поскольку он осуществлял общее руководство данной работой, контролировал ход ее выполнения и оказывал Матвееву всяческое организационное и материальное содействие, вникал в суть разработки и давал ценные советы. Матвеев согласился на это при условии, что это будет оформлено договором и за это ему будет заплачено. Карпов и Матвеев подписали соглашение, из которого следовало, что стороны признают, что они являются соавторами изобретения, и было дано описание изобретения. Оговоренную сумму Карпов немедленно передал Матвееву. Институт оформил на данное изобретение патент, в котором обладателем исключительного права на изобретение был указан институт, а авторами изобретения были указаны Матвеев и Карпов. Впоследствии Матвеев поссорился с Карповым и решил добиться исключения указания на авторство Карпова из патента. Выберите правильную юридическую оценку описанной ситуации:	ФТД.03 Технологическое предпринимательство

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		А) ситуация соответствует закону, поскольку интеллектуальные права являются передаваемыми и отчуждаемыми активами. Матвеев не имеет права оспаривать соавторство Карпова; Б) продажа авторства законом не признается и не защищается. Сделка Карпова и Матвеева ничтожна, потому что заведующий лабораторией не внес никакого личного творческого вклада в создание изобретения и не может считаться автором по закону. Матвеев имеет основания для оспаривания соавторства Карпова; В) Карпов является соавтором Матвеева в силу закона. Соглашение Карпова и Матвеева является излишним и недействительным. Матвеев не имеет права оспаривать соавторство Карпова и должен вернуть Карпову полученные от него деньги. №2. Вы провели исследование в области химии, в результате которого открыли новый закон природы, синтезировали ранее не известное вещество и написали об этом научную статью. Выделите и охарактеризуйте все охраноспособные результаты интеллектуальной деятельности: А) научное открытие, новое вещество (изобретение), научная статья (произведение науки); Б) новое вещество (изобретение), научная статья (произведение науки); В) новое вещество (изобретение) при условии его патентования, научная статья (произведение науки) при условии ее опубликования. №3. Антонов – единственный автор разработки – раскрыл ее суть в докладе на конференции. Доклад был опубликован 01 февраля 2016 г. Далее, 18 февраля 2017 г. Антонов обратился к патентному поверенному за услугами по оформлению заявки на регистрацию данной разработки как изобретения в Роспатенте. Патентный поверенный заявил о непатентоспособности данной разработки, поскольку она уже известна из уровня техники, т.к. информация о ней была раскрыта в опубликованном докладе. Прав ли патентный поверенный согласно п. 3 ст. 1350 ГК РФ: А) нет, потому что Антонов является единственным автором разработки, поэтому не «конкурирует» сам с собой и эта	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		публикация не может считаться для него вошедшей в уровень техники; Б) нет, потому что льготный срок на подачу заявки после раскрытия информации не истек; В) да, потому что по закону не имеет значения, кто раскрыл данные о разработке, а льготный срок для подачи заявки после раскрытия информации уже истек. №4. Общество с ограниченной ответственностью «Старт Ап» подало в Роспатент заявку на получение патента на коммерчески ценную разработку в качестве изобретения. К «Старт Апу» обратилась компания, заинтересованная в использовании данной разработки, с выгодным предложением приобрести временную неисключительную возможность ее использования. Юрист «Старт Апа» разъяснил руководству фирмы, что, по его мнению, в России это невозможно. Прав ли он: А) да, потому что лицензирование патентных заявок законодательством не предусмотрено; Б) отчасти да, потому что до публикации патентной заявки право использования своей разработки «Старт Ап» может предоставить только в качестве ноу-хау (при условии, что сведения сохранялись в режиме конфиденциальности), а после публикации режим ноу-хау по закону пропадает и до момента получения патента юридический объект пользования отсутствует; В) нет, потому что как до, так и после публикации патентной заявки до получения патента «Старт Ап» может предоставлять право использования соответствующей информации, несмотря на то, что отсутствует охраняемый объект интеллектуальной собственности (ноу-хау, изобретение); а если в отношении разработки соблюдался режим конфиденциальности, то это также возможно по договору о предоставлении права использования ноу-хау (но только до публикации заявки, если вся суть такого ноу-хау заключалась в данном изобретении). №5. Без каких условий лицензионный договор не будет считаться заключенным? А) предмет (конкретизация объекта ИС), способы использования объекта ИС, размер вознаграждения за использование ИС (или указание на безвозмездность договора);	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Б) предмет (конкретизация объекта ИС), способы использования объекта ИС, территория использования объекта ИС, срок действия договора, размер вознаграждения за использование ИС (или указание на безвозмездность); В) способы использования объекта ИС, срок действия договора, ответственность за нарушение договора. *№8 «Трансфер технологий и лицензирование»* №1. Что понимают под трансфером технологий? А) формальную передачу прав на использование и коммерциализацию но стороне; Б) самостоятельное практическое использование и коммерциализацию технологической разработки субъектом, выполняющим научные исследования, в собственном производстве; В) создание объекта интеллектуальной собственности для собственных нужд и дальнейшего применения для перспективных исследований и разработок; Г) нет верного ответа. №2. Можно ли назвать компанию IBM, продающую права на использование технологий, патенты на которые ей принадлежат, патентным троллем? А) да; Б) нет; В) да, но только в случае, если IBM не использует эти технологии в собственной производственной деятельности. №3. В случае, если Ваша компания разработала изобретение, провела патентный поиск, подала заявку и получила от патентного ведомства уведомление о проведении в отношении изобретения экспертизы по существу, а также получила дату приоритета и номер документа (заявки) на патент на изобретение, а также нашла покупателя на данное изобретение, какого вида договор будет заключен: А) патентная лицензия; Б) бесплатная лицензия; В) гибридная лицензия;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Г) нет верного ответа. №4. Какой раздел не является обязательным в лицензионном договоре на использование изобретения, охраняемого патентом в режиме PCT? А) информация об усовершенствованиях, вносимых в технологию, составляющую основу для предмета сделки; Б) перечень сотрудников Лицензиата и Лицензиара, имеющих доступ к информации о технологии; В) информация о сроке действия договора. №5. Какой тип лицензии (исключительная или неисключительная) наиболее выгоден для Лицензиара? А) простая (неисключительная) лицензия, потому что Лицензиар сможет продать права на разработку и другим покупателям; Б) простая (неисключительная) лицензия, потому что цена сделки будет выше, нежели чем при заключении договора исключительной лицензии, ведь объем передаваемых прав значительно больше при простой лицензии; В) исключительная лицензия, так как с Лицензиара снимается обязательство по уплате пошлин за поддержание патента в силе.	
Уметь	понимать и отбирать нормативные документы и методические материалы, необходимые для коммерциализации сложных технологий, технологического предпринимательства и управления инновационными проектами, применять их в процессе деятельности	**Примерные практические задания для зачета** 1. Поясните, к какой гипотезе и к какой модели инновационного процесса – «push» или «pull» относятся процессы, связанные с созданием: - светодиодного фонаря; - нержавеющей стали; - кондиционера; - DVD-дисков. 2. Используя схему, изображенную ниже, раскройте императивные отличия предпринимателя от менеджера, промоутера и изобретателя. Определите, в чем разница между ними по следующим направлениям: - мотивация их действий; - методы реализации новой идеи; - использование ресурсов, формы и методы привлечения необходимых ресурсов, ответственность;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		-отношение к организационной структуре. Рис. Матрица «Креативность – управленческие навыки» 3. Проанализируйте и сравните, какое влияние на существующие рынки оказывают радикальные (базисные) и улучшающие (поддерживающие) инновации. Охарактеризуйте инновации, приведенные ниже, в зависимости от глубины вносимых изменений: - новая операционная система Windows 10, расширяющая возможности пользователя, в том числе сетевые, развитие технологий защиты и безопасности.; - криптовалюта, представляющая собой цифровой актив, учет которого децентрализован, актив защищен от поддержки или кражи за счет использования криптографии и распределенной компьютерной сети. 4. Выясните, какой тип информации необходимо в первую очередь получить во время маркетингового исследования, если: - компания, занимающаяся разработкой приложения по доставке еды, нашла уникальную на рынке нишу - приготовление и доставка домашней еды по запросу соседей; - компания оценивает возможность открытия завода и переноса производства на локальный рынок для большего его освоения. 5. В ходе подготовки обоснования предпринимательского проекта были рассмотрены условия снабжения производства необходимыми материалами и условия сбыта готовой продукции.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Материалы, используемые в производстве, будут оплачены 60 % в текущем месяце, 40 % – в следующем. Запас сырья и материалов создается на месяц. Продукция будет реализована в том же месяце в кредит с оплатой покупателями через два месяца. Месячная периодичность закупок материалов и вывоза готовой продукции сохранится на весь период жизни проекта. Ежемесячный расход сырья и материалов составляет 1 500 тыс. руб.; ежемесячные продажи готовой продукции – 2 600 тыс. руб. Определите необходимую сумму финансовых средств, инвестируемых в предстоящем периоде в оборотный капитал. 6. Оцените уровень эффективности проекта, предполагающего приобретение оборудования, с двухлетним сроком реализации, используя показатели NPV и PI, если инвестиционные затраты составляют 1500 тыс. руб., дисконтная ставка – 11 %, величина чистого денежного потока за первый год – 950 тыс. руб. и за второй год – 600 тыс. руб. 7. Команда из семи человек трудилась над выполнением одного заказа. При этом каждый затратил 40 человеко-часов. Заказ принес компании 2000 млн. руб. Определите производительность труда каждого сотрудника в расчете на человеко-час. 8. Продумайте «презентацию идеи (Idea Pitch)» для компании X, которая разработала технологию управления скутером без участия человека. 9. Укажите, какие из представленных ниже слайдов PPT-презентации предпринимательского проекта нарушают правила питч-сессии. Аргументируйте ответ. 	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	идентификацией корректных нормативных документов и методических материалов, регулирующих процессы коммерциализации сложных технологий, технологического предпринимательства и управления инновационными проектами и применять их в деятельности	Разработанный и защищенный групповой и, или индивидуальный проект, выполненный в соответствии со всеми требованиями.	
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики			
Знать	• политику государства в области обеспечения информационной безопасности • национальные, межгосударственные и международные стандарты в области защиты информации • современное состояние рынка труда в области обеспечения информационной безопасности • профессиональный стандарт «Специалист по защите информации в автоматизированных системах»	Перечень вопросов: 1. Понятие информационной безопасности государства. 2. Понятие целостности и конфиденциальности информации. 3. Требования защиты информации. 4. Национальные интересы РФ в информационной сфере 5. Общие положения доктрины информационной безопасности 6. Классификация и способы информационной войны	Б1.Б.39Введение в специальность

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	• трудовое законодательство РФ		
Уметь	• анализировать информацию по вопросам национальной и информационной безопасности государства; • соблюдать нормы профессиональной этики	1. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области обороны страны в соответствии с военной политикой Российской Федерации. 2. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области государственной и общественной безопасности. 3. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в экономической сфере 4. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области науки, технологий и образования 5. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства	
Владеть	• профессиональной терминологией в области информационной безопасности; • практическими навыками соблюдения норм профессиональной этики	● Разработать глоссарий по доктрине информационной безопасности РФ ● Разработать глоссарий на тему информационные войны	
Знать	- основные профессиональные задачи специалиста по информационной безопасности; - перечень инструкций для информирования персонала об угрозах безопасности информации и о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации; - основы кибербезопасности;	1. Роль кибербезопасности в развитии цифровой экономики. 2. Понятия: Security-токен и utility-токен. 3. Основные типы социальной инженерии и способы защиты от них. 4. Организационные требования защиты информации. 5. Каким наиболее важным аспектам кибербезопасности уделяется должное внимание со стороны государства, а каким необходимо уделять больше внимания.	Б1.Б.42 Основы безопасности цифрового общества
Уметь	- критически оценивать информацию, полученную в цифровой среде;	Провести майндмэппинг и командный мозговой штурм с использованием MindMeister на темы:	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- оценить достоверность информации, полученной в цифровой среде; - строить логические умозаключения на основании поступающих информации и данных;	1. Угрозы безопасности личности, осуществляемые через цифровую среду. 2. Угрозы национальной безопасности, осуществляемые через цифровую среду. 3. Принципы ведения информационных войн.	
Владеть	- критическим мышлением для анализа информации в цифровой среде; - основами профессиональной деятельности в сфере цифровой экономики в условиях нарастающих угроз безопасности информации;	1. На основе статистики с интерактивной карты угроз на сайте Касперского за несколько лет спрогнозировать рост угроз на следующий год. Ответ оформить в виде гистограмм. 2. На основе статистики с международного агентства по кибербезопасности и безопасности инфраструктуры (CISA) за несколько лет спрогнозировать рост угроз на промышленные предприятия на следующий год. Ответ оформить в виде гистограмм.	
Знать	- политику государства в области обеспечения информационной безопасности - национальные, межгосударственные и международные стандарты в области защиты информации - современное состояние рынка труда в области обеспечения информационной безопасности - профессиональный стандарт «Специалист по защите информации в автоматизированных системах» - трудовое законодательство РФ	***Задания на производственную практику:*** *Список индивидуальных тем* 1. Современные средства защиты информации 2. Современные системы компьютерной безопасности 3. Современные криптографические системы 4. Криптоанализ, современное состояние 5. Правовые основы защиты информации 6. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними 7. Технические аспекты обеспечения защиты информации. 8. Атаки на систему безопасности и современные методы защиты 9. Современные пути решения проблемы информационной безопасности РФ 10. Организация центра мониторинга событий на основе современных систем анализа информационной безопасности 11. Информационная безопасность в условиях цифровой экономики Российской Федерации 12. Безопасность сетей беспроводной передачи данных 13. Использование хэш-функций в современном мире и их криптостойкость 14. Проблемы применения средств защиты информации в	Б2.Б.01(У) Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	- анализировать информацию по вопросам национальной и информационной безопасности государства; - соблюдать нормы профессиональной этики		
Владеть	- профессиональной терминологией в области информационной безопасности; - практическими навыками соблюдения норм профессиональной этики		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		операционной системе Windows 15. Алгоритмы тестирования генераторов псевдослучайных чисел 16. Система накопления и анализа данных для контроля за инцидентами в сфере информационной безопасности с учетом поведенческого подхода 17. Анализ законодательства в области размещения и использования ИТСНК на территории Российской Федерации 18. Анализ угроз безопасности информации. Возможные организационные меры, применяемые для нейтрализации ряда угроз безопасности информации 19. Актуальность обеспечения информационной безопасности на промышленных предприятиях 20. Безопасность в мире «Интернета вещей» 21. Безопасность распознавания личности по отпечаткам пальцев 22. Применение искусственных нейронных сетей для выявления инцидентов информационной безопасности 23. Угрозы информационной безопасности при «оплате в одно касание». 24. Анализ нормативной документации, регламентирующей ответственность за утечку сведений, составляющих государственную тайну 25. Математические модели в информационной безопасности 26. Обзор нормативно-правовой базы в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации 27. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований Cookie: принципы работы и безопасность использования	
ОК-6	**способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия**		
Знать	– суть культурных отношений в обществе, место человека в культурном процессе и жизни общества;	**Перечень теоретических вопросов к зачету:** 1. Структура и состав культурологического знания. 2. Структура современной культурологии: теория культуры,	Б1.Б.06 Культурология и межкультурное

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	– содержание актуальных культурных и общественно значимых проблем современности; – методы и приемы социокультурного анализа проблем современности, основные закономерности культурно-исторического процесса.	история культуры, философия культуры, социология культуры. 3. Культурантропология. 4. Теоретическая и прикладная культурология. 5. Методы культурологического исследования. 6. Понятие культуры и её функции. 7. Культурогенез. 8. Культура, природа и цивилизация. 9. Культура как мир смыслов и знаков. Язык и коды культуры. 10. Формы культуры: мифология, религия, искусство, наука. 11. Культурная картина мира. 12. Морфология культуры: материальная и духовная культуры. 13. Субкультура и контркультура. 14. Массовая и элитарная культура. 15. Функции, ценности и нормы культуры. 16. Типология культуры: дихотомия «Восток – Запад». 17. Общественно-историческая школа (Н.Я. Данилевский, О. Шпенглер, А. Тойнби и др.). 18. Натуралистическая школа (Ф. Ницше, З. Фрейд, К.Г. Юнг, Б.К. Малиновский и др.). 19. Социологическая школа (Т. Элиот, П. Сорокин, А. Вебер, Т. Парсонс и др.). 20. Структурно-символическая школа (Ф. Соссюр, Э. Кассирер, К. Леви-Стросс и др.). 21. Антропологическая школа (Э. Тэйлор, А. Ланг, Дж. Фрейзер, А.Н. Веселовский и др.). 22. Концепция «игровых культур» (Й. Хейзинга, Х. Ортега-и-Гассет, Е. Финки др.). 23. Межкультурные коммуникации. 24. Культура, личность и общество: аккультурация и ассимиляция. 25. Социальные институты культуры. 26. Инкультурация и социализация. 27. Модели культурной универсализации. 28. Место и роль России в диалоге культур и мировой культуре.	взаимодействие

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		29. Национальное своеобразие русской культуры: мессианское сознание. 30. Становление и развитие культуры на Руси в IX – XVIII веках: из культурной изоляции к интеграции с европейской культурой. 31. Роль личности в русской культуре XIX века. 32. Диалог культур в русском искусстве «Серебряного века». 33. Культурная модернизация. 34. Глобальные проблемы современности. 35. Культура в современном мире. **Тест:** **1. Передача от поколения к поколению знания, ритуала, артефактов:** А) естественным процессом развития общества; Б) представлением каждого человека; В) функцией культуры; Г) обязанностью государства. **2. Функцией культуры является:** А) руководство политическими институтами; Б) создание смыслов человеческой деятельности: управление законами природы; Г) развитие производительных сил. **3. Культура определяет:** А) степень развитости общества; Б) ответственность общества перед будущим поколением; В) модели поведения человека в обществе; Г) уровень жизни людей. **4. Культура складывается из:** А) ценностей, норм, средств деятельности, моделей поведения; Б) культурных традиций и новаций; В) творцов и потребителей культуры; Г) музыки, изобразительного и театрального искусства. **5. Культура представляет собой:** А) эталон поведения; Б) проявление творческих сил человека;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		В) правили приличия; Г) эстетический эталон. **6. К основным формам культуры не относится культура** А) элитарная; Б) народная; В) массовая; Г) охотников и собирателей. **7. Часть материальной и духовной культуры, созданная прошлыми поколениями, выдержавшая испытание временем и передающаяся следующим поколением как нечто ценное, называется культурным_____** А) компонентом; Б) универсалиями; В) наследием; Г) ареалом. **8. Разновидностью духовной культуры выступает_____ культура.** А) художественная; Б) этническая; В) политическая; Г) экономическая. **9. Знание индивида о мире, в первую очередь, определяется:** А) социальным положением индивида; Б) средствами массовой информации; В) актуальной культурой общества; Г) природной способностью индивида. **10. Система норм представляет собой:** А) набор запретов, подавляющих волю человека: Б) типическое в поведении человека в разных жизненных ситуациях; В) поучение, направленное на закрепление в поведении человека образцов хорошего тона; Г) кодекс социального поведения, установленный обществом. **11. Культурная норма представляет собой:** А) норму права, закрепленную законодательством;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Б) правило, обязательное для исполнения социальных ролей; В) рефлекс, выработанный обществом; Г) кодекс строителя капитализма. **12. Ценности человека формируются:** А) на основе законов добра и зла; Б) в процессе социализации; В) благодаря научному знанию; Г) вместе с молоком матери. **13. Под ценностями понимается:** А) предмет конкурентной борьбы в обществе, обладание которым позволяют человеку изменить свой социальный статус; Б) жизненный ориентир, побуждающий человека к действию и поступкам определенного рода; В) всё, что дорого стоит, привлекает внимание и является модным; Г) артефакт, демонстрирующий достижения человеческой практики в области искусства. **14. Одним из основоположников теории ценностей, в которой они представлены как феномены культуры, является...** А) Э. Кассисер; Б) З. Фрейд; В) Р. Риккард; Г) К. Ясперс. **15. В основе восточной культуры лежит (-ат)...** А) новации; Б) стремление к прогрессу; В) предпринимательство; Г) традиция. **16. Средствами организации человеческой деятельности, определяющими как она должна строиться, являются...** А) ценности; Б) идеалы; В) правила; Г) регулятив.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		17. Характер ожидаемого поведения человека, находящегося в заданной социальной позиции (руководитель, покупатель, отец и пр.) определяют нормы... А) ролевые; Б) индивидуальные; В) групповые; Г) общекультурные. **18. К числу финальных ценностей не относится (-ятся)...** А) свобода; Б) деньги; В) счастье; Г) любовь. **19. Текстом культуры является:** А) Интернет-форум; Б) выступление оратора на тему культуры; В) картина мира, свойственная данной культуры; Г) любой опубликованный в печати текст. **20. Символ позволяет:** А) получить общественное признание; Б) повысить эффективность; В) понять достоинства своей культуры; Г) отличить своих от чужих.	
Уметь	– анализировать и оценивать социокультурную ситуацию; – объективно оценивать многообразные культурные процессы и явления; – планировать и осуществлять свою деятельность с позиций сотрудничества, с учетом результатов анализа культурной информации.	**Практические задания**: 1. Приведите примеры процессов ассимиляции и диверсификации. 2. Каково влияние субкультур на развитие культуры? Приведите примеры изменения норм поведения в связи с доступностью и тиражированием различных субкультур. 3. Определите, кому принадлежат следующие высказывания: • «... Каждой великой культуре присущ тайный язык мирочувствования, вполне понятный лишь тому, чья душа вполне принадлежит этой культуре»; • «Начала цивилизации одного культурно-исторического типа не передаются народам другого типа. Каждый тип	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		вырабатывает ее для себя при большем или меньшем влиянии чуждых, ему предшествовавших или современных цивилизаций»; • «Таким образом, Дьявол обречен на проигрыш не потому, что он сотворен Богом, а потому, что он просчитался. Он играл руками Божьими, испытывая злобную удовлетворенность от вмешательства божественных рук. Зная, что Господь не отвергнет или не сможет отвергнуть предложенного пари. Дьявол не ведает, что Бог молча и терпеливо ждет, что предложение будет сделано. Получив возможность уничтожить одного из избранников Бога, Дьявол в своем ликовании не замечает, что он тем самым дает Богу возможность совершить акт нового творения. И таким образом божественная цель достигается с помощью Дьявола, но без его ведома»; • «У каждой культуры своя собственная цивилизация»; • «Цивилизация есть неизбежная судьба культуры. Будущий Запад не есть безграничное движение вперед и вверх, по линии наших идеалов... Современность есть фаза цивилизации, а не культуры. В связи с этим отпадает ряд жизненных содержаний как невозможных... Как только цель достигнута и... вся полнота внутренних возможностей завершена и осуществлена вовне, культура внезапно коченеет, она отмирает, ее кровь свертывается, силы надламываются — она становится цивилизацией. И она, огромное засохшее дерево в первобытном лесу, еще многие столетия может топорщить свои гнилые сучья»; • «Неминуемость – и закономерное наступление, чередование этих стадий – делает периоды развития всех культур абсолютно тождественными, длительность фаз и срок существования самой культуры – отмеренными, нерушимыми»; • «Ход развития культурно-исторических типов всего ближе уподобляется тем многолетним одноплодным растениям, у которых период роста бывает неопределенно продолжителен, но период цветения и плодоношения – относительно короток и истощает раз и навсегда их жизненную силу»; • «Ни овладение чужой новейшей технологией, ни ревностное сохранение традиционного образа жизни не может быть полным и окончательным Ответом на Вызов чуждой цивилизации». 4. Предшественник Н.Я. Данилевского немецкий профессор	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Г. Рюккерт впервые высказал мысль о замкнутых на себя исторических образованиях в работе «Учебник по мировой истории в органическом изложении» (1857). Вдумайтесь в название его работы и сформулируйте, исследования в области какой сферы науки повлияли на позиции обоих мыслителей. 5. Сопоставьте точки зрения О. Шпенглера и Н.Я. Данилевского по вопросу о стадиях развития культуры и их судьбах. Сформулируйте, что общего в их концепциях культуры, что различно. 6. Прочитайте цитату и сформулируйте, какую роль в современной культуре отводит О. Шпенглер крестьянству: «Крестьянство, связанное корнями своими с самой почвой, живущее вне стен больших городов, которые отныне – скептические, практические, искусственные – одни являются представителями цивилизации, это крестьянство теперь уже не идет в счет. «Народом» теперь считается городское население, неорганическая масса, нечто текучее. Крестьянин отнюдь не демократ – ведь это понятие также есть часть механического городского существования – следовательно, крестьянином пренебрегают, осмеивают, презирают и ненавидят его. После исчезновения старых сословий, дворянства и духовенства он является единственным органическим человеком, единственным сохранившимся пережитком культуры».	
Владеть	– навыками коммуникаций в профессиональной сфере, критики и самокритики, терпимостью; – навыками культурного сотрудничества, ведения переговоров и разрешения конфликтов; – навыками толерантного восприятия социальных и культурных различий.	**Блок творческих заданий для выявления уровня креативного показателя личности:** 1. Обсудите следующие темы: • Какую роль в современном мире играет процесс аккультурации? • Какой тип общественного устройства делает человека более счастливым? • Каково соотношение массовой и элитарной культуры в современном обществе? Сформулируйте свое мнение по вопросу о том, является ли массовая культура явлением положительным или негативным. • Согласны ли вы с тем, что кризис идентичности, идущий в обществах, переживающих системную деформацию, порождает национализм и экстремизм?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		• Верно ли убеждение некоторых культурологов в том, что религия является основанием любой культуры? • Можно согласиться (не согласиться) с мнением Л. Мамфорда, что в современном обществе гуманизм и социальная справедливость принесены в жертву техническому прогрессу; прогресс стал божеством, наука и техника – религией, ученые – сословием новых жрецов. • Как вы относитесь к выражению: «Хочешь овладеть миром – придумай ему религию»? • Современный человек должен быть похож на человека эпохи Возрождения – сложная личность, творец себя и культуры. • Я считаю (не считаю), что возможно достижение коммунизма на Земле. • «Золотое правило нравственности» – от Канта и до наших дней. • Я разделяю (не разделяю) мнение О. Шпенглера о том, что если культура – это «живое тело души», то цивилизация – ее мумия. • Как я понимаю афоризм А. Тойнби: «Самое оживленное движение часто наблюдается в тупиках истории». • Правы ли были О. Шпенглер и Н.Я. Данилевский, пророча гибель западной культуры? • Можно ли заимствовать чужое без ущерба собственному культурному наследию и стоит ли оставаться на позициях традиционализма, рискуя тем самым оказаться в изоляции? • Человеческими поступками в большей мере движут его сознательные стремления, а не подсознательные влечения (или наоборот). • Взгляд на развитие русского народа с точки зрения теории пассионарности Л.Н. Гумилева. • Современная культура теряет (или увеличивает) игровой элемент в жизни человека. • Роль психоанализа в современной культуре. • Нет и не может быть единой общечеловеческой цивилизации. • Совершенную типологию культуры создать невозможно. • Определяющим для поведения человека является тип его	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		ментальности. 2. Выскажите свое мнение по поводу того, насколько востребованы идеи Ф. Ницше или К. Маркса в современном мире. 3. Согласны ли вы с мнением 3. Фрейда о целях человеческих стремлений, о невозможности достижения счастья? Напишите рассуждение на данную тему. 4. Назовите несколько произведений современной литературы или кинофильмов, в которых используется психоаналитическая теория Фрейда; проанализируйте одно из них, с точки зрения теории психоанализа.	
Знать	принципы и алгоритм принятия решений в нестандартных ситуациях, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия	1. Команда как особый вид малой группы. Типы команд. 2. Основные характеристики коллектива как разновидности малой группы. 3. Лидерство в команде. 4. Этапы командообразования. 5. Принципы командной работы. 6. Категории команд в зависимости от цели формирования. 7. Пути командообразования. 8. Понятие «роль». Виды и функции ролей, выполняемых участниками команды. 9. Ролевая модель функциональной команды Р. Белбина. Ее использование в практике командообразования. 10. Стихийное и целенаправленное формирование команды. 11. Управление взаимоотношениями в команде 12. Определение общения. Функции общения. 13. Проблемы, барьеры, ошибки в общении. 14. Отражение проблемы общения в теоретических концепциях. 15. Источники распознавания состояний партнера. 16. Интерпретация невербального поведения партнера. 17. Гендерные особенности в деловом общении. 18. Инструменты управления командными взаимоотношениями. 19. Работа с конфликтами в команде. 20. Трудности работы в команде. 21. Тренинг командообразования: содержание и особенности	Б1.Б.07 Технология командообразования и саморазвития

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		проведения. 22. Виды тренингов командообразования и особенности их применения. 23. Тим-билдинг как способ формирования команды. 24. Веревочный курс как способ формирования команды.	
Уметь	находить организационно- управленческие решения в нестандартных ситуациях.	Отрабатывается в больших тренинговых играх «Катастрофа на воздушном шаре», «Утро на даче» и т.п.	
Владеть	умением находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность.	- Отрабатывается в «Тренинге принятия управленческих решений», деловых играх «Теремок», «Самолеты» и т.п. - Представить одно или несколько командных дел (зависит от трудоемкости) любой направленности: профессиональной, учебной, научно-исследовательской, общественно-полезной, культурной, благотворительной, спортивной и др. Это могут быть: конкурсы, флешмобы, акции, выступления, соревнования, субботники, конференции и др. Командное дело может быть представлено в виде фото- или видеопрезентации. Требования: -продолжительность не более 10 мин.; -участие всех членов команды (обязательно); -форма подачи – свободная; -понятная и интересная форма представления материала.	
Знать	-принципы функционирования профессионального коллектива, понимать роль корпоративных норм и стандартов -принципы и алгоритм принятия решений в нестандартных ситуациях, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия -о социальных, этнических, конфессиональных и культурных особенностях представителей тех или иных социальных общностей	**Примерное индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;	Б2.Б.04(Пд) Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	-работать в коллективе, эффективно выполнять задачи профессиональной деятельности -находить организационно - управленческие решения в нестандартных ситуациях -работая в коллективе, учитывать социальные, этнические, конфессиональные, культурные особенности представителей различных социальных общностей в процессе профессионального взаимодействия в коллективе, толерантно воспринимать эти различия	– изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии?	
Владеть	-приемами взаимодействия с сотрудниками, выполняющими различные профессиональные задачи и обязанности -навыками находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность -способами и приемами предотвращения возможных конфликтных ситуаций в процессе профессиональной деятельности		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. 44) Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ОК-7 способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности			
Знать	- лексический запас должен составить не менее 3000 лексических единиц с учетом вузовского минимума и потенциального словаря, включая термины профилирующей специальности; - определенные приемы, позволяющие совершать познавательную и коммуникативную деятельность; - структурные типы простого предложения,	***Соотнесите английские слова и выражения с их русскими эквивалентами по теме «О себе»:*** A first-year student Хорошо с A Bachelor degree Первокур Well-educated Степень б To run the household Обязанно Duties about the house Вести дом	Б1.Б.02Иностранный язык

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	грамматические формы и конструкции; порядок слов простого предложения; - виды письменных и устных высказываний в различных коммуникативных ситуациях; - разговорные формулы этикета профессионального общения, приемы структурирования научного дискурса.	***Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Мои планы на будущее»*** An area of specialization Дальнейш Further development Способно Abilities and skills Аспирант A high degree of proficiency Область с Postgraduate studies Высокий ***Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Значение иностранного языка в карьере будущего специалиста»*** Accepted language Хорошо в Have a strong hold of English Написани Spelling Непонима Miscommunication Уверенно зыке To be a confident speaker Принятый ***Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Студенческая жизнь»*** Independence Выбирать To do a course Расписан Timetable Независи To take time out from study Сделать п To hang out with your friends Изучать к ***Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Географическое положение и политическая система страны изучаемого языка»*** Constitutional monarchy Корона County ВВП Island Конституц Gross national product Остров Crown Графство	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Культура и традиции страны изучаемого языка» Originate — Происход Annual celebration — Ежегодно Religious significance — Религиоз Official days off — Фейервер Fireworks — Официал ***Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Крупные города страны изучаемого языка»*** To be situated — Столица Capital — Быть расп Date back to — Знаменит Famous for — Датирова Bathing resort — Морской ***Исправьте грамматические ошибки по теме «Порядок слов в простом предложении»*** 1) We get usually up at 7 o'clock. 2 When you do your home assignment? 3) Where you were yesterday? ***Исправьте грамматические ошибки по теме «Числительное»*** 1) My birthday is on the twenty-one of September. 2) I am thirty (13) years old. 3) It is 5th of December. ***Исправьте грамматические ошибки по теме «Местоимение»*** 1)Peter is ill. Can you visit her? 2) The text is difficult. Do you understand all? 3) I haven't called somebody.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Исправьте грамматические ошибки по теме «Существительное» 1) What are the news? 2) Three man came into the room and sat in the armchairs. 3) In evening we usually watch TV. ***Исправьте грамматические ошибки по теме «Прилагательное и наречие»*** 1) Everest ist the most tallest mountain in the world. 2) The results of the experiment turned out to be much best. 3) I think this song is worst than the previous one. ***Выберите правильный ответ на вопросы лингвострановедческого характера «Высшее образование в стране изучаемого языка»*** 1. What's the main difference between a college and a university in the USA? Colleges are smaller Colleges offer only undergraduate degrees Colleges are smaller and they offer only undergraduate degrees 2. What's the difference between a state (public university) and a private university? State universities are funded by the government State universities are usually larger and admit a wider range of students State universities are funded by the government and admit a wider range of students Who funds private institutions of higher education in the USA? US government They are funded from tuition fees, research grants and gifts.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	- понимать аутентичную нормативную монологическую и диалогическую речь носителей иностранного языка; - работать с оригинальной литературой научного характера, сопоставлять и определять/ выбирать пути и способы научного исследования (изучение статей, монографий, рефератов, трактатов, диссертаций); - применять полученные знания для преодоления трудностей при переводе с учетом вида перевода, его целей и условий осуществления.	Прочитайте текст и определите, является высказывание истинным или ложным. My Plans for the Future I am a first-year student now and I have chosen metallurgy as an area of specialization. I am sure it is a very demanding job. That is why I am looking now for opportunities for further devel-opment of my abilities and knowledge in the chosen field. For me, choosing a career is not only a matter of future prestige and wealth. In my opinion, a job should be interesting and socially important. To my mind, people should find satisfaction in their job. Money is naturally very important too. I am rather ambitious. I like to win competitions and be the best. I'd like to become a good special-ist. I am sure the most important qualities of a good specialist are to be hard-working, to speak for-eign languages, to be scientifically-minded, to be energetic, to study for extra qualifications in free time, to be sociable. I think I am good at mathematics and physics. It were my favourite subjects at school and I am sure it is one of the most important subjects at the University. I would like to be a monitor (the leader of the student Government at the Department). To my mind it is a good opportunity to develop my organizational and interpersonal skills and get a solid back-ground. I am willing to be actively engaged in research and scientific discussions covering the problems of steel making technology improvement. I would like to take part in the student scientific confer-ences. My dream is to be a postgraduate student. My goal is to achieve a high degree of proficiency. I hope I'll get my Bachelor's degree in five years, and then I am planning to complete my master's degree. And I'd like to begin my PhD program. Postgraduate study at the university offers us the opportunity to study the subject of our first de-gree at an advanced level, or develop new skills and knowledge. The University offers us the oppor-tunity to enhance our career prospects by developing knowledge and skills relevant to our chosen career 1) The carrier choice is not socially important, but depends on your abilities. 2) The most important qualities of a good specialist are to be	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		industrious, to speak several for-eign languages, etc. 3) To develop the organizational and interpersonal skills and get a solid background one can become a monitor. Прочитайте текст и определите, является высказывание истинным или ложным. Colleges, universities, and institutes: the distinctions Degree-granting institutions in the United States can be called colleges, institutes or universities. As a general rule, colleges tend to be smaller and usually offer only undergraduate degrees, while a university also offers graduate degrees. The words “school”, “college”, and “university” are often used interchangeably. An institute usually specializes in degree programs in a group of closely related subject areas, so you will also come across degree programs offered at institutes of technology, institutes of fashion, institutes of art and design, and so on. Within each college or university you will find schools, such as the school of arts and sciences or the school of business. Each school is responsible for the degree programs offered by the college or university in that area of study. Technical and vocational colleges. These institutions specialize in preparing students for entry into, or promotion within, the world of work. They offer certificate and other short-term programs that train students in the theory behind a specific vocation or technology, as well as how to work with the technology. Programs usually last two years or less. There are several thousand technical and vocational colleges across the United States, and they may be private or public institutions. State universities are founded and subsidized by U.S. state governments (for example, California, Michigan or Texas) to provide low-cost education to residents of that state. They may also be called public universities to distinguish them from private institutions. Some include the words “state university” in their title or include a regional element such as “eastern” or “northern”. State universities tend to be very large, within enrollments of 20, 000 or more students, and generally admit a wider range of students than private universities. State university tuition costs are generally lower than those of private universities. Also, in-state residents (those who live and pay taxes in that particular state) pay much lower tuition than out-of-state residents. International students, as well	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		as those from other states, are considered out-of-state residents and therefore do not benefit from reduced tuition at state institutions. In addition, international students may have to fulfill higher admission requirements than in-state residents. Private universities are funded by a combination of endowments, tuition fees, research grants, and gifts from their alumni. Tuition fees tend to be higher at private universities than at state universities, but there is no destinction made between state and non-state residents. Colleges with a religious affiliation and single-sex colleges are private. In general, private universities have enrollments of fewer than 20,000 students, and private colleges may have 2,000 or fewer students on their campuses. 1) State university tuition costs are generally lower than those of private universities. 2) Within each college or university you will find schools. 3) Technical and vocational colleges offer certificate and other short-term programs that train students in the theory behind a specific vocation or technology, as well as in how to work with the technology. Дополните диалог, используя предложенные ниже реплики Jane: Hello, Maria! You look great today! Maria: _____It's very warm today, isn't it? So I have decided to put on my new dress. Jane: Yes, the weather is lovely, as well as your new dress. But have you heard about the rain this afternoon? Maria: _____But that is okey. I have an umbrella. Jane: Oh, you are lucky, but I have no umbrella. I need to go back home to take it. Maria: Yes, be quick. Look, the sky is already full of clouds. Jane: I run. Bye, _____ Maria: Bye! Yes, I've heard about that. Hi,! Thank you! see you later. Дополните диалог, используя предложенные ниже реплики A: _____ B: Yes, I'll have the fillet steak. A: _____	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		B: Rare, please. And I'd like a glass of red wine, and some mineral water. A: Still or sparkling? B: Sparkling. A: _____ Are you ready to order? How would you like your steak? Fine. Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «О себе» to be a first-year student, to consist of, to live, my hobby is, I prefer, my favourite subjects, to spend time, at the university I, when I have free time, usually I Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Мои планы на будущее» My future specialty, department, carrier plans, to make a carrier, to do courses, to pick up a foreign language, a very demanding job, opportunities for further development of my abilities and knowledge, to take part in the student scientific conferences Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Значение иностранного языка в карьере будущего специалиста» to improve your career prospects, many benefits, give a competitive edge over other applicants, have the option to work abroad, miscommunication, feel more at ease when speaking with fellow employees, management, or clients. Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Студенческая жизнь» the first step to independence, to achieve your study goals, to plan a timetable, to do a course work, to take time out from study, tutorials and labs, to hang out with friends, to attend lectures and classes Прочитайте текст, переведите и выпишете предложения, передающие его основную идею. Student Life	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Becoming a student is often the first step to independence, particularly if you are moving away from home. You'll get to meet new people and there are lots of chances to socialise. However, you may find yourself struggling to achieve your study goals. Student life is different for everyone. How can I prepare for student life? Talk to people who have done the course or degree you're doing. They may be able to give you tips and advice about the workload, and make suggestions for how you can prepare. If you're moving to a different place, try to arrive a few days before you start your course. That way you'll have time to get familiar with the town/city layout, and learn your way around. Work out how you will get around. If there is no suitable public transport in the city, can you get a bike or car? Do you need to get a driver's licence? If you're moving into a flat, ask your parents if you can take any furniture with you (eg bed, dresser, desk, chair, sofa). Decide on your accommodation early on. If you want to live on campus, you'll need to get in early. How do you set realistic goals and plan timetables at university? It's tempting to try to achieve too much in your first year of study, which is common with new stu-dents. This can leave you feeling overwhelmed and unmotivated, because you may not leave enough time to do course work or take time out from study. Remember to leave time for things such as pre-paring for lectures, part-time work and spending time with friends. Why should you go to lectures, classes, tutorials or labs? Classes or lectures can be less structured than at school. You may have many opportunities to do other things instead of going to class. For example, it may seem more appealing to hang out with your friends. However, you need to be aware that when exam time comes you may have to spend a lot of time in the library looking up what was taught during the lectures you missed. You may not even be sure what’s asked of you for the exam. Try to take a sensible approach to attending lectures and classes – they are worth it.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		1) Is becoming a student the first step to independence? Why? 2) Why is it useful to talk to people who have done the course or degree you're doing? 3) Why should you arrive in the city before you start your course?	
Владеть	- подготовленной, а также неподготовленной монологической и диалогической речью в пределах изученного языкового материала и в соответствии с избранной специальностью; - терминологией по специальности, а также дискурсивными, лексико-фразеологическими, грамматическими и стилистическими трудностями в текстах, относящихся к сфере основной профессиональной деятельности; - правильно оперировать языковыми средствами английского языка в ситуациях устного общения; - всеми видами чтения (изучающее, ознакомительное, поисковое и просмотровое); - письмом в пределах изученного материала (250-300 слов).	Заполните пропуски. Выберите один вариант ответа. 1. Shame on you Nick! You never do any work! You are so ……. ! a) hard-working b) lazy c) shy d) self-confident 2. I don't like cooking. I prefer to buy ready-made food in the nearest …….. . a) cookery b) newsagent c) butcher's d) baker's 3. The Fenders don't go in for sports. But every morning Mr. Fender and his son James exercise with the ……. . a) puck b) dumbbells c) ski slope d) raft 4. When I travel I usually book tickets ……. . a) early b) fast c) in advance d) slow 5. What a pity! Julia broke her leg and now she is …… . a) on leave b) unemployed c) dismissed	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		d) on sick leave 6. The level of ……. is really very high in this city. a) unemployless b) unemployful c) unemployment d) unemployed 7. Nancy's hair …….. long and wavy. a) are b) is c) am d) were 8. The Nile is …….. river in Africa. a) the longest b) longer c) long d) longest 9. Where …….. your father …….. ? a) do, works b) does, works c) do, work d) does, work 10. Look! Mike and Fred …… football in the yard. a) are playing b) play c) playing d) is playing 11. Max and Roberta …….. yesterday. a) don't go shopping b) didn't went shopping c) didn't go shopping d) doesn't went shopping	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		12. I …… my basketball team yesterday at 5 o'clock. a) supported b) support c) was supporting d) am supporting 13. In two weeks Ann …… . a) will get married b) is getting married c) got married d) gets married 14. When the match ……over, I ……. to my friend Ali. a) will be, will go b) is, go c) will be, go d) is, will go 15. In some years I ……. to travel around the world. a) can b) should c) will be able d) must 16. How …….. time do you need to repair my car? – Two hours. a) much b) many c) few d) a little Выберите реплику, наиболее соответствующую ситуации общения 17. Helen: Hi, meet my friend Andrew! Mary: …… . a) Hello, Andrew! Pleased to meet you!	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		b) Very well! c) And what is that? d) I don't want! I'm very busy! 18. Helga: …….. . Barbara: Oh, thank you very much, Helga! It's so pleasant! a) Hello! What's the matter with you, Barbara? b) You look wonderful! Your dress is very beautiful! c) You should change your shoes, they don't match this suit. d) It's not a good idea to wear this handbag with this hat. 19. Passer-by 1: …… . Passer-by 2: Go straight down to the traffic lights, then turn left. a) How do you get to your office? b) I'm lost! Help me! c) Does this bus go to the centre? d) Excuse me! Do you know where the nearest metro station is, please? Заполните пропуск. Выберите один вариант ответа. 20. What is the capital of the UK? a) Bristol b) Cardiff c) London d) Washington 21. The UK is ……. . a) absolute monarchy b) parliamentary monarchy c) federal republic d) democracy republic 22. What is the Tower of London nowadays? a) a prison b) a queen's residence c) a museum d) a university	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		23. What river flows through London? a) the Thames b) the Avon c) the Severn d) the Trent 24. What is the name of the English Queen? a) Elizabeth II b) Victoria c) Elizabeth I d) Mary I 25. Прочитайте текст. Выберите один вариант ответа. Определите, является ли утверждение: The fashion industry is not based on some youth preferences, there is no kind of business in produc-ing special clothes and accessories for teens a) истинным b) ложным c) в тексте нет информации Youth Problems 1. What are the main youth problems? Everyone knows and at the same time no one knows. As sand through fingers - youth problems are always changing. Thirty years ago Johnny Rotten sang " Too many problems oh why am I here, I don't need to be me 'cos you're all too clear, well and I can see there's something wrong with you but what do you expect me to do? Problems, problems, the problem is YOU!" The idea of that punk styled song is simple clear. All our failures depend on us. Imagine your life without money, can you do that? No fancy clothes, no fashionable clubs, no entertainments, no troubles. Americans say "No mass - no fuss" in such case. Don't you think teen-agers depend on money greatly? They are obsessed on their appearance, they need to be clothed fashionable and in modern style. Some of them, who are lacking money prefer to wear jeans and plain clothes, this is their way out. The fashion industry is based on some youth preferences; there is a kind of	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		business in producing special clothes and accessories for teens, Kira Plastinina, for exam-ple. Young try to do their best in getting labeled and fancy stuff; they are really crazy about such things. External life may force out their spiritual life, and that are dangerous circumstances. 2. Another youth problem is mutual understanding in their families. It's hardly believable sit-uation when a teen feels comfortable with his relatives, even in a tight-bonded family. Parents want them to be serious, to study hard and to think about their future, but rare senior could understand teen's tormented soul. In past life grown-ups were the same teens, but they don't remember that state. Our parents were bits, hippies, and they struggled for their personal independence, just like us! But things change, tastes grow differ and differ, and we can't understand each other, we lose the connection. If teens could obey their olds implicitly, that'll be very convenient for the last ones. Lib-eral seniors are absolute rarities, so teens have to look for common language with their parents in any case. We all know the moral disaster of being misunderstood. Try harder - and you'll make friends with your relatives. Sometimes young fall apart with their families and begin to take drugs, alcohol. That is not the reaction on the emotional environment, that is the reflection of tortured inside world. Drug addicts are spread all over the world, but in their majority they are young people. Junkies are used to hang on with the same disappointed people, sometimes they had to steal money or jewelry from their houses, to get the drug. It is obviously damaged way. Normally up-brought youth avoid junkies, and addicts could not find the way-out of their abusement. 3. There is the proverb which says “A word can kill, a word can save”; everything is up to you and your attitude towards people. I don't believe we can't rescue people surrounding us. There are special rehabilitation centers for junkies, anonymous help is offered for people. So don't lose your chance to be safe and sound, to live long and unforgettable lives, and one day you'll be thanked for your compassion paid to drowned people. “Life is very short, there is no time for fussing and fighting, my friend” (Paul Mc Cartney) (From http://www.native-english.ru) 26. Прочитайте текст. Выберите один вариант ответа. Определите, является ли утверждение: Special rehabilitation centers for junkies are rather expensive and not very popular among young people	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		a) истинным b) ложным c) в тексте нет информации 27. Прочитайте текст. Выберите один вариант ответа. Определите, является ли утверждение: Taking drugs or alcohol is not the reaction on the emotional environment, that is the reflection of tor-tured inside world a) истинным b) ложным c) в тексте нет информации 28. Укажите, какой части текста (1, 2, 3) соответствует следующая информация: Misunder-standing between teens and adults is common in many families, it's hardly believable situation when a teen feels comfortable with his relatives, even in a tight-bonded family a) 1 b) 2 c) 3 29. Укажите, какой части текста (1, 2, 3) соответствует следующая информация: Can you im-agine your life without money? Teenagers depend on money greatly a) 1 b) 2 c) 3 30. Ответьте на вопрос: What problems (according to the text) are actual for modern teenagers? a) violence and cruelty b) unemployment and lack of respect c) misunderstanding of grown-ups and drug addiction d) lack of money and good friends 31. Ответьте на вопрос: What are teenagers really crazy about? a) higher education and travelling b) night clubs and parties	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		c) love and relationships with opposite sex d) labeled and fancy stuff 32. Определите основную идею текста: a) Fathers and Sons b) drug addiction as the main world problem c) all our failures depend on us d) teenagers and their problems 33. Расположите части нижепредставленного письма в правильном порядке. Выберите варианты согласно указанной последовательности. 1. January 28th 2. Hope to hear from you soon 3. Flat 14, 8 Jefferson Street Nashville NSH9 001 4. Yours, Alex Duck 5. Dear Melanie 6. I don't like to write long and boring letters so I stop here, but I like to communicate with people about interesting things. I hope we'll be able to become good friends. 7. I've seen your ad and liked it very much. So I decided to write you. My name is Alex. I'm 22. I like travelling very much. My hobby is basketball. Besides, I'm fond of reading. My favourite writer is Charles Dickens. a) 5, 7, 4, 3, 1, 6, 2 b) 3, 1, 5, 7, 6, 2, 4 c) 1, 3, 5, 7, 6, 4, 2 d) 1, 3, 5, 6, 7, 2, 4	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		34. Определите, к какому виду письма относится выше представленный текст: a) Memo b) CV c) personal letter d) inquiry letter	
Знать	– структуру и содержание межкультурного взаимодействия; – суть ценностно-смысловых отношений в межличностной коммуникации; – материальную и духовную роль культуры в развитии современного общества; – движущие силы и закономерности культурного процесса, многовариантность культурного процесса.	**Перечень теоретических вопросов к зачету:** 1. Структура и состав культурологического знания. 2. Структура современной культурологии: теория культуры, история культуры, философия культуры, социология культуры. 3. Культурантропология. 4. Теоретическая и прикладная культурология. 5. Методы культурологического исследования. 6. Понятие культуры и её функции. 7. Культурогенез. 8. Культура, природа и цивилизация. 9. Культура как мир смыслов и знаков. Язык и коды культуры. 10. Формы культуры: мифология, религия, искусство, наука. 11. Культурная картина мира. 12. Морфология культуры: материальная и духовная культуры. 13. Субкультура и контркультура. 14. Массовая и элитарная культура. 15. Функции, ценности и нормы культуры. 16. Типология культуры: дихотомия «Восток – Запад». 17. Общественно-историческая школа (Н.Я. Данилевский, О. Шпенглер, А. Тойнби и др.). 18. Натуралистическая школа (Ф. Ницше, З. Фрейд, К.Г. Юнг, Б.К. Малиновский и др.). 19. Социологическая школа (Т. Элиот, П. Сорокин, А. Вебер, Т. Парсонс и др.). 20. Структурно-символическая школа (Ф. Соссюр, Э. Кассирер, К. Леви-Стросс и др.). 21. Антропологическая школа (Э. Тэйлор, А. Ланг, Дж. Фрейзер, А.Н. Веселовский и др.).	Б1.Б.06Культурология и межкультурное взаимодействие

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		22. Концепция «игровых культур» (Й. Хейзинга, Х. Ортега-и-Гассет, Е. Финки др.). 23. Межкультурные коммуникации. 24. Культура, личность и общество: аккультурация и ассимиляция. 25. Социальные институты культуры. 26. Инкультурация и социализация. 27. Модели культурной универсализации. 28. Место и роль России в диалоге культур и мировой культуре. 29. Национальное своеобразие русской культуры: мессианское сознание. 30. Становление и развитие культуры на Руси в IX – XVIII веках: из культурной изоляции к интеграции с европейской культурой. 31. Роль личности в русской культуре XIX века. 32. Диалог культур в русском искусстве «Серебряного века». 33. Культурная модернизация. 34. Глобальные проблемы современности. 35. Культура в современном мире. **Тест:** **1. Культурология как система знаний о культуре изучает:** А) образ жизни людей; Б) культурный уровень людей; В) шедевры мировой культуры; Г) символ значения артефактов. **2. При семиотическом подходе к изучению культуры особое внимание обращается на:** А) движущие силы культуры; Б) нормы и санкции; В) символы и знаки культуры; Г) функции культуры в обществе. **3. Предметом изучения культурологии являются:** А) теории развития общества, культурные эпохи; Б) взаимосвязи между различными историческими	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		периодами; В) модели культуры, ценности, нормы, человеческое поведение; Г) мировая художественная культура, манеры поведения человека в обществе. **4. Использование исторического метода исследования культуры предполагает особое внимание к изучению:** А) роли выдающихся личностей в истории культуры; Б) генезиса, развития п угасания культурных явлений во времени; В) возможности реставрации памятников культуры; Г) античной культуры. **5. Метод исследования, принятый функциональной школой, – это:** А) анализ продуктов жизнедеятельности; Б) ведение наблюдения за образом жизни сообщества; В) ведение эксперимента над исследуемыми группами; Г) размышление над объектами мира природы и мира человека. **6. К предметному полю культурологии не относится...** А) культуроведение; Б) психология культуры; В) социология; Г) богословие культуры. **7. Получение ценностных суждений является главной целью_____метода исследования культуры.** А) структурно-функционального; Б) исторического; В) философского; Г) компаративного. **8. В зависимости от целей культурологического познания в предметной области культурологии выделяют теоретический, фундаментальный и _____ уровни.** А) компаративный; Б) эмпирический; В) диахронический; Г) прикладной.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		9. Культуру общества и его субъектов изучает: А) социология; Б) культурная антропология; В) культурология; Г) философия культуры. **10. В соответствии с задачами культурологической науки все её знания подразделяются на два вида – фундаментальные и_____знания.** А) прикладные; Б) юридические; В) технические; Г) педагогические. **11. Культурологическое знание востребовано:** А) экологией; Б) теорией систем; В) географией; Г) политологией. **12. Изучение нравов и обычаев народов необходимо для:** А) обеспечение межкультурной коммуникации; Б) освоения новых территорий; В) просвещения отсталых народов; Г) повышения собственного культурного уровня. **13. Культурология опирается на достижения_____наук.** А) исторических; Б) математических; В) биологических; Г) политических. **14. Статус культурологии современной системе наук определяется:** А) использованием её методов и выводов в других отраслях гуманитарного знания; Б) включением курса «Культурологи» в образовательный процесс; В) продолжительной историей; Г) нравственным и эстетическим содержанием культурологии.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		15. Взаимосвязь культурологии и социологии проявляется в: А) общей генеалогии; Б) сходных методах исследования; В) тождестве научных выводов; Г) единой терминологии. **16. К наукам, с которыми контактирует культурология, углубляя свои представления о культуре, не относится...** А) логика Б) философия В) социология Г) этнография. **17. К наукам об общих аспектах человеческой деятельности, без относительно к её предмету, относятся_____науки.** А) экономические; Б) искусствоведческие; В) технические; Г) культурологические. **18. Главное отличие культурной антропологии от культурологии заключается в том, что культурная антропология носит по преимуществу_____характер.** А) практический; Б) обобщающий; В) ретроспективный; Г) понимающий. **19. Прикладная культурология изучает:** А) эволюцию теоретической концепции; Б) закономерности культурного процесса; В) народное творчество; Г) повседневная практика людей. **20. Предметом исторической культурологии является:** А) происхождения человеческого разума; Б) структура современной культурологии; В) перспективы культурного развития; Г) эволюция культурных форм.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	– общаться с представителями других культур, используя приемы межкультурного взаимодействия; – решать задачи межличностного и межкультурного взаимодействия; – анализировать проблемы культурных процессов; – применять понятийно-категориальный аппарат, основные законы культурологии как гуманитарной науки в профессиональной деятельности; – анализировать и оценивать культурные процессы и явления, планировать и осуществлять свою деятельность с учетом результатов этого анализа.	**Практические задания:** 1. Прочитайте фрагмент из работы Р. Итса и сформулируйте свое отношение к его точке зрения. Ответьте на вопросы. Жизнь наших далеких предков протекала в экстремальных условиях, богатых множеством случайных совпадений, которые воспринимались первобытным сознанием как следствие проявления невидимых и всесильных «чар». Они порождают видимость большой вероятности связи происшедших с человеком несчастий с действиями над его фетишами или реальностью проклятий, заклинаний, колдовства. Если еще добавить сюда сам факт психологического ожидания беды: что-то случилось с твоей чурингой, с твоим фетишем и т. п., то количество совпадений или случайных связей несвязанных причин и следствий увеличится. • Почему на первых этапах развития человеческого общества появляется вера в абсолютную связь фетиша с судьбой человека? • Подкреплялась ли эта связь общественным сознанием первобытной эпохи? • Почему подобные ситуации часто находили свое подтверждение в окружающем реальном мире? • Приведите известные вам примеры: а) магического обряда; б) тотемных представлений; в) анимистических представлений. 2. Рассмотрите основные мировые религии по трем основным моментам: религиозное сознание, культовая деятельность и религиозные организации. Имейте в виду, что они тесно связаны, взаимодействуют и образуют целостную религиозную систему. 3. Опишите какой-либо известный вам опыт межкультурного взаимодействия. Были ли в вашей жизни проблемы с пониманием поведения представителей другой культуры? Можете ли вы их объяснить? Обратите внимание при объяснении, что поведение человека следует рассматривать в рамках его культуры, а не своей, т. е. следует проявлять больше эмпатии, чем симпатии. Симпатия подразумевает, что человек мысленно ставит себя на место другого, следует «золотому правилу нравственности»: «поступай с людьми так, как хотел бы, чтобы	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		поступали с тобой». Но при симпатии используются свои собственные способы интерпретации поведения других людей. При общении же с носителями других культур следует применять эмпатический подход, т. е. представить себя на месте другого человека, принять его мировоззрение, понять его чувства, желания, поступки, исходить из рамок его культуры. Сущность эмпатического подхода отражает «платиновое правило»: «поступай с другими так, как они поступали бы сами с собой». 4. Определите, в какой историко-культурный период были сделаны следующие высказывания (если возможно, назовите автора): • «Как плодородное поле без возделывания не даст урожая, так и душа. Возделывание души – это и есть философия: она выпалывает в душе пороки, приготовляет души к приятию посева и вверяет ей – сеет, так сказать, только те семена, которые, вызрев, приносят обильнейший урожай»; • «Человек – это слабое, беспомощное, достойное жалости и участия существо. Но в своей слабости он обнаруживает огромную силу. Уповая на Веру, он может сказать «да» хаотическому и страшному миру»; • «Человек, забывший об интересах общества, и правитель, забывший об интересах граждан, – не римляне, а варвары»; • «Культура не воспитание меры, гармонии и порядка, а преодоление ограниченности, как культивирование неисчерпаемости, бездонности личности, как ее постоянное духовное совершенствование»; • «Все эти сказанные художества весьма и весьма различны друг от друга; так что если кто исполняет хорошо одно из них и хочет взяться за другие, то почти никому они не удаются так, как то, которое он исполняет хорошо; тогда как я изо всех моих сил старался одинаково орудовать во всех этих художествах; и в своем месте я покажу, что я добился того, о чем я говорю»; • «И тогда через хаос, через абсурдность, через чудовищность жизни, как солнце через тучи, глянет око Божье. Бога, который имеет личность, и личность, отображенную в каждой человеческой личности»; • «Поступай так, чтобы ты всегда относился к человечеству	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		и в своем лице, и в лице всякого другого так же, как к цели, и никогда не относился бы к нему только как к средству»; • «Начала цивилизации одного культурно-исторического типа не передаются народам другого типа. Каждый тип вырабатывает ее для себя при большем или меньшем влиянии чуждых, ему предшествовавших или современных цивилизаций»; • «Мне хотелось бы словом «гуманность» охватить все, что я до сих пор говорил о человеке, о воспитании его благородства, разума, свободы, высоких помыслов и стремлений, сил и здоровья, господства над силами Земли»; • «Все хорошо, что исходит из рук Творца всех вещей. В руках человека все вырождается»; • «Воспитание человеческого рода – это процесс и генетический и органический; процесс генетический – благодаря передаче, традиции, процесс органический – благодаря усвоению и применению переданного. Мы можем как угодно назвать этот генезис человека во втором смысле, мы можем назвать его культурой, т. е. возделыванием почвы, а можем вспомнить образ света и назвать его просвещением, тогда цепь культуры и просвещения протянется до самой земли. Различие между народами просвещенными и непросвещенными – не качественное, а только количественное»; • «...Что такое человек во Вселенной? Небытие в сравнении с бесконечностью, все сушее в сравнении с небытием, среднее между всем и ничем. Он не в силах даже приблизиться к пониманию этих крайностей – конца мироздания и его начала, неприступных, скрытых от людского взора непроницаемой тайной, и равно не может постичь небытие, из которого возник, и бесконечность, в которой растворяется»; • «Причина всех бедствий и несчастий людей, – состоит в невежестве. Преодолеть свое печальное положение, выйти из него люди могут только через просвещение, а рост его неодолим. В умах идет скрытая и непрерывная революция и... с течением времени само невежество себя дискредитирует»; • «Все, что вне меня, – отныне чуждо мне. У меня нет в этом мире ни близких, ни мне подобных, ни братьев. Я на земле, как на чужой планете, куда свалился с той, на которой жил прежде.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Если я и различаю, что вокруг себя, – то лишь скорбные и раздирающие сердце предметы, и на все, что касается и окружает меня, не могу кинуть взгляда без того, чтобы не найти там какого-нибудь повода к презрительному негодованию и удручающей боли»; • «Ход развития культурно-исторических типов всего ближе уподобляется тем многолетним одноплодным растениям, у которых период роста бывает неопределенно продолжителен, но период цветения и плодоношения – относительно короток и истощает раз и навсегда их жизненную силу»; • «Всякая культура (даже материальная) есть культура духа; всякая культура имеет духовную основу – она есть продукт творческой работы духа над природными условиями».	
Владеть	– навыками межкультурного взаимодействия; – критического восприятия культурно значимой информации; – навыками социокультурного анализа современной действительности; – навыками социального взаимодействия, сотрудничества в позиций расовой, национальной, религиозной терпимости.	**Блок творческих заданий для выявления уровня креативного показателя личности:** 1. Проанализируйте существующие определения культуры с точки зрения их отношения к человеку. Является ли культура системой, позволяющей человеку приспособиться к жизни или она враждебна для человека, разрушает его, подавляет его свободу? Предложите собственное понимание культуры. 2. Выдающийся философ XX в. Л. Витгенштейн заявлял: «Пределы моего мира – пределы моего языка». Поразмышляйте вслух на эту тему. 3. Прочитайте любую понравившуюся вам статью, затрагивающую проблемы семиотики, дайте ей оценку, выразив свое согласие или несогласие и обосновав его. Например, можно взять работы Ю.М. Лотмана, посвященные семиотике русского быта и литературы XVIII и XIX вв. 4. Попробуйте разобрать какое-нибудь литературное или кинематографическое произведение с точки зрения семиотики. Согласны ли вы с объяснением Ю.М. Лотмана отношений между Татьяной, Онегиным и Ленским в романе Пушкина «Евгений Онегин»? Эти персонажи не понимали друг друга потому, что они использовали разные культурные знаковые системы. Онегин был ориентирован на английский байронический романтизм с его культом разочарованности в жизни и трагизмом, Ленский – на немецкий романтизм с его восторженностью и ученостью, Татьяна,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		с одной стороны, на английский сентиментализм с его чувствительностью, порядочностью и «хорошими концами», а с другой – на русскую народную культуру (поэтому она из всех трех оказалась наиболее гибкой).	
Знать	– понятие и содержание управленческой деятельности	Сущность и содержание теории управления. Цели и задачи управления. Объект и субъект управления. Система управления. Виды управления. Принципы управления. Эволюция управления в науку управления. Школы управленческой мысли Новая управленческая парадигма. Внутренняя среда организации. Внутренние переменные: структура, цели, задачи, технология, люди. Определение структуры управления. Факторы и принципы формирования структуры. Влияние среды на личность и поведение. Значение и определение внешней среды. Характеристики внешней среды. Сложность, подвижность, неопределенность внешней среды. Среда прямого и косвенного воздействия. Понятие и значение функций управления. Виды функций управления. Эволюция организационных структур. Механизм мотиваций. Содержание структуры мотиваций. Процессуальные теории мотиваций. Типы контроля. Процесс контроля. Система эффективного контроля. Методы управления и их классификация. Экономические методы управления. Организационные методы управления. Социально-психологические методы управления. Процесс управления, его этапы. Основные свойства процесса управления. Взаимосвязь структуры и процесса управления. Сущность и виды коммуникаций. Классификационная схема организационных	Б1.Б.10Основы управленческой деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		коммуникаций. Внешние и внутренние коммуникации. Вертикальные, горизонтальные коммуникации, коммуникации между руководителем и подчиненным, неформальные коммуникации. Процесс коммуникации. Основные этапы коммуникационного процесса.	
Уметь	– анализировать внешнюю и внутреннюю среду организации как объекта управленческой деятельности	Тестовое задание «Модель организации как объекта управления» Тестовое задание «Организационно-правовые формы субъектов экономики» Тестовое задание «Организационные структуры управления»	
Владеть	– основными навыками управленческой деятельности: планирования, организации, мотивации, контроля и коммуникаций	Практическое задание 2 «Типология и развитие организационных структур» Практическое задание 3 «Разработка линейно-функциональной ОСУ»	
Знать	- лексический запас должен составить не менее 3000 лексических единиц с учетом вузовского минимума и потенциального словаря, включая термины профилирующей специальности; - определенные приемы, позволяющие совершать познавательную и коммуникативную деятельность; - структурные типы простого предложения, грамматические формы и конструкции; порядок слов простого предложения; - виды письменных и устных высказываний в различных коммуникативных ситуациях; - разговорные формулы этикета профессионального общения, приемы структурирования научного дискурса.	Оценочные средства для зачета Соотнесите английские слова и выражения с их русскими эквивалентами по теме «О себе»: A first-year student Хорошо образованный A Bachelor degree Первокурсник Well-educated Степень бакалавра To run the household Обязанности по дому Duties about the house Вести домашнее хозяйство Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Мои планы на будущее» An area of specialization Дальнейшее развитие Further development Способности и навыки Abilities and skills Аспирантура A high degree of proficiency Область специализации Postgraduate studies Высокий уровень профессионализма	Б1.В.01 Иностранный язык в профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Значение иностранного языка в карьере будущего специалиста» Accepted language Хорошо владеть английским Have a strong hold of English Написание Spelling Непонимание Miscommunication Уверенно разговаривать на иностранном зыке To be a confident speaker Принятый язык Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Студенческая жизнь» Independence Выбираться куда-либо с друзьями To do a course Расписание Timetable Независимость To take time out from study Сделать перерыв в учебе To hang out with your friends Изучать курс Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Географическое положение и политическая система страны изучаемого языка» Constitutional monarchy Корона County ВВП Island Конституционна монархия Gross national product Остров Crown Графство Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Культура и традиции страны изучаемого языка» Originate Происходить Annual celebration Ежегодное празднование Religious significance Религиозное значение Official days off Фейерверк Fireworks Официальные выходные	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Крупные города страны изучаемого языка» To be situated Столица Capital Быть расположенным Date back to Знаменит ч-л Famous for Датироваться Bathing resort Морской курорт Исправьте грамматические ошибки по теме «Порядок слов в простом предложении» 1) We get usually up at 7 o'clock. 2 When you do your home assignment? 3) Where you were yesterday? Исправьте грамматические ошибки по теме «Числительное» 1) My birthday is on the twenty-one of September. 2) I am thirty (13) years old. 3) It is 5th of December. Исправьте грамматические ошибки по теме «Местоимение» 1)Peter is ill. Can you visit her? 2) The text is difficult. Do you understand all? 3) I haven't called somebody. Исправьте грамматические ошибки по теме «Существительное» 1) What are the news? 2) Three man came into the room and sat in the armchairs. 3) In evening we usually watch TV. Исправьте грамматические ошибки по теме «Прилагательное и наречие»	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		1) Everest ist the most tallest mountain in the world. 2) The results of the experiment turned out to be much best. 3) I think this song is worst than the previous one. Выберите правильный ответ на вопросы лингвострановедческого характера «Высшее образование в стране изучаемого языка» 1. What's the main difference between a college and a university in the USA? a) Colleges are smaller b) Colleges offer only undergraduate degrees c) Colleges are smaller and they offer only undergraduate degrees 2. What's the difference between a state (public university) and a private university? a) State universities are funded by the government b) State universities are usually larger and admit a wider range of students c) State universities are funded by the government and admit a wider range of students 3. Who funds private institutions of higher education in the USA? a) US government b) They are funded from tuition fees, research grants and gifts. Выберите правильный ответ на вопросы по страноведению «Геополитические особенности страны изучаемого языка» 1) How many countries does the United Kingdom consist of? a) 2 b) 3 c) 4 2) What is the state system of the United Kingdom? a) a constitutional monarchy	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		b) a parliamentary republic 3) What is the symbol of the United Kingdom? a) a rose b) a bald eagle c) Britannia Выберите правильный ответ на вопросы лингвострановедческого характера «Культура и традиции страны изучаемого языка» What is the Scottish national costume for men? a) the kilt b) the tuxedo c) the bearskin What is the most famous sport event in Scotland? a) the Highland games b) the Ccommonwealth Games c) the Wimbledon Championship What country is called a land of castles and princes? a) England b) Northern Ireland c) Wales Выберите правильный ответ на вопросы лингвострановедческого характера «Крупные города страны изучаемого языка» What are the best English resorts? a) Bristol and Southampton b) Brighton and Bath c) Leeds and Bradford What is the capital of Scotland? a) Manchester b) Edinburg	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		c) Liverpool What is the most important airport in England? a) Gatwick b) Heathrow c) Stansted	
Уметь	- понимать аутентичную нормативную монологическую и диалогическую речь носителей иностранного языка; - работать с оригинальной литературой научного характера, сопоставлять и определять/ выбирать пути и способы научного исследования (изучение статей, монографий, рефератов, трактатов, диссертаций); - применять полученные знания для преодоления трудностей при переводе с учетом вида перевода, его целей и условий осуществления.	Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «О себе» to be a first-year student, to consist of, to live, my hobby is, I prefer, my favourite subjects, to spend time, at the university I, when I have free time, usually I Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Мои планы на будущее» My future specialty, department, carrier plans, to make a carrier, to do courses, to pick up a foreign language, a very demanding job, opportunities for further development of my abilities and knowledge, to take part in the student scientific conferences Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Значение иностранного языка в карьере будущего специалиста» to improve your career prospects, many benefits, give a competitive edge over other applicants, have the option to work abroad, miscommunication, feel more at ease when speaking with fellow employees, management, or clients. Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Студенческая жизнь» the first step to independence, to achieve your study goals, to plan a timetable, to do a course work, to take time out from study, tutorials and labs, to hang out with friends, to attend lectures and classes	
Владеть	- подготовленной, а также неподготовленной монологической и диалогической речью в пределах изученного языкового материала и в соответствии с избранной специальностью; - терминологией по специальности, а также	**Задание 1.*Расположите следующие слова в алфавитном порядке; переведите их с помощью словаря.*** Physics, wave, charge, particle, ray, hydrogen, discovery, field, development, farm, detector, time, work, law, research, power, phenomenon, importance, achievement, data, velocity, plant, equipment, zero, unit, circumference, movement, establishment, X-ray, et cetera.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	дискурсивными, лексико-фразеологическими, грамматическими и стилистическими трудностями в текстах, относящихся к сфере основной профессиональной деятельности; - правильно оперировать языковыми средствами английского языка в ситуациях устного общения; - всеми видами чтения (изучающее, ознакомительное, поисковое и просмотровое); - письмом в пределах изученного материала (250-300 слов).	**Задание 2.*Переведите следующие предложения.*** *Обратите внимание! Одно и то же слово в зависимости от функции в предложении может принадлежать к разным частям речи. Каждая часть речи в словарной статье подается с новой строки и обозначается арабской цифрой с точкой. Сокращенные названия частей речи приводятся в начале словаря.* 1. The wire ends here. 2. The wire ends were snipped off. 3. Flashes blind people. 4. The study of this phenomenon is very important. 5. Physicists study the structure of matter. 6. The new device radically changes our method of work. 7.The hall houses a computer exhibition. **Задание 3.*Восстановите исходные формы слов, т.е. формы, которые можно найти в словаре. Проверьте себя по словарю.*** *Помните! Слова приводятся в словаре в исходных формах (глагол - в инфинитиве, существительное - в общем падеже единственного числа, прилагательное - в положительной степени и т.п.).* Biggest, best, given, flies, drying, dying, stopped, worst, phenomena, men, better, feet, nuclei, sought, wound, crises. **Задание 4.*Переведите следующие предложения; предварительно установите исходную форму выделенных слов.*** 1. The **earliest** man could not measure or count at all. 2.He **used** his **fingers**, **hands** and **feet** for **measuring**. 3.**Later** he **started** to use **pieces** of wood or metal of exact **lengths** as **standards**. 4.And now in **measuring** we still use such **words** as foot. **Задание 5.*Дайте словарное расположение послелогов; переведите словосочетания с помощью словаря.*** *Словосочетания глагола с наречием приводятся в словаре после знака (параллелограмм).* To look through, down, like, for, after, at, about, forward. **Задание 6.*Переведите предложения. Найдите в словаре выделенные фразеологические сочетания.*** *Фразеологические сочетания приводятся в англо-русском словаре со знаком (ромб).*	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Значение фразеологических сочетаний или идиоматических выражений следует искать в словаре по знаменательным словам, а не по служебным. 1. He used to drop in every now and then. 2.There was not much point in doing that. 3.It pays in the long run, you know. 4.I can't make head or tail of what is written here. 5.There is no point to store data which is out of date. **1. Translate the following noun-groups.** domestic orders, domestic demand, consumer goods, steel market, business activities, business opportunity, supply chain, supply capabilities, industry association, production volume, steel products, steel import, steel business, steel consumption, unemployment rate, growth trend, long-term debt, machine-tool industry, order value, GDP growth rate, record high temperature, general machinery makers, good spring weather, electric appliance manufacturers, strong consumer demand, small and medium size enterprises, zero growth period, forecast GDP figure, home electronic appliances, production and business approaches, corporation and business statistics survey, home theatre video equipment, new high value durable consumer goods. **2. Translate the following sentences paying attention to the meaning of the word "one".** The new high-speed computers have a number of advantages over the old ones. 2. This property is more important than the one mentioned above. 3. One can easily accelerate the speed using the accelerator. 4. Heat always passes from a cold body to a hot one. 5. On these test pieces one could not determine externally any corrosive action. 6. One should also note that isotopes may be employed in measuring the diffusion of metals. 7. Electrons, as one knows, are minute negative charges of electricity. 8. The videophone is a telephone with a TV screen in which one can see a person one is speaking with. 9. One must remember that electric currents ordinary flow only in a complete circuit. 10. One important use of food is to serve as a source of energy. **1. Read and translate the following text (some paragraphs). Write down the terms.** **THE ENERGY VECTOR OF THE 21st CENTURY**	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
ОК-8 способностью к самоорганизации и самообразованию			
Знать	способы самоорганизации и развития своего интеллектуального, культурного, духовного, нравственного, физического и профессионального уровня.	1. Понятие жизненного пути. 2. Понятие жизненной позиции. 3. Понятие жизненной перспективы. 4. Понятие жизненного сценария. 5. Личность как субъект жизненного пути. 6. Личностный рост и его патогенные механизмы. 7. Признаки остановки личностного роста. 8. Понятие индивидуального коучинга и условия его успешности.	Б1.Б.07 Технология командообразования и саморазвития
Уметь	находить недостатки в своем общекультурном и профессиональном уровне развития и стремиться их устранить; планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения; осуществления деятельности.	Проводить и анализировать тесты на выявление типа темперамента, общей эмоциональной направленности, своей командной роли, личностной агрессивности и конфликтности.	
Владеть	технологиями организации процесса самообразования; приемами целеполагания во временной перспективе, способами планирования, организации, самоконтроля и самооценки деятельности.	Составить резюме, портфолио, которое отражает видение собственного развития в будущей профессиональной деятельности, научно-исследовательской работе, общественной, культурно-творческой, спортивной и др. сферах (выбрать для себя приоритет).	
Знать	– порядок и особенности выполнения научно-исследовательских работ по государственным контрактам – отличительные признаки инновационной продукции	*Теоретические вопросы:* 1. Порядок и особенности выполнения научно- исследовательских работ по государственным контрактам. 2. Научно-техническая продукция как товар особого рода.	Б1.Б.40 Продвижение научной продукции
Уметь	– приобретать знания в области продвижения научной продукции – определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий,	*Практические задания:* 1. Определить области применения изобретения в соответствии с МПК: - Заявка 2015127606/02 - Заявка 2015153533	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	глобальный информационный ресурсов	- Заявка 2017116674 - Заявка 2017124014 2. Определить вектор развития устройства/технологии (дерево эволюции): - ДВС - Электродвигатель - Телевизор - Производство стекла - Спортивный велосипед	
Владеть	– классификацией научно-технической продукции, профессиональным языком предметной области знания – практическими навыками оценки качества для научно-технической продукции, навыками составления конкурсной документации	*Творческие задания:* 1. Описать жизненный цикл нововведений. 2. Описать научно-производственный цикл. 3. Привести классификации научно-технической продукции. 4. Указать особенности оценки качества для научно-технической продукции. 5. Привести виды охранных документов интеллектуальной собственности. Указать их особенности. 6. Описать виды научно-технических услуг.	
Знать	особенности организации процесса деятельности в технологическом предпринимательстве, основы самоорганизации и самообразования необходимые для управления инновационными проектами в процессе технологического предпринимательства;	*«Создание и развитие стартапа»* №1. Стартап – это: А) недавно появившаяся компания; Б) маленькая компания; В) новая компания в сфере IT; Г) временная организация, созданная для поиска бизнес-модели; Д) все ответы верные. №2. Основные характеристики стартапа: А) гибкость и оперативность принятия решений; Б) проектная, а не продуктовая составляющая; В) воспроизводимая бизнес-модель Г) масштабируемость; Д) все ответы верные. №3. Суть методики HADI-циклов состоит из: А) гипотеза – действие – данные – выводы; Б) скрытый режим – активные продажи – сделки –	ФТД.03 Технологическое предпринимательство

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		взаимодействие с появившимися клиентами; В) информирование, «шум» – активное привлечение потребителей – динамичное взаимодействие – возврат отказавшихся потребителей; Г) создание продукта – поиск потребителей – тестирование каналов – построение бизнес-модели; Д) нет верного ответа. №4. Модель SPACE описывает: А) 5 параметров, характеризующих стартап; Б) 3 «орбиты», одну из которых необходимо выбрать стартапу для устойчивого развития; В) модель выбора клиентом продукта, продажную цену, уникальность продукта, описание стартапа как поставщика и количество потенциальных покупателей; Г) нет верного ответа; Д) все ответы верные. №5. Стадии развития стартапа: А) поиск PRODUCT/MARKET FIT (идея – MVP) - соответствие продукта рынку – рост – «Долина смерти» – укрепление позиций, дальнейшие рост – масштабирование, захват рынков – IPO; Б) идея – PRESEED – SEED – раунд A – раунд B – раунд C – раунд D – IPO; В) идея – стартап – разработка – тестирование – стабилизация – масштабирование; Г) зарождение – первая версия продукта – доработка продукта – тестирование бизнес-модели – стабильная монетизация – масштабирование бизнеса (расширение базы клиентов, выход на новые рынки) Д) нет верного ответа; Е) все ответы верные.	
Уметь	ставить цели профессионально-личностного развития при решении задач в сфере коммерциализации сложных технологий, организации процесса технологического предпринимательства и управления инновационными проектами с учётом	**Комплексное задание по разработке предпринимательского проекта и его презентации:** Разработайте и сформируйте PPT-презентацию Вашего сквозного проекта по следующим пунктам: - «наименование предпринимательского проекта, авторы»; - «маркетинг, оценка рынка» (продаваемый продукт, цена,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	индивидуально-личностных особенностей, возможностей самоорганизации и самообразования;	каналы дистрибуции, продвижение); - «product development, разработка продукта» (традиционные аналоги, новизна, преимущества, инвестиционные затраты, производственная себестоимость); - «customer development, выведение продукта на рынок» (перечень мероприятий по выводу продукта на рынок, их стоимость); - «инструменты привлечения финансирования» (виды источников финансирования, их преимущества и недостатки); - «оценка инвестиционной привлекательности проекта»; - «риски проекта» (основные риски и инструменты их преодоления).	
Владеть	методами и технологиями постановки целей профессионально- личностного развития и их реализации, критической оценки результатов самоорганизации, самообразования при решении задач в сфере коммерциализации сложных технологий, организации процесса технологического предпринимательства и управления инновационными проектами	Разработанный и защищенный групповой и, или индивидуальный проект, выполненный в соответствии со всеми требованиями.	
ОК-9 способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности			
Знать	Основные средства и методы физического воспитания, анатомо-физиологические особенности организма и степень влияния физических упражнений на работу органов и систем организма. Основные средства и методы физического воспитания, основные методики планирования самостоятельных занятий по физической культуре с учетом анатомо-физиологических особенностей организма. Основные средства и методы физического воспитания, основные методики планирования самостоятельных занятий по физической культуре с учетом анатомо-физиологических особенностей организма и организации ЗОЖ, с целью укрепления здоровья, повышения уровня физической	*Перечень теоретических вопросов к зачету* 1. Дайте определение понятию «физическая культура» и раскройте его 2. Дайте определение основным понятиям теории физической культуры, ее компонентам. 3. Сформулируйте цель, задачи и опишите формы организации физического воспитания. 4. Назовите задачи физического воспитания студентов в вузе. 5. Перечислите основные компетенции студента, формируемые в результате освоения дисциплины «Физическая культура». 6. Перечислите основные требования, предъявляемые к студенту в процессе освоения дисциплины «Физическая культура». 7. Перечислите основные требования, необходимые для успешной аттестации студента (получение «зачета») по дисциплине «Физическая культура».	Б1.Б.41 Физическая культура и спорт

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	подготовленности.		
Уметь	Применять полученные теоретические знания по организации и планированию занятий по физической культуре анатомо-физиологических особенностей организма. Применять теоретические знания по организации самостоятельных занятий с учетом собственного уровня физического развития и физической подготовленности. Использовать тесты для определения физической подготовленности с целью организации самостоятельных занятий по определенному виду спорта с оздоровительной направленностью, для подготовки к профессиональной деятельности.	*Перечень заданий для зачета:* 1. Какие методы физического воспитания вы знаете? Кратко опишите их. 2. В чем отличие двигательного умения от двигательного навыка? 3. Перечислите основные физические качества, дайте им определения. 4. Какие формы занятий физическими упражнениями вы знаете? 5. Что такое ОФП? Его задачи. 6. В чем отличие ОФП от специальной физической подготовки? 7. Что представляет собой спортивная подготовка? 8. Для чего нужны показатели интенсивности физических нагрузок? 9. Расскажите об энергозатратах организма при выполнении нагрузок в зонах различной мощности?	
Владеть	Средствами и методами физического воспитания. Методиками организации и планирования самостоятельных занятий по физической культуре. Методиками организации физкультурных и спортивных занятий с учетом уровня физической подготовленности и профессиональной деятельности, навыками и умениями самоконтроля	*Задания на решение задач из профессиональной области, комплексные задания:* **1. ППФП в системе физического воспитания студентов;** **2. Факторы, определяющие ППФП студентов;** **3. Средства ППФП студентов;** **4. Основы методики самостоятельных занятий физическими упражнениями;** 5. Индивидуальный выбор спорта или систем физических упражнений.	
Знать	основные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике; формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; знание технических приемов и двигательных действий базовых видов спорта; современные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с	Показателем хорошего самочувствия является? указание учителя желание заниматься спортом анкетирование учебная успеваемость 2. С возрастом максимальные показатели частоты сердечных сокращений: растут не меняются снижаются изменяются по временам года 3. Кто в футбольной команде может играть руками? бек	Б1.Б.ДВ.01.01 Элективные курсы по физической культуре и спорту

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	учебной и производственной деятельностью; основные способы самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств; технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	форвард голкипер хавбек 4. Лыжные гонки – это: бег на лыжах по дистанции спуск с горы на лыжах бег на лыжах со стрельбой катание на лыжах за буксиром 5. Как определять пульс? пальцами на артерии у лучезапястного сустава глядя на себя в зеркало положив руку на солнечное сплетение сжав пальцы в замок 6. Оздоровительная тренировка позволяет добиться: Максимального расслабления Улучшение физических качеств Рекордных на мировом уровне спортивных результатов Сокращения рабочего дня 7. С какого расстояния пробивается пенальти в футболе? От 3-х до 5-ти метров 7 метров 11 метров от 15-ти до 20-ти метров 8. В какие спортивные игры играют с мячом? бильярд большой теннис бадминтон керлинг 9. Гиревой спорт – это вид спорта, направленный на развитие следующих качеств: скоростные качества силовые способности координационные способности гибкость 10. Какие действия игрока разрешены правилами баскетбола? бег с мячом в руках передачи и броски мяча	

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>столкновения, удары, захваты, толчки, подножки
разговоры с судьей во время игры
11. Каковы отличительные черты соревновательной деятельности?
наличие телевизионной трансляции
выявление сильнейшего
предварительное информирование о соревнованиях в газетах
красивая форма на спортсменах</td><td rowspan="2"></td></tr>
<tr><td>Уметь</td><td>использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;
выполнять физические упражнения разной функционально направленности, использовать их в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;
использовать разнообразные формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;
использовать знания технических приемов и двигательных действий базовых видов спорта в игровой и соревновательной деятельности;
анализировать и выделять эффективные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;
анализировать индивидуальные показатели здоровья, умственной и физической работоспособности, физического развития и физических качеств;
самостоятельно выполнять и контролировать выполнение Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</td><td>Нормативы VI ступени ВФСК ГТО для мужчин
МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ | ГТО Всероссийский физкультурно-спортивный комплекс «Готов к труду и обороне» | ДИРЕКЦИЯ СПОРТИВНЫХ И СОЦИАЛЬНЫХ ПРОЕКТОВ
Нормативы испытаний (тестов)
Всероссийского физкультурно-спортивного комплекса
«Готов к труду и обороне» (ГТО)
VI. СТУПЕНЬ
(возрастная группа от 18 до 29 лет)*
МУЖЧИНЫ
<table><tr><th rowspan="3">№ п/п</th><th rowspan="3">Испытания (тесты)</th><th colspan="6">Нормативы</th></tr><tr><th colspan="3">от 18 до 24 лет</th><th colspan="3">от 25 до 29 лет</th></tr><tr><th></th><th></th><th></th><th></th><th></th><th></th></tr><tr><td colspan="8">Обязательные испытания (тесты)</td></tr><tr><td rowspan="3">1.</td><td>Бег на 30 м (с)</td><td>4,8</td><td>4,6</td><td>4,3</td><td>5,4</td><td>5,0</td><td>4,6</td></tr><tr><td>или бег на 60 м (с)</td><td>9,0</td><td>8,6</td><td>7,9</td><td>9,5</td><td>9,1</td><td>8,2</td></tr><tr><td>или бег на 100 м (с)</td><td>14,4</td><td>14,1</td><td>13,1</td><td>15,1</td><td>14,8</td><td>13,8</td></tr><tr><td>2.</td><td>Бег на 3000 м (мин, с)</td><td>14.30</td><td>13.40</td><td>12.00</td><td>15.00</td><td>14.40</td><td>12.50</td></tr><tr><td rowspan="3">3.</td><td>Подтягивание из виса на высокой перекладине (количество раз)</td><td>10</td><td>12</td><td>15</td><td>7</td><td>9</td><td>13</td></tr><tr><td>или сгибание и разгибание рук в упоре лёжа на полу (количество раз)</td><td>28</td><td>32</td><td>44</td><td>22</td><td>25</td><td>39</td></tr><tr><td>или рывок гири 16 кг (количество раз)</td><td>21</td><td>25</td><td>43</td><td>19</td><td>23</td><td>40</td></tr><tr><td>4.</td><td>Наклон вперёд из положения стоя на гимнастической скамье (от уровня скамьи – см)</td><td>+6</td><td>+8</td><td>+13</td><td>+5</td><td>+7</td><td>+12</td></tr><tr><td colspan="8">Испытания (тесты) по выбору</td></tr><tr><td>5.</td><td>Челночный бег 3х10 м (с)</td><td>8,0</td><td>7,7</td><td>7,1</td><td>8,2</td><td>7,9</td><td>7,4</td></tr><tr><td rowspan="2">6.</td><td>Прыжок в длину с разбега (см)</td><td>370</td><td>380</td><td>430</td><td>–</td><td>–</td><td>–</td></tr><tr><td>или прыжок в длину с места толчком двумя ногами (см)</td><td>210</td><td>225</td><td>240</td><td>205</td><td>220</td><td>235</td></tr><tr><td>7.</td><td>Метание спортивного снаряда весом 700 г (м)</td><td>33</td><td>35</td><td>37</td><td>33</td><td>35</td><td>37</td></tr></table>
Нормативы VI ступени ВФСК ГТО для женщин</td></tr>
</table>

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>
Нормативы испытаний (тестов)
Всероссийского физкультурно-спортивного комплекса
«Готов к труду и обороне» (ГТО)

VI. СТУПЕНЬ
(возрастная группа от 18 до 29 лет)*
ЖЕНЩИНЫ
<table>
<tr><th rowspan="3">№ п/п</th><th rowspan="3">Испытания (тесты)</th><th colspan="6">Нормативы</th></tr>
<tr><th colspan="3">от 18 до 24 лет</th><th colspan="3">от 25 до 29 лет</th></tr>
<tr><th></th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="8">Обязательные испытания (тесты)</td></tr>
<tr><td>1.</td><td>Бег на 30 м (с)</td><td>5,9</td><td>5,7</td><td>5,1</td><td>6,4</td><td>6,1</td><td>5,4</td></tr>
<tr><td></td><td>или бег на 60 м (с)</td><td>10,9</td><td>10,5</td><td>9,6</td><td>11,2</td><td>10,7</td><td>9,9</td></tr>
<tr><td></td><td>или бег на 100 м (с)</td><td>17,8</td><td>17,4</td><td>16,4</td><td>18,8</td><td>18,2</td><td>17,0</td></tr>
<tr><td>2.</td><td>Бег на 2000 м (мин, с)</td><td>13.10</td><td>12.30</td><td>10.50</td><td>14.00</td><td>13.10</td><td>11.35</td></tr>
<tr><td>3.</td><td>Подтягивание из виса лёжа на низкой перекладине 90 см (количество раз)</td><td>10</td><td>12</td><td>18</td><td>9</td><td>11</td><td>17</td></tr>
<tr><td></td><td>или сгибание и разгибание рук в упоре лёжа на полу (количество раз)</td><td>10</td><td>12</td><td>17</td><td>9</td><td>11</td><td>16</td></tr>
<tr><td>4.</td><td>Наклон вперёд из положения стоя на гимнастической скамье (от уровня скамьи – см)</td><td>+8</td><td>+11</td><td>+16</td><td>+7</td><td>+9</td><td>+14</td></tr>
<tr><td colspan="8">Испытания (тесты) по выбору</td></tr>
<tr><td>5.</td><td>Челночный бег 3х10 м (с)</td><td>9,0</td><td>8,8</td><td>8,2</td><td>9,3</td><td>9,0</td><td>8,7</td></tr>
<tr><td>6.</td><td>Прыжок в длину с разбега (см)</td><td>270</td><td>290</td><td>320</td><td>–</td><td>–</td><td>–</td></tr>
<tr><td></td><td>или прыжок в длину с места толчком двумя ногами (см)</td><td>170</td><td>180</td><td>195</td><td>165</td><td>175</td><td>190</td></tr>
<tr><td>7.</td><td>Поднимание туловища из положения лёжа на спине (количество раз за 1 мин)</td><td>32</td><td>35</td><td>43</td><td>24</td><td>29</td><td>37</td></tr>
</table>
Тесты промежуточного контроля физической подготовленности студентов 1-4 курсов специального медицинского отделения (юноши)
</td><td></td></tr>
<tr><td>Владеть</td><td>практическими навыками использования регулятивных, познавательных, коммуникативных действий в спортивной, физкультурной, оздоровительной и социальной практике;
навыками использования физических упражнений разной функционально направленности в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;
практическими навыками использования разнообразных форм и видов физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;</td><td>Тесты промежуточного контроля физической подготовленности студентов 1-4 курсов специального медицинского отделения (юноши)

<table>
<tr><td>№ п/п</td><td>Контрольные упражнения</td><td>Оценка</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>1.</td><td>Бег 30 м (сек)</td><td>5,5</td><td>5,9</td><td>6,3</td><td>6,7</td><td>7,1</td></tr>
<tr><td>2.</td><td>12-минутный бег (м)</td><td>2100</td><td>1950</td><td>1800</td><td>1500</td><td>1200</td></tr>
<tr><td>3.</td><td>Прыжки в длину с места (см) или</td><td>230</td><td>220</td><td>210</td><td>200</td><td>190</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr>
<td></td>
<td>технических приемами и двигательными действиями базовых видов спорта, навыками активного применения их в игровой и соревновательной деятельности;
навыками использования современных технологий укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;
основными способами самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств;
навыками подготовки к выполнению Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</td>
<td>
<table>
<tr><td></td><td>приседание на 2-х ногах для студентов с опущением внутренних органов (кол-во раз)</td><td>70</td><td>60</td><td>50</td><td>40</td><td>30</td></tr>
<tr><td>4.</td><td>Подтягивание в висе (кол-во раз)</td><td>8</td><td>6</td><td>4</td><td>2</td><td>1</td></tr>
<tr><td>5.</td><td>Поднимание туловища из положения лежа на спине, ноги согнуты в коленях, руки за головой(кол-во раз)</td><td>40</td><td>30</td><td>20</td><td>10</td><td>5</td></tr>
<tr><td>6.</td><td>Наклон вперед, стоя на гимнастической скамейке, ноги прямые на ширине ступни. Пальцы рук ниже или выше уровня скамейки (см)</td><td>5</td><td>0</td><td>+5</td><td>+10</td><td>+15</td></tr>
</table>
Примечание: для студентов с черепно-мозговой травмой или миопией свыше – 8D упр. 5 исключается, прыжок в длину с места заменяется приседанием.
Для студентов с пороком сердца упр. 1 исключается, а упр. 2 выполняется в объеме 70% от принятых норм.

Тесты промежуточного контроля физической подготовленности студентов 1-4 курсов специального медицинского отделения (девушки)

<table>
<tr><td>№</td><td>Контрольные</td><td>Оценка</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

<table>
<tr><td>Структурный элемент компетенции</td><td>Планируемые результаты обучения</td><td>Оценочные средства</td><td>Структурный элемент образовательной программы</td></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>п/п</td><td>упражнения</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>1.</td><td>Бег 30 м (сек)</td><td>6,4</td><td>7,0</td><td>7,4</td><td>7,8</td><td>8,3</td></tr>
<tr><td>2.</td><td>12-минутный бег (м)</td><td>1200</td><td>1050</td><td>900</td><td>600</td><td>300</td></tr>
<tr><td rowspan="2">3.</td><td rowspan="2">Прыжки в длину с места (см) или приседание на 2-х ногах для студентов с опущением внутренних органов (кол-во раз)</td><td>160</td><td>150</td><td>140</td><td>130</td><td>120</td></tr>
<tr><td>50</td><td>40</td><td>30</td><td>20</td><td>10</td></tr>
<tr><td>4.</td><td>Сгибание и разгибание рук в положении лежа на животе (кол-во раз)</td><td>50</td><td>40</td><td>30</td><td>20</td><td>10</td></tr>
<tr><td>5.</td><td>Поднимание туловища из положения лежа на спине, ноги согнуты в коленях, руки за головой (кол-во раз)</td><td>30</td><td>20</td><td>15</td><td>10</td><td>5</td></tr>
<tr><td>6.</td><td>Наклон вперед, стоя на гимнастической скамейке, ноги прямые на ширине ступни. Пальцы рук ниже или выше уровня скамейки (см)</td><td>10</td><td>5</td><td>0</td><td>+5</td><td>+10</td></tr>
</table>
Примечание: для студентов с черепно-мозговой травмой или миопией свыше – 8D упр. 5 исключается, прыжок в длину с места заменяется приседанием.
Для студентов с пороком сердца упр. 1 исключается, а упр. 2 выполняется в объеме 70% от принятых норм.
</td><td></td></tr>
<tr><td>Знать</td><td>основные понятия и универсальные учебные действия (регулятивные, познавательные,</td><td>Тестовые вопросы:
1. Показателем хорошего самочувствия является?</td><td>Б1.Б.ДВ.01.02
Адаптивные курсы</td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике; формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; знание технических приемов и двигательных действий базовых видов спорта; современные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью; основные способы самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств; технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	указание учителя желание заниматься спортом анкетирование учебная успеваемость 2. С возрастом максимальные показатели частоты сердечных сокращений: растут не меняются снижаются изменяются по временам года 3. Кто в футбольной команде может играть руками? бек форвард голкипер хавбек 4. Лыжные гонки – это: бег на лыжах по дистанции спуск с горы на лыжах бег на лыжах со стрельбой катание на лыжах за буксиром 5. Как определять пульс? пальцами на артерии у лучезапястного сустава глядя на себя в зеркало положив руку на солнечное сплетение сжав пальцы в замок 6. Оздоровительная тренировка позволяет добиться: Максимального расслабления Улучшение физических качеств Рекордных на мировом уровне спортивных результатов Сокращения рабочего дня 7. С какого расстояния пробивается пенальти в футболе? от3-х до 5-ти метров 7 метров 11 метров от 15-ти до 20-ти метров 8. В какие спортивные игры играют с мячом? бильярд	по физической культуре и спорту

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		большой теннис бадминтон керлинг 9. Гиревой спорт – это вид спорта, направленный на развитие следующих качеств: скоростные качества силовые способности координационные способности гибкость 10. Какие действия игрока разрешены правилами баскетбола? бег с мячом в руках передачи и броски мяча столкновения, удары, захваты, толчки, подножки разговоры с судьей во время игры 11. Каковы отличительные черты соревновательной деятельности? наличие телевизионной трансляции выявление сильнейшего предварительное информирование о соревнованиях в газетах красивая форма на спортсменах выполнение нормативов общефизической подготовленности; - заполнение дневника самоконтроля. <u>Примерная тематика рефератов</u> 1. Диагноз и краткая характеристика заболевания студента. 2. Влияние заболевания на личную работоспособность и самочувствие. 3. Медицинские противопоказания при занятиях физическими упражнениями и применение других средств физической культуры при данном заболевании (диагнозе). 4. Составление и обоснование индивидуального комплекса физических упражнений и доступных средств физической культуры (с указанием примерной дозировки). 5. Физическая культура в общекультурной и профессиональной подготовке специалиста. 6. Физическая культура и спорт как социальные феномены общества. 7. Основы здорового образа жизни. 8. Общая физическая и специальная подготовка в системе	

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td></td><td>физического воспитания.
9. Основы оздоровительной физической культуры.
10. Общие положения, организация и судейство соревнований.
11. Допинг и антидопинговый контроль.
12. Массаж, как средство реабилитации.
13. Лечебная физическая культура: средства и методы.
14. Подвижная игра, как средство и метод физического развития.
15. Тестирование уровня физического развития студентов.
16. Современные проблемы физической культуры и спорта.
17. Комплекс ГТО: история и современность
Тестыпромежуточногоконтроляфизическойподготовленностистудентов1-4курсовс нарушениями слуха:</td><td></td></tr>
<tr><td>Уметь</td><td>использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;
выполнять физические упражнения разной функционально направленности, использовать их в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;
использовать разнообразные формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;
использовать знания технических приемов и двигательных действий базовых видов спорта в игровой и соревновательной деятельности;
анализировать и выделять эффективные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики</td><td>Нормативы VI ступени ВФСК ГТО для мужчин
МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ | ГТО Всероссийский физкультурно-спортивный комплекс «Готов к труду и обороне» | ДИРЕКЦИЯ СПОРТИВНЫХ И СОЦИАЛЬНЫХ ПРОЕКТОВ
Нормативы испытаний (тестов)
Всероссийского физкультурно-спортивного комплекса
«Готов к труду и обороне» (ГТО)
VI. СТУПЕНЬ
(возрастная группа от 18 до 29 лет)*
МУЖЧИНЫ
<table><tr><th rowspan="3">№ п/п</th><th rowspan="3">Испытания (тесты)</th><th colspan="6">Нормативы</th></tr><tr><th colspan="3">от 18 до 24 лет</th><th colspan="3">от 25 до 29 лет</th></tr><tr><th></th><th></th><th></th><th></th><th></th><th></th></tr><tr><td colspan="8">Обязательные испытания (тесты)</td></tr><tr><td rowspan="3">1.</td><td>Бег на 30 м (с)</td><td>4,8</td><td>4,6</td><td>4,3</td><td>5,4</td><td>5,0</td><td>4,6</td></tr><tr><td>или бег на 60 м (с)</td><td>9,0</td><td>8,6</td><td>7,9</td><td>9,5</td><td>9,1</td><td>8,2</td></tr><tr><td>или бег на 100 м (с)</td><td>14,4</td><td>14,1</td><td>13,1</td><td>15,1</td><td>14,8</td><td>13,8</td></tr><tr><td>2.</td><td>Бег на 3000 м (мин, с)</td><td>14.30</td><td>13.40</td><td>12.00</td><td>15.00</td><td>14.40</td><td>12.50</td></tr><tr><td rowspan="3">3.</td><td>Подтягивание из виса на высокой перекладине (количество раз)</td><td>10</td><td>12</td><td>15</td><td>7</td><td>9</td><td>13</td></tr><tr><td>или сгибание и разгибание рук в упоре лёжа на полу (количество раз)</td><td>28</td><td>32</td><td>44</td><td>22</td><td>25</td><td>39</td></tr><tr><td>или рывок гири 16 кг (количество раз)</td><td>21</td><td>25</td><td>43</td><td>19</td><td>23</td><td>40</td></tr><tr><td>4.</td><td>Наклон вперёд из положения стоя на гимнастической скамье (от уровня скамьи – см)</td><td>+6</td><td>+8</td><td>+13</td><td>+5</td><td>+7</td><td>+12</td></tr><tr><td colspan="8">Испытания (тесты) по выбору</td></tr><tr><td>5.</td><td>Челночный бег 3х10 м (с)</td><td>8,0</td><td>7,7</td><td>7,1</td><td>8,2</td><td>7,9</td><td>7,4</td></tr><tr><td>6.</td><td>Прыжок в длину с разбега (см)</td><td>370</td><td>380</td><td>430</td><td>–</td><td>–</td><td>–</td></tr><tr><td>6.</td><td>или прыжок в длину с места толчком двумя ногами (см)</td><td>210</td><td>225</td><td>240</td><td>205</td><td>220</td><td>235</td></tr><tr><td>7.</td><td>Метание спортивного снаряда весом 700 г (м)</td><td>33</td><td>35</td><td>37</td><td>33</td><td>35</td><td>37</td></tr></table></td><td></td></tr>
</table>

<table>
<tr><td>Структурный элемент компетенции</td><td>Планируемые результаты обучения</td><td>Оценочные средства</td><td>Структурный элемент образовательной программы</td></tr>
<tr><td></td><td>предупреждения заболеваний, связанных с учебной и производственной деятельностью;
анализировать индивидуальные показатели здоровья, умственной и физической работоспособности, физического развития и физических качеств;
самостоятельно выполнять и контролировать выполнение Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</td><td>Нормативы VI ступени ВФСК ГТО для женщин
МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ | ГТО Всероссийский физкультурно-спортивный комплекс «Готов к труду и обороне» | ДИРЕКЦИЯ СПОРТИВНЫХ И СОЦИАЛЬНЫХ ПРОЕКТОВ
Нормативы испытаний (тестов)
Всероссийского физкультурно-спортивного комплекса
«Готов к труду и обороне» (ГТО)
VI. СТУПЕНЬ
(возрастная группа от 18 до 29 лет)*
ЖЕНЩИНЫ
<table>
<tr><th rowspan="3">№ п/п</th><th rowspan="3">Испытания (тесты)</th><th colspan="6">Нормативы</th></tr>
<tr><th colspan="3">от 18 до 24 лет</th><th colspan="3">от 25 до 29 лет</th></tr>
<tr><th></th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="8">Обязательные испытания (тесты)</td></tr>
<tr><td rowspan="3">1.</td><td>Бег на 30 м (с)</td><td>5,9</td><td>5,7</td><td>5,1</td><td>6,4</td><td>6,1</td><td>5,4</td></tr>
<tr><td>или бег на 60 м (с)</td><td>10,9</td><td>10,5</td><td>9,6</td><td>11,2</td><td>10,7</td><td>9,9</td></tr>
<tr><td>или бег на 100 м (с)</td><td>17,8</td><td>17,4</td><td>16,4</td><td>18,8</td><td>18,2</td><td>17,0</td></tr>
<tr><td>2.</td><td>Бег на 2000 м (мин, с)</td><td>13.10</td><td>12.30</td><td>10.50</td><td>14.00</td><td>13.10</td><td>11.35</td></tr>
<tr><td rowspan="2">3.</td><td>Подтягивание из виса лёжа на низкой перекладине 90 см (количество раз)</td><td>10</td><td>12</td><td>18</td><td>9</td><td>11</td><td>17</td></tr>
<tr><td>или сгибание и разгибание рук в упоре лёжа на полу (количество раз)</td><td>10</td><td>12</td><td>17</td><td>9</td><td>11</td><td>16</td></tr>
<tr><td>4.</td><td>Наклон вперёд из положения стоя на гимнастической скамье (от уровня скамьи – см)</td><td>+8</td><td>+11</td><td>+16</td><td>+7</td><td>+9</td><td>+14</td></tr>
<tr><td colspan="8">Испытания (тесты) по выбору</td></tr>
<tr><td>5.</td><td>Челночный бег 3х10 м (с)</td><td>9,0</td><td>8,8</td><td>8,2</td><td>9,3</td><td>9,0</td><td>8,7</td></tr>
<tr><td rowspan="2">6.</td><td>Прыжок в длину с разбега (см)</td><td>270</td><td>290</td><td>320</td><td>–</td><td>–</td><td>–</td></tr>
<tr><td>или прыжок в длину с места толчком двумя ногами (см)</td><td>170</td><td>180</td><td>195</td><td>165</td><td>175</td><td>190</td></tr>
<tr><td>7.</td><td>Поднимание туловища из положения лёжа на спине (количество раз за 1 мин)</td><td>32</td><td>35</td><td>43</td><td>24</td><td>29</td><td>37</td></tr>
</table></td><td></td></tr>
<tr><td>Владеть</td><td>практическими навыками использования регулятивных, познавательных, коммуникативных действий в спортивной, физкультурной, оздоровительной и социальной практике;
навыками использования физических упражнений разной функционально направленности в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;
практическими навыками использования разнообразных форм и видов физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;
техническими приемами и двигательными действиями базовых видов спорта, навыками</td><td>Тестытекущегоиитоговогоконтроляфизическойподготовленностистудентов1-4 (юноши) для лиц с нарушениями зрения
<table>
<tr><td rowspan="2">п/п</td><td rowspan="2">Контрольныеупражнения</td><td rowspan="2">Месяц</td><td colspan="5">Оценка</td></tr>
<tr><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>1.</td><td>Ходьба (м)</td><td>дек,май</td><td>2100</td><td>1950</td><td>1800</td><td>1500</td><td>1200</td></tr>
<tr><td rowspan="2">2.</td><td rowspan="2">Приседаниена2-хногах(кол-вораз)</td><td rowspan="2">окт, март</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>70</td><td>60</td><td>50</td><td>40</td><td>30</td></tr>
<tr><td>2.</td><td>Подтягивание на низкой перекладине (Юноши)</td><td>дек,май</td><td>8</td><td>6</td><td>4</td><td>2</td><td>1</td></tr>
</table>
Тестытекущегоиитоговогоконтроляфизическойподготовленностист</td><td></td></tr>
</table>

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td>активного применения их в игровой и соревновательной деятельности;
навыками использования современных технологий укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;
основными способами самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств;
навыками подготовки к выполнению Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</td><td>удентов1-4 (девушки) для лиц с нарушениями зрения
<table>
<tr><th>п/п</th><th>Контрольныеупражнения</th><th>Месяц</th><th colspan="5">Оценка</th></tr>
<tr><td></td><td></td><td></td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>1.</td><td>Ходьба (м)</td><td>дек,май</td><td>1200</td><td>1050</td><td>900</td><td>600</td><td>300</td></tr>
<tr><td rowspan="2">2.</td><td rowspan="2">Приседаниена2-хногах(кол-вораз)</td><td rowspan="2">окт, март</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>50</td><td>40</td><td>30</td><td>20</td><td>10</td></tr>
<tr><td>3.</td><td>Подтягивание на низкой перекладине (Девушки)</td><td>дек,май</td><td>6</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
</table>
Тестытекущегоиитоговогоконтроляфизическойподготовленностистудентов1-4курсовдлялиц с нарушениями опорно-двигательного аппарата (ДЦП) при повреждениях нижних конечностей
<table>
<tr><th>п/п</th><th>Контрольныеупражнения</th><th>Месяц</th><th colspan="5">Оценка</th></tr>
<tr><td></td><td></td><td></td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>1.</td><td>Подтягивание на низкой перекладине (Девушки)</td><td>дек, май</td><td>6</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>2.</td><td>Подтягивание на низкой перекладине (Юноши)</td><td>дек, май</td><td>8</td><td>6</td><td>4</td><td>2</td><td>1</td></tr>
</table>
Тестытекущегоиитоговогоконтроляфизическойподготовленностистудентов1-4курсовдлялиц с нарушениями опорно-двигательного аппарата (ДЦП) при повреждениях верхних конечностей
<table>
<tr><th>п/п</th><th>Контрольныеупражнения</th><th>Месяц</th><th colspan="5">Оценка</th></tr>
<tr><td></td><td></td><td></td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>1.</td><td>Приседаниена2-хногах(кол-вораз) (Юноши)</td><td>окт, март</td><td>40</td><td>30</td><td>20</td><td>10</td><td>5</td></tr>
<tr><td>2.</td><td>Приседаниена2-хногах(кол-вораз) (Девушки)</td><td>окт, март</td><td>30</td><td>20</td><td>15</td><td>10</td><td>5</td></tr>
</table></td><td></td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ			
ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач			
Знать	– основные законы физики, границы применимости этих законов и их связь с явлениями и процессами, происходящими в природе; − методы анализа физических процессов и явлений; − физико-математический аппарат, используемый для описания физических закономерностей	**Перечень теоретических вопросов к экзамену (1 семестр)** 1. Физика как наука. Экспериментальный подход. Понятие о материи. 2. Кинематика поступательного движения. Понятие радиус-вектора, скорости и ускорения. 3. Начальные условия. Прямая и обратная задачи механики. 4. Движение по окружности. Угол поворота, угловая скорость и угловое ускорение. Связь угловых и линейных величин. 5. Криволинейное движение. Тангенциальное и нормальное ускорение. Полное ускорение. Угол между скоростью и ускорением. 6. Инерциальные системы отсчета. Принцип относительности Галилея. 7. Понятие силы, массы и импульса. Законы Ньютона. Основной закон динамики поступательного движения. 8. Фундаментальные взаимодействия. Виды сил в механике. 9. Основные динамические характеристики вращательного движения: момент инерции, момент импульса, момент силы 10. Момент импульса и момент силы относительно точки. Основное уравнение динамики вращательного движения. 11. Вращение вокруг неподвижной оси. Момент инерции. Расчет моментов инерции простых тел. Теорема Штейнера. 12. Законы сохранения в механике. Замкнутая система. Законы сохранения импульса и момента импульса. 13. Работа и мощность. Кинетическая энергия поступательного и вращательного движения. 14. Консервативные силы. Потенциальная энергия. 15. Работа и энергия. Закон сохранения полной механической энергии. 16. Два способа описания взаимодействия. Движение частицы в одномерном стационарном поле. Связь между силой и	Б1.Б.09Физика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		потенциальной энергией. 17. Гармонические колебания. Амплитуда, частота, начальная фаза, период. 18. Математический и физический маятник. 19. Энергия гармонических колебаний. 20. Затухающие колебания. Характеристики затухания. Энергия затухающих колебаний. 21. Вынужденные колебания. Резонанс. 22. Общее понятие о волнах. Характеристики бегущей волны. 23. Волновое уравнение плоской волны. 24. Наложение упругих волн. Стоячая волна и ее особенности. 25. Постулаты Эйнштейна. Замедление времени. Лоренцево сокращение длины. Релятивистские инварианты. Интервал. 26. Релятивистский импульс. Связь массы, энергии и импульса частицы. Энергия покоя. Законы сохранения при релятивистских скоростях. 27. Макросистема. Микросостояние и макросостояние системы. Статистический подход. Понятие вероятности и средней величины. 28. Функция распределения случайной величины. Распределение молекул по проекциям скоростей. 29. Распределение молекул по модулю скорости. Наиболее вероятная, средняя и среднеквадратичная скорости. 30. Атомы и молекулы как элементарные частицы вещества. Их количественные характеристики. 31. Модель идеального газа. Давление и температура с точки зрения молекулярно-кинетической теории. 32. Уравнение состояния идеального газа. Изопроцессы 33. Распределение молекул идеального газа по высоте в поле тяжести Земли. Барометрическая формула. 34. Понятие степеней свободы молекулы. Теорема о равнораспределении энергии по степеням свободы. 35. Внутренняя энергия как функция состояния системы. Первое начало термодинамики. 36. Работа как функция процесса. Изохорический,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		изобарический и изотермический процессы. 37. Понятие теплоемкости. Теплоемкость при изохорическом, изобарическом и изотермическом процессах. 38. Адиабатический процесс. Уравнение Пуассона. Постоянная адиабаты. Первое начало термодинамики для адиабатического процесса 39. Циклический процесс. Коэффициент полезного действия тепловой машины. 40. Цикл Карно. Второе начало термодинамики. Формулировки Клаузиуса и Кельвина. 41. Проблема необратимости тепловых процессов. Энтропия системы и ее свойства. Теорема Нернста. Термодинамическая шкала температур. 42. Основное уравнение термодинамики. Энтропия идеального газа. Изменение энтропии при изопроцессах. 43. Статистический вес макросостояния. Суть необратимости. Статистический смысл энтропии. Формула Больцмана. **Перечень теоретических вопросов к экзамену (2 семестр)** 1. Силы взаимодействия в природе. Электростатическое поле. Закон Кулона. Напряженность электростатического поля. Принцип суперпозиции. 2. Силовые лини. Поток вектора напряженности электростатического поля. Теорема Гаусса. 3. Потенциал. Теорема о циркуляции вектора напряженности электростатического поля. Связь между напряженностью и потенциалом. 4. Электроемкость. Конденсаторы. Соединение конденсаторов. Энергия конденсатора. Энергия электрического поля. 5. Электрическое поле в диэлектриках. Поляризация. 6. Электрический ток. Плотность тока. Уравнение непрерывности. Закон Ома в дифференциальной и интегральной формах.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		7. Сопротивление проводников. Сторонние силы. Закон Ома в интегральной форме. 8. Правила Кирхгофа для расчета разветвленных цепей. Мощность тока. Закон Джоуля-Ленца. 9. Единая природа электрического и магнитного поля. Поле движущегося заряда. Принцип суперпозиции магнитных полей. Закон Био-Савара. 10. Поток и циркуляция вектора индукции магнитного поля. Теорема Гаусса и теорема о циркуляции. 11. Сила Лоренца. Сила Ампера. 12. Закон электромагнитной индукции Фарадея. Правило Ленца. Вихревое электрическое поле. 13. Явление самоиндукции. Индуктивность. Энергия контура с током. Энергия магнитного поля. 14. Колебательный контур. Свободные гармонические и затухающие электрические колебания. Энергия колебаний. 15. Вынужденные электрические колебания. Векторная диаграмма напряжений. Резонанс тока. 16. Переменный ток. Индуктивное и емкостное сопротивление. Мощность в цепи переменного тока. Действующие значения тока и напряжения. 17. Электрическое поле в веществе. Поляризация диэлектрика. Вектор электрического смещения. Диэлектрическая проницаемость вещества. 18. Магнитное поле в веществе. Намагниченность. Напряженность магнитного поля. Магнитная проницаемость вещества. Ферромагнетики. 19. Система уравнений Максвелла как обобщение разрозненных явлений электричества и магнетизма. Материальные уравнения. 20. Свойства уравнений Максвелла. Предсказание существования электромагнитных волн. 21. Электромагнитные волны. Волновое уравнение. Свойства электромагнитных волн. 22. Плоская электромагнитная волна и ее основные	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		характеристики. Энергия и импульс электромагнитной волны. 23. Естественный и поляризованный свет. Степень поляризации линейно поляризованного света. Закон Малюса. 24. Поляризация при отражении и преломлении света на границе раздела диэлектриков. Угол Брюстера. Двойное лучепреломление. 25. Способы поляризации естественного света. Призма Николя. Вращение плоскости поляризации света при прохождении через оптически активную среду. 26. Шкала электромагнитных волн. Особенности оптического диапазона. Показатель преломления среды. 27. Когерентные волны. Интерференция световых волн. Сложение интенсивностей в случае некогерентных и когерентных колебаний. 28. Оптическая разность хода. Связь оптической разности хода двух волн с разностью фаз между ними. Условия максимума и минимума. 29. Схема Юнга для наблюдения интерференции. Временная и пространственная когерентность. 30. Интерференция в тонких пленках. Наблюдение колец Ньютона в отраженном и проходящем свете. 31. Явление дифракции. Дифракция Френеля и Фраунгофера. Принцип Гюйгенса-Френеля. 32. Дифракция Френеля на круглом отверстии. Зоны Френеля. Графический метод сложения амплитуд 33. Дифракция Фраунгофера на узкой прямолинейной щели. Дифракционная решетка как совокупность конечного числа щелей. **Перечень теоретических вопросов к зачету (3 семестр)** 1. Тепловое излучение тела. Закон Стефана-Больцмана. Закон смещения Вина. Гипотеза Планка.	

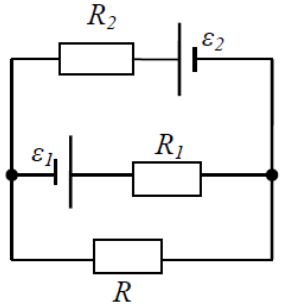
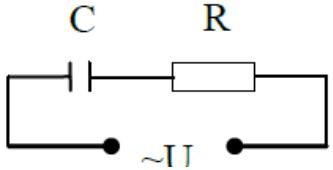
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		2. Фотоэффект. Законы Столетова. Формула Эйнштейна. 3. Фотоны. Давление света. Корпускулярно-волновой дуализм света. 4. Рассеяние фотона на свободном электроне. Формула Комптона. 5. Волновые свойства частиц. Длина волны де Бройля. Экспериментальные подтверждения гипотезы де Бройля. 6. Принцип неопределенности. Соотношение неопределенностей Гейзенберга. Особенности процесса измерения в квантовой механике. 7. Физическое истолкование волн де Бройля. Волновая функция и ее свойства. Плотность вероятности обнаружения частицы. 8. Основная задача квантовой механики. Нестационарное и стационарное уравнение Шрёдингера. 9. Частица в одномерной бесконечной прямоугольной потенциальной яме. Квантование энергии. Собственные функции состояния частицы. 10. Прохождение частицы через потенциальный барьер. Туннельный эффект. 11. Квантовый гармонический осциллятор. 12. Планетарная модель атома. Постулаты Бора. Квантование энергии водородоподобной системы. 13. Излучение водородоподобных систем. Спектральные серии атома водорода. Обобщенная формула Бальмера. 14. Спектры многоэлектронных атомов. Закон Мозли. 15. Уравнение Шредингера для атома водорода. Квантование момента импульса. Правила отбора. 16. Спин электрона. Квантовые числа, описывающие состояние электрона в атоме. Кратность вырождения энергетических уровней. Принцип Паули. 17. Принцип тождественности одинаковых частиц. Бозоны и фермионы. Квантовые распределения. 18. Свободные электроны в металле. Энергия Ферми. Зонная теория твердых тел.	

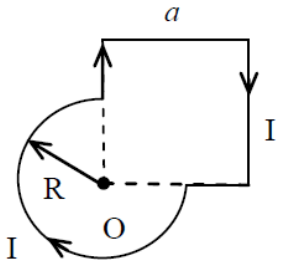
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		19. Электропроводность металлов и полупроводников. Сверхпроводимость. 20. Явление радиоактивности. Основной закон радиоактивного распада. Постоянная распада. Период полураспада. 21. Состав и характеристики атомного ядра. Капельная модель. Размер и спин ядра. 22. Масса и энергия связи атомного ядра. Зависимость удельной энергия связи от массового числа. Оболочечная модель ядра. 23. Ядерные реакции. Энергия реакции. Реакции деления и синтеза ядер. 24. Радиоактивные ряды. Основные закономерности α-излучения ядер. Длина свободного пробега α-частиц. 25. Три вида β-распада. Энергетический спектр β-частиц. Нейтрино. 26. Особенности γ-излучения ядер. Прохождение γ-квантов через вещество. 27. Классификация элементарных частиц. Лептоны. Лептонный заряд. 28. Адроны. Барионный заряд. Кварковая модель адронов.	
Уметь	– применять физические законы и физико-математический аппарат для формализации описания физических явлений и процессов и решения задач в рамках физики и смежных дисциплин	**Примерный перечень практических заданий для экзамена (1 семестр)** 1. Частица движется с ускорением (м/с^2). Определить модуль скорости частицы в момент времени t = 2 с и пройденный ею к этому моменту путь, если в начальный момент времени t = 0 t её скорость была (м/с) 2. Сколько оборотов сделали колеса автомобиля после включения тормоза до полной остановки, если в момент начала торможения автомобиль имел скорость v_0 = 60 км/ч и остановиляся за t = 3 с после начала торможения? Диаметр колеса D = 0,7 м. Чему равно среднее угловое ускорение колес при торможении? 3. На тело массы m, лежащее на гладкой горизонтальной	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		плоскости, в момент t = 0 начала действовать сила, зависящая от времени как $F = kt$, где k – постоянная. Направление этой силы все время составляет угол α с горизонтом. Найти: а) скорость тела в момент отрыва от плоскости; б) путь пройденный телом к этому моменту. 4. Через неподвижный блок, укрепленный на краю стола, перекинута нить, к которой привязаны три груза массами m_1 = 800 г, m_2 = 700 г, m_3 = 200 г. Масса блока M = 500 г, радиус R = 0,38 м. Грузы 1 и 2 лежат на столе, груз 3 висит по другую сторону блока. Считая нить невесомой и нерастяжимой и пренебрегая трением, определите ускорение грузов, а так же расстояние S, которое груз m_3 пройдет от начала движения до того момента, когда кинетическая энергия вращения блока будет $E_к$ = 1,1 Дж 5. На конах тонкого однородного стержня длиной l и массой $3m$ прикреплены маленькие шарики массами m и $2m$. Определить момент инерции I такой системы относительно оси, перпендикулярной стержню и проходящей через точку О, лежащую на оси стержня и отстоящую на расстояние $\frac{1}{4}l$ от конца с большей массой. При расчетах принять l = 1 м, m= 0,1 кг. Шарики рассматривать как материальные точки 6. Человек массой m = 60 кг, стоящий на краю горизонтальной платформы массой M = 120 кг, вращающейся по инерции вокруг неподвижной вертикальной оси с частотой n = 12 мин$^{-1}$, переходит к её центру. Считая платформу круглым однородным диском, а человека – точечной массой, определите, с какой частотой будет тогда вращаться платформа 7. Материальная точка массой m = 2 кг двигалась под действием некоторой силы, направленной вдоль оси OX согласно уравнению . Найти мощность развиваемую силой в момент времени t_1 = 2 с и t_2 = 5 с. 8. Снаряд, летящий со скоростью 16 м/с, разорвался на два	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		осколка, массы которых 6 кг и 10 кг. Скорость первого осколка 12 м/с и направлена под углом 600 к скорости снаряда. Найти величину скорости второго осколка и ее направление. 9. Определить начальную фазу гармонического колебания тела, если через 0,25 с от начала движения смещение, изменяющееся по закону синуса, было равно половине амплитуды. Период колебания 6 с 10. Найти период малых вертикальных колебаний шарика массы 40 г, укреплённого на середине горизонтально натянутой струны длины 1 м. Натяжение струны считать постоянным и равным 10 Н 11. Через N=8 полных колебаний пружинного маятника ампли- туда колебаний уменьшилась в 2 раза. Найдите промежуток времени за который это произошло если жесткость пружины к =10 Н/м, а масса гру- за на пружине m=50 гр. Рассчитайте энергию ΔЕ, потерянную маятником за 8 колебаний, если начальная амплитуда А0=20 см. 12. Масса движущейся частицы увеличилась в 1,5 раза. Какую скорость имеет частица? Какая относительная ошибка будет допущена, если кинетическую энергию частицы в этих условиях рассчитывать классическим образом? 13. Вычислить плотность газа, для которого наиболее вероятная скорость молекул при нормальном атмосферном давлении составляет 400 м/с. 14. Определите число молекул и количество молей воды в бутылке вместимостью 0,33 л 15. Сжатый азот, имевший первоначально температуру 400 К, сначала очень быстро(адиабатически) расширили до объема 7 л, а затем очень медленно(изотермически), сжали. В обоих процессах давление из-менялось в 4 раза. Найти: 1) объемы газа в начальном и конечном состоя-ниях; 2) изменение средней арифметической скорости молекул азота в адиабатическом процессе. 16. Кислород, находящийся при давлении 0,5 МПа и температу- ре 350 К, подвергли сначала изотермическому	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		расширению от объема 1 л до объема 2 л, а затем изобарному расширению, в результате которого объем газа увеличился до 3 л. Определить:1) работу, совершенную газом; 2) изменение его внутренней энергии; 3) количество подведенной теплоты 17. Азот нагревался при постоянном давлении. Ему было сообщено количество теплоты Q = 21 кДж. Определить работу A, которую совершил при этом газ, и изменение ΔU его внутренней энергии. 18. Двухатомный идеальный газ совершает процесс, в ходе которого молярная теплоемкость С газа остается постоянной и равной 7R/2. Определите показатель политропы n этого процесса. 19. Идеальный трехатомный газ количеством вещества v = 2 моль занимает объемV_1 = 10 л и находится под давлением p_1 = 250 кПа. Сначала газ подвергли изохорному нагреванию до температуры T_2 = 500 К, затем – изотермическому расширению до начального давления, а после этого в результате изобарного сжатия возвратили в первоначальное состояние. Постройте график цикла и определите термический КПД цикла. 20. В котле паровой машины температура равна 400 К, а температура холодильника 300К. Какова теоретически возможная максимальная работа А машины, если в топке сожжено 500кг дров с удельной теплотой сгорания $1{,}26 \cdot 10^7$ Дж/кг 21. Два моля идеального газа сначала изохорически охладили, а затем изобарически расширили так, что температура газа стала равна первоначальной. Найти приращение энтропии газа, если его давление в данном процессе изменилось в n = 3,3 раза. 22. Лед массой m1=2кг при температуре t1=0C° был превращен в воду той же температуры с помощью пара, имеющего температуру t2=100C°. Определить массу m2 израсходованного пара. Каково измене-ние ΔS энтропии системы лед-пар?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Примерный перечень практических заданий для экзамена (2 семестр) 1. Определить напряжённость электростатического поля E в центре квадрата со стороной a, если в трёх вершинах квадрата находятся одинаковые точечные заряды q 2. Тонкая нить согнута в полуокружность и заряжена так, что электрический заряд равномерно распределен по ее длине. Каков радиус этой полуокружности, если известно, что в центре ее кривизны напряженность поля 10 кВ/м, а потенциал 630 В. 3. На рис. ε1=1,5 В, ε2=3,7 В и сопротивления R1=10 Ом, R2=20 Ом и R=5,0 Ом. Внутренние сопротивления источников пренебрежимо малы. Определите: 1) значение и направление тока через сопротивление R; 2) тепловую мощность, которая выделяется на сопротивлении R.?  4. Каким должно быть сопротивление R электрической цепи, изображенной на рисунке, чтобы ток, текущий по нему был равен I=0,5 А, если C=5 мкФ, U=200 В, частота переменного тока ν=100 Гц?  5. Ток I=100A течет по тонкому проводнику, изогнутому так,	

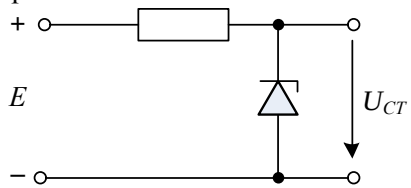
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		как показано на рисунке. Найти индукцию B магнитного поля в точке O контура, если радиус изогнутой части проводника R=0,1 м, а сторона квадрата *a*=0,2 м  6. По двум параллельным прямым проводам длиной *l* = 1 м каждый текут одинаковые токи. Расстояние *d* между проводами равно 1 см. Токи взаимодействуют с силой *F* = 1 мН. Найти силу тока *I* в проводах 7. Катушка состоит из N = 75 витков и имеет сопротивление R= 9 Ом. Магнитный поток через ее поперечное сечение меняется по закону Ф = kt , где k= 1,2 мВб/с. Определите: а) э.д.с. индукции, возникающую в этом контуре; б) силу индукционного тока; в) заряд, который протечет по контуру за первые 9 с изменения поля. 8. Электрон, ускоренный напряжением U=200 В, влетает в однородное магнитное поле с индукцией B=0,7·10-4 Тл перпендикулярно силовым линиям. Найти радиус окружности, по которой движется электрон в магнитном поле и период его вращения. 9. Индуктивность *L* катушки (без сердечника) равна 0,1 мГн. При какой силе тока *I* энергия *W* магнитного поля равна 100 мкДж 10. Расстояние между двумя когерентными источниками света(λ=0,5 мкм) равно d=0,1 мм. Расстояние между интерференционными полосами на экране в средней части интерференционной картины равно Δx=1,0 см. Определить расстояние от источников до экрана 11. Плосковыпуклая линза выпуклой стороной лежит на стеклянной пластинке. В отраженном свете с длиной волны	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		λ = 0,6 мкм наблюдается интерференционная картина. Считая, что радиусы интерференционных колец r много меньше радиуса кривизны линзы R=1,2 м, определите: а) толщину слоя воздуха там, где видно первое светлое кольцо Ньютона, б) радиус первого кольца 12. Между двумя плоскопараллельными стеклянными пластинками положили очень тонкую проволочку, расположенную параллельно линии соприкосновения пластинок и находящуюся на расстоянии L=75 мм от нее. В отраженном свете с длиной волны λ=0,5 мкм на верхней пластинке видны интерференционные полосы. Определите диаметр поперечного сечения проволочки, если на протяжении *a* = 30 мм насчитывается m = 16 светлых полос 13. На щель шириной a = 0,05 мм падает нормально монохроматический свет с длиной волны λ = 0,6 мкм. Определить угол φ между первоначальным направлением пучка света и направлением на четвертую темную дифракционную полосу 14. Дифракционная решетка установлена на расстоянии 80 см от экрана. На решетку падает монохроматический свет с длиной волны 0,65 мкм. На экране расстояние между максимумами первого и второго порядка равно 5,2 см. Сколько всего максимумов образует эта дифракционная решетка? 15. Какую трубку с раствором сахара (C·ℓ) необходимо поставить между двумя скрещенными поляризаторами, чтобы интенсивность света, вышедшего из второго поляризатора оказалась в 3 раза меньше интенсивности естественного света, падающего на первый поляризатор? Считать, что удельное вращение раствора равно 6,23 град/(% ·м), Трубка поглощает 15% проходящего через нее света, поляризаторы прозрачны 16. Определить, во сколько раз уменьшится интенсивность света, прошедшего через два поляризатора, расположенные так, что угол между их главным плоскостями α = 60°, а в каждом из поляризаторов теряется 8% интенсивности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		падающего на него света	
Владеть	опытом анализа происходящих физических явлений и процессов и решения типовых и более сложных физических задач	**Примерный перечень практических заданий для зачета (3 семестр)** 1. Черное тело нагрели от температуры 600К до 2400К. Во сколько раз увеличилась общая тепловая энергия, излучаемая телом? На сколько изменилась длина волны, соответствующая максимуму энергии излучения и спектральный состав излучения? 2. Определить наименьший задерживающий потенциал, необходимый для прекращения эмиссии с поверхности фотокатода, если он освещается излучением с длиной волны 0,4 мкм, а красная граница для материала катода равна 0,67 мкм 3. Фотон с энергией 1 МэВ рассеялся на свободном покоившемся электроне. Найти кинетическую энергию электрона отдачи, если в результате рассеяния длина волны фотона изменилась на 25% 4. При движении частицы вдоль оси x скорость ее может быть определена с точностью (ошибкой) до 1 см/с. Найти неопределенность координаты, если частицей является: 1) электрон, 2) дробинка массой 0,1г 5. Собственная функция, описывающая состояние микрочастицы в бесконечно глубокой потенциальной яме шириной ℓ, имеет вид — . Используя условия нормировки, определить постоянную *C*. 6. Вычислить радиусы первых трех орбит электрона в атоме водорода 7. Найти наибольшую и наименьшую длины волн серии Пашена в спектре излучения водорода. Сравнить полученные значения с длинами волн видимого излучения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		8. Первоначальная масса изотопа иридия $^{192}_{77}Ir$ равна m = 5 г, период полураспада 75 суток. Определите, сколько ядер распадется за 1 секунду в этом препарате. Сколько атомов этого препарата останется через 30 суток и во сколько раз изменится активность препарата за это время? 9. В центре Солнца протекает термоядерная реакция синтеза гелия из водорода, в которой из четырех протонов образуется ядро He^4 и два позитрона. Запишите эту реакцию. Какие еще частицы образуются в ней? 10. Какое количество U^{235} «выгорает» за год в ядерном реакторе с электрической мощностью 1 ГВт и к.п.д. 38%? Считать, что распад ядер урана под действием тепловых нейтронов приводит к образованию изотопов ксенона-141, стронция-92 и трех вторичных нейтронов.	
Знать	– Математические методы расчёта электрических цепей, теорию четырёхполюсников, Фурье преобразование и преобразования Лапласса, основы цифровой обработки сигналов	– Что такое делитель напряжения – В чём заключается анализ цепей методом контурных токов – В чём заключается анализ цепей методом узловых потенциалов – Что такое волновое сопротивления и волновая нагрузка – Что такое «длинная линия» – Что такое «стоячая волна» – Какие типы фильтров вы знаете – Что такое АЧХ и ФЧХ – Что такое спектр сигнала – Что такое ряд Фурье – Что такое интеграл Фурье – В чём заключается преобразование Лапласа – Что такое p-n переход – Принцип работы диода. Основные характеристики – Принцип работы биполярного транзистора. Основные параметры – Принцип работы полевого транзистора. Основные параметры	Б1.Б.22Электроника и схемотехника

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– Что такое обратная связь – Схемы на основе ОУ – Что такое «таблица истинности» – Какие логические элементы вы знаете – Для чего используются карты Карно – Что такое комбинационная логическая схема – Что такое последовательностная логическая схема – Что значит синхронная цифровая схемы – Каковы основные характеристики АЦП – Что такое частота дискретизации – Объясните теорему Котельникова –	
Уметь	– Рассчитывать электрические цепи, рассчитывать параметры четырёхполюсников, рассчитывать параметры и характеристики фильтров и усилителей сигналов, рассчитывать процессы в длинных линиях, рассчитывать схемы на операционных усилителях, рассчитывать цифровые схемы	– Какой ток протекает в цепи, состоящей из последовательно соединенных источника напряжения с напряжением 5 В, источника тока с током 1 мА и резистора с сопротивлением 1 кОм? Какое напряжение возникнет на резисторе? – Составьте дифференциальное уравнение цепи с параллельно соединенными источником тока, резистором, конденсатором и катушкой индуктивности. – Реальный источник сигнала, состоящий из последовательно соединенных идеального источника гармонического напряжения с амплитудой 5 В и резистора (внутреннего сопротивления) с сопротивлением 1 кОм, подключен к внешней нагрузке с сопротивлением 2 кОм. Используя теорему об эквивалентном генераторе, рассчитайте параметры дополнительного эквивалентного источника тока, подключаемого к нагрузке, который обеспечивает полную компенсацию сигнала от первого источника. – По какому закону изменяется амплитуда бегущей волны в линии с потерями? Рассчитайте уменьшение падающей волны в линии длиной 100 м, если коэффициент затухания $\alpha = 0,05$ 1/м. – Как изменяется начальная фаза бегущей волны вдоль линии, если коэффициент фазы $\beta = 2\pi 10\text{-}2$ рад/м? Каковы длина волны в длинной линии и фазовая скорость распространения волны, если частота сигнала равна 20 МГц?	

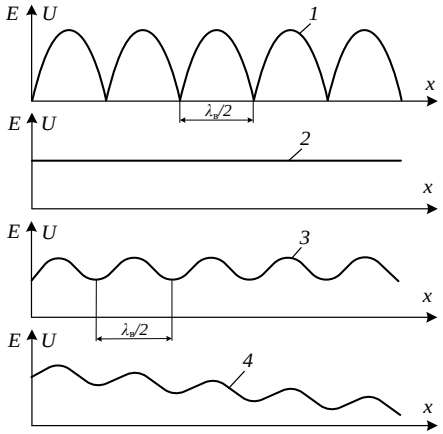
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– Нарисуйте амплитудный и фазовый спектры гпрмонического сигнала с амплитудой 1 В, частотой 2 кГц и начальной фазой 45о. Как изменятся эти спектры, если амплитуда сигнала уменьшится в два раза? – В источниках питания ЭВМ для стабилизации напряжения используются стабилитроны. Как работает схема стабилизации напряжения, приведенная на рисунке? Как изменится напряжение стабилизации, если последовательно соединить два стабилитрона? Почему не рекомендуется параллельное соединение двух стабилитронов?  – Используя эквивалентную схему усилителя ОЭ в области средних частот, нарисуйте эквивалентную схему этого усилителя в области низких частот. Какие конденсаторы нужно учесть в этой схеме? – Рассчитайте амплитуду напряжения на выходе умножителя частоты в два раза, выполненного на аналоговом перемножителе, если коэффициент k перемножителя равен 0,1, а амплитуда входного сигнала равна 2 В. – Рассчитайте частоту колебаний автогенератора с линией задержки в цепи ПОС. ФЧХ линии задержки равна $\varphi(\omega) = -\tau\omega$, где время задержки $\tau = 10$ мкс. Усилитель автогенератора вносит фазовый сдвиг равный 180о. Баланс амплитуд выполняется только для самой низкой частоты колебаний: на высоких частотах коэффициент усиления усилителя быстро уменьшается. – Постройте схему четырехразрядного суммирующего двоичного счетчика с модулем, равным 12. – Нарисуйте схему трехразрядного вычитающего счетчика с показаниями, изменяющимися от 7 до 2. – Как с помощью элементов И, ИЛИ, НЕ можно построить реверсивный трехразрядный счетчик? – Нарисуйте временную диаграмму записи в трехразрядный	

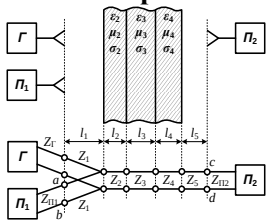
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		последовательный регистр двоичного кода, равного 101. Какой из регистров – последовательный или параллельный имеет большее быстродействие? – Рассчитайте частоту дискретизации последовательности прямоугольных импульсов с амплитудой 5 В, длительности импульса τ = 1 мс, периодом повторения импульсов T = 5 мс. Верхняя граничная частота этого сигнала определяется уровнем шума с амплитудой, равной 10 мВ. – Рассчитайте среднеквадратичное значение шума квантования в десятиразрядном АЦП, если этот АЦП преобразовывает напряжение в диапазоне от 0 до UМАКС = 10 В. Важным параметром цифровых систем воспроизведения звука является динамический диапазон, рассчитываемый по формуле D = 20lg(UД/σ), UД – максимальное действующие значение гармонического сигнала, равное 0,707(UМАКС/2), σ – среднеквадратичное значение шума квантования. Для высококачественных цифровых систем динамический диапазон D не должен быть хуже 86 дБ. Отвечает ли рассматриваемый АЦП этим требованиям?	
Владеть	– Навыками проектирования схем аналоговой и цифровой электроники для обработки информации	– Рассчитайте среднюю величину потребляемого тока одним транзистором микропроцессора, содержащего 10 миллионов транзисторов и потребляющего от источника питания с напряжением 2 В мощностью 5 Вт. Почему современные микропроцессоры имеют пониженное напряжение питания и почему в них, в основном, используются полевые транзисторы? – В каком случае влияние распределенных параметров в длинной линии при прочих равных условиях больше: при увеличении в 2 раза частоты сигнала или при увеличении в 2 раза длины линии? – Где больше модуль коэффициента отражения в линии с потерями: в сечении нагрузки или на входе линии? – Отраженная волна взаимодействует с третьей частью падающей волны в линии с малыми потерями с резистивной нагрузкой. Нарисовать распределение амплитуды напряжения смешанной волны вдоль линии. Рассчитать КСВ и КБВ. – Докажите ортогональность гармонической базисной системы. Рассчитайте нормы сигналов, составляющих гармонический базис. Является ли гармонический базис ортонормированным базисом?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– Почему сумма комплексных составляющих ряда Фурье дает в результате вещественный сигнал? – Докажите, что спектральная плотность сигнала на отрицательных частотах комплексно сопряжена с ее значениями на положительных частотах. – Объясните причину появления помех в работе переносного радиоприемника, если его близко расположить от компьютера. Как изменится уровень этих помех, если приемник переключить на более высокочастотный диапазон? – Во сколько раз надо увеличить сопротивление нагрузки, чтобы получить двукратное увеличение коэффициента усиления в каскадах ОЭ и ОБ? Чем ограничивается величина сопротивления нагрузки в этих усилителях? – Можно ли для детектирования АМ-сигналов использовать транзисторы? Как нелинейный усилитель превратить в амплитудный детектор? – Сравнивая схемы элемента ТТЛ и КМДП логического элемента, назовите причины, по которым в микропроцессорах используются элементы на полевых транзисторах. – Можно ли собрать JK-триггер на основе асинхронного RS-триггера? – Объясните возникающий при просмотре кинофильмов эффект вращения колеса в обратную сторону (или остановки вращения) при движении автомобиля, если известна частота смены кадров при съемке. – Как можно уменьшить шум квантования при программной реализации на ЭВМ цифровой обработки сигналов? – Каким будет сигнал на выходе цифрового ФНЧ первого порядка, если на его вход ошибочно, нарушая условия Котельникова, подать гармонический сигнал с частотой больше, чем половина частоты дискретизации? Нарисуйте график входного и выходного сигналов.	
Знать:	Физические основы функционирования систем обработки и передачи информации. Основные физические явления и законы, используемые при построении средств защиты	**Вопросы для зачета** 1. Направленные и лазерные микрофоны. 2. Типы микрофонов и их характеристики. 3. Закладные устройства и их характеристики.	Б1.Б.29Техническая защита информации

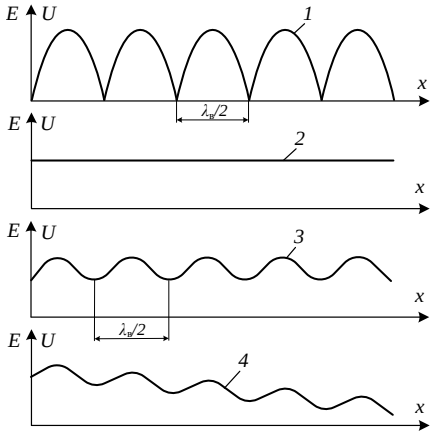
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информации от утечки по техническим каналам. Технические каналы утечки информации.	4. Требования защиты информации. 5. Методы и средства защиты речевой информации. 6. Физические АЭП - преобразователи – источники опасных сигналов. 7. Характеристики технических каналов утечки информации. 8. Пассивные и активные методы защиты информации в акустическом канале. 9. Материально-вещественные каналы утечки информации. 10. Акустические каналы утечки информации.	
Уметь:	Применять соответствующий математический аппарат при проведении расчетов защищенности информации Контролировать безотказное функционирование технических средств защиты информации. Заменять отказавшие технические средства защиты информации.	Задания: 1. Проверить работоспособность генератора шума ГШ-1000М для защиты информации от утечки за счёт побочных электромагнитных излучений. 2. Проверить работоспособность устройства защиты Прокруст 2000. 3. Проверить работоспособность устройства для подавления сигнала сотовой связи.	
Владеть:	Навыками работы с нормативными правовыми актами в области технической защиты информации. Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.	1. С использованием графического метода рассчитать радиус зоны R2 для ЭВТ. 2. Рассчитать показатель защищенности технических средств обработки и передачи цифровой речи по каналу ПЭМИ. 3. Рассчитать показатель защищенности цифровой речи в радиоканале. 4. Для представленной схемы помещения выбрать контрольные точки (КТ) и разработать схемы измерений по акустическому каналу для этих КТ. 5. Проанализировать математическую модель утечки речевой информации по акустическому каналу. 6. Проанализировать математическую модель утечки речевой информации по виброакустическому каналу. 7. Проанализировать математическую модель утечки речевой информации по каналам, использующим перехват электромагнитных и электрических сигналов. 8. Проанализировать математическую модель утечки речевой информации по лазерному каналу.	
Знать	– физическую сущность процессов,	**Типовые вопросы к экзамену:**	Б1.В.ДВ.01.01 Основы

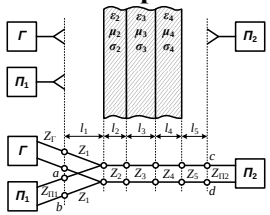
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	происходящих в системах передачи информации в целом; – физическую сущность процессов, происходящих в отдельных узлах систем передачи информации; – физическую сущность процессов, происходящих в элементах узлов систем передачи информации.	1. Виды радиотехнических систем передачи информации. 2. Особенности использования радиочастотного спектра. 3. Таблицы радиочастот. Особенности распространения и использования радиоволн СВЧ-диапазона. 4. Таблицы радиочастот. Особенности распространения использования радиоволн УКВ-диапазона. 5. Таблицы радиочастот. Особенности распространения и использования радиоволн КВ-диапазона. 6. Таблицы радиочастот. Особенности распространения и использования радиоволн СВ-диапазона. 7. Таблицы радиочастот. Особенности распространения и использования радиоволн ДВ и СДВ-диапазона. 8. Детектирование высокочастотных колебаний. Детекторные каскады приемников. 9. Сигналы в радиотехнике. Классификация, физические характеристики. 10. Радиопомехи и способы борьбы с ними. 11. Линии связи. Разновидности каналов связи. Провода, коаксиальные кабели, волноводы, волоконно-оптический кабель, радиоволны различного диапазона. 12. Электрические фильтры. Назначение и характеристики. 13. Фильтры источников питания постоянного тока. 14. Фильтры нижних частот (ФНЧ). Назначение и характеристики. 15. Фильтры верхних частот (ФВЧ). Назначение и характеристики. 16. Полосовые и заградительные фильтры. **Типовые вопросы к зачету** 1. Спектры периодических сигналов. 2. Спектры непериодических колебаний. 3. Характеристики случайных сигналов и помех. 4. Системы производственной радиосвязи. 5. Системы сотовой радиосвязи. 6. Системы радиорелейной радиосвязи. 7. Системы транкинговой радиосвязи. 8. Системы спутниковой связи.	радиотехники

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		9. Антенны узкополосных сигналов. 10. Антенны широкополосных сигналов. **Типовое практическое задание** Поясните характер распространения УКВ-радиоволн в различных режимах (см. рисунок)  Рассчитайте волновое сопротивление длинной линии согласно исходным данным (задаются преподавателем): $\underline{Z} = \dfrac{\underline{Z}_{\text{н}} + j\underline{Z}_{\text{л}}\text{tg}2\pi\dfrac{l_{\text{ни}}}{\Lambda}}{\underline{Z}_{\text{л}} + j\underline{Z}_{\text{н}}\text{tg}2\pi\dfrac{l_{\text{ни}}}{\Lambda}}$ Приведите условия, при которых реализуется режим 2 (см. рисунок).	
Уметь:	– разрабатывать модели процессов, происходящих в системах передачи информации в целом; – разрабатывать модели процессов, происходящих в отдельных узлах систем передачи информации; – разрабатывать модели процессов, происходящих в элементах узлов систем передачи информации.	**Типовые вопросы к защите тем:** Виды сигналов и помех в телекоммуникационных системах и их математические модели. Каналы связей и их математические модели: 1. Определение понятия «канал» в теории связи в зависимости от рассматриваемых сечений при связи «точка-точка». 2. Связь с понятиями модели OSI. 3. Концептуальные модели каналов. 4. Основные математические модели физических и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационных каналов. 5. Показатели качества каналов передачи информации. 6. Каналы связей. 7. Первичные сети и каналы связей. 8. Аппаратура линий связи. 9. Характеристики линий связи. 10. Пропускная способность каналов. 11. Способы передачи данных. 12. Аналоговая модуляция. 13. Дискретная (цифровая) модуляция. 14. Способы цифрового кодирования данных. 16. Методы синхронизации. 17. Методы обнаружения искажений **Типовое практическое задание**  Разработайте импедансную модель распространения сигнала СВЧ-диапазона через трехслойный диэлектрический объект (см. рисунок) с известными геометрическими и электромагнитными характеристиками.	
Владеть	− математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом; − математическим аппаратом для описания процессов, происходящих в отдельных узлах систем передачи информации; − математическим аппаратом для описания процессов, происходящих в элементах узлов систем передачи информации.	**Типовые вопросы к защите тем:** 1. Методы мультиплексирования и демультиплексирования сигналов, основанные на частотном разделении. 2. Методы мультиплексирования и демультиплексирования сигналов, основанные на временном разделении. 3. Методы мультиплексирования и демультиплексирования сигналов, основанные на кодовом разделении. 4. Синхронная цифровая иерархия (SDH). 5. Синхронный (STM) режим передачи в цифровых сетях. 6. Эталонная модель взаимосвязи открытых систем (модель OSI).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		7. Телекоммуникационные сети с маршрутизацией информации (узловые сети). 8. Коммутация каналов. 9. Коммутация сообщений. 10. Способы коммутации пакетов. 11. Задержки, потери и перегрузки в сетях с пакетной коммутацией. 12. Управление потоками в сетях пакетной коммутации. 13. Интеграция и конвергенция цифровых телекоммуникационных сетей. 14. Основные и дополнительные услуги связи. 15. Цифровые сети с интеграцией служб (ISDN). 16. Концептуальные модели каналов. 17. Показатели качества каналов передачи информации.	
Знать	– физическую сущность процессов, происходящих в системах передачи информации в целом; – физическую сущность процессов, происходящих в отдельных узлах систем передачи информации; – физическую сущность процессов, происходящих в элементах узлов систем передачи информации.	**Типовые вопросы к экзамену:** 1. Виды радиотехнических систем передачи информации. 2. Особенности использования радиочастотного спектра. 3. Таблицы радиочастот. Особенности распространения и использования радиоволн СВЧ-диапазона. 4. Таблицы радиочастот. Особенности распространения использования радиоволн УКВ-диапазона. 5. Таблицы радиочастот. Особенности распространения и использования радиоволн КВ-диапазона. 6. Таблицы радиочастот. Особенности распространения и использования радиоволн СВ-диапазона. 7. Таблицы радиочастот. Особенности распространения и использования радиоволн ДВ и СДВ-диапазона. 8. Детектирование высокочастотных колебаний. Детекторные каскады приемников. 9. Сигналы в радиотехнике. Классификация, физические характеристики. 10. Радиопомехи и способы борьбы с ними. 11. Линии связи. Разновидности каналов связи. Провода, коаксиальные кабели, волноводы, волоконно-оптический кабель, радиоволны различного диапазона. 12. Электрические фильтры. Назначение и характеристики.	Б1.В.ДВ.01.02 Физические основы передачи информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		13. Фильтры источников питания постоянного тока. 14. Фильтры нижних частот (ФНЧ). Назначение и характеристики. 15. Фильтры верхних частот (ФВЧ). Назначение и характеристики. 16. Полосовые и заградительные фильтры. **Типовые вопросы к зачету** 1. Спектры периодических сигналов. 2. Спектры непериодических колебаний. 3. Характеристики случайных сигналов и помех. 4. Системы производственной радиосвязи. 5. Системы сотовой радиосвязи. 6. Системы радиорелейной радиосвязи. 7. Системы транкинговой радиосвязи. 8. Системы спутниковой связи. 9. Антенны узкополосных сигналов. 10. Антенны широкополосных сигналов. **Типовое практическое задание** Поясните характер распространения УКВ-радиоволн в различных режимах (см. рисунок)  Рассчитайте волновое сопротивление длинной линии согласно исходным данным (задаются преподавателем):	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		$$\underline{Z} = \frac{\underline{Z}_{н} + j\underline{Z}_{л}\mathrm{tg}2\pi\frac{l_{ни}}{\Lambda}}{\underline{Z}_{л} + j\underline{Z}_{н}\mathrm{tg}2\pi\frac{l_{ни}}{\Lambda}}$$ Приведите условия, при которых реализуется режим 2 (см. рисунок).	
Уметь:	− разрабатывать модели процессов, происходящих в системах передачи информации в целом; − разрабатывать модели процессов, происходящих в отдельных узлах систем передачи информации; − разрабатывать модели процессов, происходящих в элементах узлов систем передачи информации.	**Типовые вопросы к защите тем:** Виды сигналов и помех в телекоммуникационных системах и их математические модели. Каналы связей и их математические модели: 1. Определение понятия «канал» в теории связи в зависимости от рассматриваемых сечений при связи «точка-точка». 2. Связь с понятиями модели OSI. 3. Концептуальные модели каналов. 4. Основные математические модели физических и информационных каналов. 5. Показатели качества каналов передачи информации. 6. Каналы связей. 7. Первичные сети и каналы связей. 8. Аппаратура линий связи. 9. Характеристики линий связи. 10. Пропускная способность каналов. 11. Способы передачи данных. 12. Аналоговая модуляция. 13. Дискретная (цифровая) модуляция. 14. Способы цифрового кодирования данных. 16. Методы синхронизации. 17. Методы обнаружения искажений **Типовое практическое задание** 	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Разработайте импедансную модель распространения сигнала СВЧ-диапазона через трехслойный диэлектрический объект (см. рисунок) с известными геометрическими и электромагнитными характеристиками.	
Владеть	− математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом; − математическим аппаратом для описания процессов, происходящих в отдельных узлах систем передачи информации; − математическим аппаратом для описания процессов, происходящих в элементах узлов систем передачи информации.	**Типовые вопросы к защите тем:** 18. Методы мультиплексирования и демультиплексирования сигналов, основанные на частотном разделении. 19. Методы мультиплексирования и демультиплексирования сигналов, основанные на временном разделении. 20. Методы мультиплексирования и демультиплексирования сигналов, основанные на кодовом разделении. 21. Синхронная цифровая иерархия (SDH). 22. Синхронный (STM) режим передачи в цифровых сетях. 23. Эталонная модель взаимосвязи открытых систем (модель OSI). 24. Телекоммуникационные сети с маршрутизацией информации (узловые сети). 25. Коммутация каналов. 26. Коммутация сообщений. 27. Способы коммутации пакетов. 28. Задержки, потери и перегрузки в сетях с пакетной коммутацией. 29. Управление потоками в сетях пакетной коммутации. 30. Интеграция и конвергенция цифровых телекоммуникационных сетей. 31. Основные и дополнительные услуги связи. 32. Цифровые сети с интеграцией служб (ISDN). 33. Концептуальные модели каналов. 34. Показатели качества каналов передачи информации. **Типовая задача** В короткозамкнутом коаксиальном кабеле с волновым сопротивлением 75 Ом на расстоянии 5 м от короткозамкнутого конца кабеля проходит ток с амплитудой 100 мА. Определить амплитудные значения напряжения и тока на расстояниях 0,21; 0,47; 1,83; 2,5 и 3,5 м от короткозамкнутого конца кабеля при длине волны	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		2,5 м и построить графики (временные диаграммы) зависимостей амплитуд тока и напряжения по этим отрезкам.	
Знать	- Основные физические явления и процессы, имеющие отношение к профессиональной деятельности - Физические основы функционирования систем обработки и передачи информации.	***индивидуальное задание на производственную практику:*** *Список индивидуальных тем* 28. Современные средства защиты информации 29. Современные системы компьютерной безопасности 30. Современные криптографические системы 31. Криптоанализ, современное состояние 32. Правовые основы защиты информации 33. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними 34. Технические аспекты обеспечения защиты информации. 35. Атаки на систему безопасности и современные методы защиты 36. Современные пути решения проблемы информационной безопасности РФ 37. Организация центра мониторинга событий на основе современных систем анализа информационной безопасности 38. Информационная безопасность в условиях цифровой экономики Российской Федерации 39. Безопасность сетей беспроводной передачи данных 40. Использование хэш-функций в современном мире и их криптостойкость 41. Проблемы применения средств защиты информации в операционной системе Windows 42. Алгоритмы тестирования генераторов псевдослучайных чисел 43. Система накопления и анализа данных для контроля за инцидентами в сфере информационной безопасности с учетом поведенческого подхода 44. Анализ законодательства в области размещения и использования ИТСНК на территории Российской Федерации 45. Анализ угроз безопасности информации. Возможные организационные меры, применяемые для нейтрализации ряда угроз безопасности информации	Б2.Б.01(У) Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь:	- Определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач - Анализировать физические явления и процессы формализации и решения профессиональных задач		
Владеть:	- основными методами математической формализации - методами анализа физических явлений и процессов при решении профессиональных задач - средствами анализа физических явлений и процессов для формализации и решения профессиональных задач		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		46. Актуальность обеспечения информационной безопасности на промышленных предприятиях 47. Безопасность в мире «Интернета вещей» 48. Безопасность распознавания личности по отпечаткам пальцев 49. Применение искусственных нейронных сетей для выявления инцидентов информационной безопасности 50. Угрозы информационной безопасности при «оплате в одно касание». 51. Анализ нормативной документации, регламентирующей ответственность за утечку сведений, составляющих государственную тайну 52. Математические модели в информационной безопасности 53. Обзор нормативно-правовой базы в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации 54. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований Cookie: принципы работы и безопасность использования	
ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники			
Знать	- основные понятия линейной алгебры и аналитической геометрии - возможности координатного метода для исследования различных геометрических объектов - аналитические способы описания алгебраических структур и геометрических объектов	**Теоретические вопросы для экзамена** 1. Матрицы. Действия над матрицами. 2. Определители матриц, их свойства (любые два с док-вом). 3. Минор, алгебраическое дополнение. Вычисление определителя разложением по строке (столбцу), понижением порядка. 4. Обратная матрица, теорема о существовании и единственности обратной матрицы (док-во). 5. Элементарные преобразования матриц. Эквивалентные матрицы. Ранг матрицы. Свойства ранга. Теорема о рангах эквивалентных матриц (без док-ва). 6. Ступенчатая матрица. Теорема о ранге ступенчатой матрицы (док-во). 7. Системы линейных алгебраических уравнений (СЛАУ)	Б1.Б.11 Алгебра и геометрия

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		(определения: совместной, несовместной СЛАУ, решения СЛАУ). Условия совместности СЛАУ. 8. Матричная запись СЛАУ. Решение СЛАУ с помощью обратной матрицы. 9. Формулы Крамера (вывод). 10. Определенные и неопределенные СЛАУ. Метод Гаусса. 11. Однородные СЛАУ. Фундаментальная система решений. 12. Векторы. Линейные операции над векторами. Коллинеарные и компланарные векторы. Деление отрезка в данном отношении. 13. Скалярное произведение векторов, его свойства. Угол между векторами. Условие перпендикулярности двух векторов. Проекция вектора $\bar{a}$ на вектор $\bar{b}$. Механический смысл скалярного произведения. 14. Скалярное произведение в базисе $\bar{i}, \bar{j}, \bar{k}$ (вывод). 15. Векторное произведение векторов, его свойства. Геометрический и механический смысл векторного произведения. Условие коллинеарности двух векторов. 16. Векторное произведение в базисе $\bar{i}, \bar{j}, \bar{k}$ (вывод). 17. Смешанное произведение векторов, его свойства. Геометрический смысл смешанного произведения. Условие компланарности трех векторов. 18. Смешанное произведение в базисе $\bar{i}, \bar{j}, \bar{k}$ (вывод). 19. Уравнение прямой на плоскости. Способы задания. Основные задачи. 20. Преобразование координат на плоскости: параллельный перенос, поворот. 21. Кривые второго порядка: окружность, эллипс, гипербола, парабола, их геометрические свойства и уравнения. 22. Уравнение плоскости в пространстве. Способы задания. Основные задачи. 23. Уравнение прямой в пространстве. Прямая и плоскость в пространстве. Основные задачи. 24. Поверхности второго порядка: цилиндрические, конические и поверхности вращения.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		25. Классификацияповерхностей второго порядка 26. Приведение уравнения поверхности второго порядка к каноническому виду	
Уметь	- сопоставлять реальную задачу с определенной областью математических знаний, - распознавать возможность аналитического решения задачи, - самостоятельно разрабатывать алгоритм решения задачи, - применять типичные математические модели линейной алгебры и аналитической геометрии в профессиональной деятельности; - корректно обосновывать необходимость предложенного метода решения задачи; - формализовать задачу и находить ее решение, используя свойства математических объектов алгебры и геометрии; - интерпретировать формально (математически) полученный результат	***Примерные практические задания для экзамена:*** 1. Решить систему линейных алгебраических уравнений $\begin{cases} x-4y-2z=-3, \\ 3x+y+z=5, \\ 3x-5y-6z=-7. \end{cases}$ 2. Решить систему линейных алгебраических уравнений $\begin{cases} x+y+z=0, \\ 2x-y-z=0, \\ 3x+4y+z=0. \end{cases}$ 3. Написать уравнение прямой , проходящей через точку $M(\ ,2)$ параллельной прямой $5x+2y+20=0$. 4. Вычислить $\bar{a}\cdot\bar{b}$ и $\bar{a}\times\bar{b}$, если $\bar{a}=(\ ,1,1)$, $\bar{b}=(\ ,2,1)$. 5. Написать уравнение прямой AB, если $A(-1,2)$, $B(\ ,-1)$ 6. Написать уравнение прямой, проходящей через точку $M(\ ,0)$ параллельной прямой $\frac{x-2}{3}=\frac{y-4}{-1}$. 7. Показать, что прямые $2x-y-20=0$ и $-x-2y-3=0$ перпендикулярны. 8. Показать, что прямые $2x-y+4=0$ и $-4x+2y-10=0$ параллельны. 9. Написать уравнение прямой, отсекающей на осях координат отрезки 2 и 3. 10. В какой точке прямая, проходящая через точки А(3,-2) и В(-1,2), пересекает ось Оу. 11. Найти расстояние между прямыми 4x-3y-7=0 и 4x-3y+3=0. 12. Написать канонические и параметрические уравнения прямой, проходящей через точки М(2,1,-1) и К(3,3,-1). 13. Провести прямую через точку А(2,0,-1) перпендикулярно плоскости 3x+4y-z+4=0.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		14. Провести плоскость через точку A(2,0,-1) параллельно плоскости 3x+4y-z+4=0. 15. Провести плоскость через точки A(1,0,2), B(-1,2,0), C(3,3,2). 16. Доказать, что прямые взаимно перпендикулярны: $\frac{x}{1}=\frac{y-2}{-2}=\frac{z}{3}$ и $\begin{cases}3x+y-5z+1=0,\\2x+3y-8z+3=0.\end{cases}$ 17. Доказать, что прямые параллельны: $\frac{x+2}{3}=\frac{y-1}{-2}=\frac{z}{1}$ и $\begin{cases}x+y-z=0\\x-y-5z-8=0\end{cases}$. 18. Найти угол между прямой, проходящей через точку A(-1,0,-5) и точку B(1,2,0), и плоскостью x-3y+z+5=0. 19. Определить тип и построить линию: $x^2-9y^2+2x+18y+73=0$, $2x^2+3y^2-4x+6y-7=0$., $y^2-4x-2y-3=0$, $y=\frac{3x-3}{2x+5}$, $y=-6+\sqrt{4(x-3)^2-100}$ 20. Привести к каноническому виду уравнение поверхности. Определить ее вид. $y^2+2z^2+4xy-4yz-4yz+2=0.$	
Владеть	- методами работы с алгебраическими и геометрическими объектами, - методами построения и изучения математических моделей конкретных явлений и процессов для решения расчетных и исследовательских задач; - практическими навыками доказательства суждениий; - умением теоретически обосновывать	***Примерные прикладные задачи и задания*** **Задача 1.** В каких задачах аналитической геометрии используются квадратичные формы? **Задание 2.** Собственные числа матриц используются для классификации кривых второго порядка и поверхностей второго порядка. Опишите алгоритм. **Задание 3.** Подготовьте доклад на тему: - Кривые третьего порядка; кривые четвертого порядка; трансцендентные кривые.	

<table>
<tr><td>Структурный элемент компетенции</td><td>Планируемые результаты обучения</td><td>Оценочные средства</td><td>Структурный элемент образовательной программы</td></tr>
<tr><td></td><td>выводы;
- математическими методами описания реальных процессов в профессиональной деятельности.</td><td>
Задача 4. Создайте анимационный график, изображающий построение кривых в полярной системе координат
Задача 5. Создайте анимационный график, изображающий построение кривых, заданных параметрически.
Задача 6. Предприятие специализируется по выпуску изделий трех видов: A, B, C; при этом используется сырье трех типов: S_1, S_2, S_3. Нормы расхода каждого вида сырья на единицу изделия каждого вида и объем расхода сырья на 1 день заданы таблицей:
<table>
<tr><td>Вид сырья</td><td colspan="3">Расходы сырья на единицу продукции, усл. ед.</td></tr>
<tr><td></td><td>A</td><td>B</td><td>C</td></tr>
<tr><td>S_1</td><td>2</td><td>3</td><td>1</td></tr>
<tr><td>S_2</td><td>4</td><td>1</td><td>2</td></tr>
<tr><td>S_3</td><td>1</td><td>2</td><td>3</td></tr>
</table>
Найти ежедневный объем выпуска изделий каждого вида.
Получить систему уравнений и решить ее тремя способами: по формулам Крамера, с помощью обратной матрицы и методом Гаусса.

Задача 7. Предприятие выпускает m видов изделий с использованием k видов сырья. Нормы расхода сырья для производства единицы продукции каждого вида даны матрицей $A_{m\times k}$. Стоимость единицы сырья задана матрицей C. Найти затраты каждого вида сырья при заданном плане выпуска Q и суммарные затраты на сырье. Представить результаты с помощью матриц A, C, Q.
$A=\begin{pmatrix}2&8&1&0\\6&7&3&2\\4&5&1&1\\3&3&0&1\end{pmatrix}$ C= (2 3 8) Q=
(20 100 50 100)

Задача 8. Верно ли утверждение: всякую кривую, заданную
</td><td></td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		в полярной системе координат, можно представить аналитически в виде функции в декартовой системе координат. Приведите доказательство . **Задача 9**. Изучите способы описания поверхностей в цилиндрической и сферической системах координат. **Задача 10**. Когда у однородной системы линейных алгебраических уравнений существует отличное от нулевого решение? Зачем нужна фундаментальная система решений?	
Знать	- основные положения теории пределов функции; - основные теоремы дифференциального и интегрального исчисления функций одной и нескольких переменных, - основные понятия теории функций комплексной переменной; - основные методы решения обыкновенных дифференциальных уравнений - основные понятия теории числовых и функциональных рядов	**Теоретические вопросы для экзамена** 1. Функция. Способы задания. Область определения. Основные элементарные функции, их свойства, графики. 2. Предел функции в точке. Предел функции в бесконечности. Односторонние пределы. 3. Бесконечно малые и бесконечно большие функции, связь между ними. Свойства бесконечно малых функций. 4. Теоремы о пределах. Раскрытие неопределенностей. 5. Замечательные пределы. 6. Сравнение бесконечно малых функций. Эквивалентные бесконечно малые функции и основные теоремы о них. Применение к вычислению пределов. 7. Непрерывность функции в точке. Точки разрыва и их классификация. 8. Основные теоремы о непрерывных функциях. Свойства функций непрерывных на отрезке. 9. Производная функции, ее геометрический и физический смысл. 10. Уравнения касательной и нормали к кривой. Дифференцируемость функции в точке. 11. Производная суммы, разности, произведения, частного функций. Производная сложной и обратной функций. 12. Дифференцирование неявных и параметрически заданных функций. Логарифмическое дифференцирование. 13. Производные высших порядков. 14. Дифференциал функции. Геометрический смысл дифференциала. Основные теоремы о дифференциалах. 15. Применение дифференциала к приближенным вычислениям. 16. Основные теоремы дифференциального исчисления: Ролля, Лагранжа и Коши.	Б1.Б.12Математический анализ

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		17. Правило Лопиталя. 18. Условия монотонности функций. Экстремумы функций. Необходимое и достаточное условия экстремума функции. 19. Наибольшее и наименьшее значения функции на отрезке. 20. Выпуклость графика функции. Точки перегиба. Необходимое и достаточное условия точек перегиба. 21. Асимптоты графика функции. 22. Первообразная. Неопределенный интеграл и его свойства. Таблица основных интегралов. 23. Основные методы интегрирования: замена переменной и интегрирование по частям. 24. Интегрирование рациональных функций. 25. Интегрирование тригонометрических функций. 26. Интегрирование иррациональных функций. 27. Определенный интеграл как предел интегральной суммы, его свойства. 28. Формула Ньютона – Лейбница. Основные свойства определенного интеграла. 29. Вычисление определенного интеграла (замена переменной, интегрирование по частям). Интегрирование четных и нечетных функций в симметричных пределах. 30. Несобственные интегралы. 31. Геометрические и физические приложения определенного интеграла. 32. Область определения ФНП. Предел, непрерывность. Свойства функций, непрерывных в ограниченной замкнутой области. 33. Частные производные первого порядка, их геометрическое истолкование. 34. Частные производные высших порядков. 35. Дифференцируемость и полный дифференциал функции. 36. Применение полного дифференциала к приближенным вычислениям. Дифференциалы высших порядков. 37. Производная сложной функции. Полная производная. 38. Инвариантность формы полного дифференциала. 39. Дифференцирование неявной функции. 40. Касательная плоскость и нормаль к поверхности. 41. Экстремум функции двух переменных. Необходимое и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		достаточное условие экстремума. 42. Условный экстремум. Метод множителей Лагранжа. 43. Наибольшее и наименьшее значения функции в замкнутой области. **Экзамен во 2 семестре** 44. Двойной интеграл: основные понятия и определения. 45. Геометрический и физический смысл двойного интеграла. 46. Основные свойства двойного интеграла. 47. Вычисление двойного интеграла в декартовых координатах. 48. Вычисление двойного интеграла в полярных координатах. 49. Приложения двойного интеграла. 50. Тройной интеграл: основные понятия, свойства. 51. Вычисление тройного интеграла в декартовых координатах. 52. Замена переменных в тройном интеграле. Вычисление тройного интеграла в цилиндрических и сферических координатах. 53. Геометрический и физический смысл, приложения тройного интеграла. 54. Дифференциальные уравнения: основные понятия. Задачи, приводящие к дифференциальным уравнениям. 55. Теорема существования и единственности решения дифференциального уравнения. 56. Уравнения с разделяющимися переменными. 57. Однородные дифференциальные уравнения 1 порядка. 58. Линейные уравнения. Уравнения Бернулли. 59. Уравнение в полных дифференциалах. 60. Дифференциальные уравнения высших порядков: основные понятия. 61. Уравнения, допускающие понижение порядка. 62. Линейные дифференциальные уравнения высших порядков. Линейные однородные дифференциальные уравнения 2, n-го порядков. 63. Интегрирование ЛОДУ с постоянными коэффициентами. 64. Линейные неоднородные ДУ. Структура общего решения ЛНДУ. 65. Метод вариации произвольных постоянных. 66. Интегрирование ЛНДУ с постоянными коэффициентами и правой частью специального вида.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		67. Системы дифференциальных уравнений. Теорема существования и единственности решения. Метод исключения для решения нормальных систем дифференциальных уравнений. 68. Числовые ряды. Сходимость и сумма ряда. Свойства рядов. 69. Ряд геометрической прогрессии. Необходимый признак сходимости числового ряда. Гармонический ряд. 70. Достаточные признаки сходимости знакоположительных рядов. Признаки сравнения. Признак Даламбера. 71. Достаточные признаки сходимости знакоположительных рядов. Радикальный признак Коши. Интегральный признак Коши. 72. Знакочередующиеся и знакопеременные ряды. Признак Лейбница. Абсолютная и условная сходимость ряда. 73. Функциональные ряды. Область сходимости. Степенные ряды. Теорема Абеля. Радиус сходимости. Свойства степенных рядов. 74. Ряды Тейлора и Маклорена. Разложение функций в степенные ряды. 75. Применение степенных рядов в приближенных вычислениях. 76. Тригонометрические ряды. Определение коэффициентов тригонометрического ряда. Условие разложимости функций в ряд Фурье. 77. Ряды Фурье для четных и нечетных функций. Ряды Фурье для функции произвольного периода. Разложение в ряд Фурье непериодических функций. 78. Комплексные числа. Операции над комплексными числами. 79. Функции комплексной переменной. 80. Производная ФКП 81. Интеграл от ФКП 82. Степенные ряды с комплексными членами. 83. Ряд Тейлора 84. Ряд Лорана. Изолированные особые точки. 85. Элементы теории вычетов **Зачет в 3 семестре**	
Уметь	- решать задачи по изучаемым	***Примерные практические задания для экзамена и***	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	теоретически разделам; - обсуждать способы эффективного решения дифференциальных уравнений и их систем; определять эффективность решения задачи, полученного с помощью численных методов; распознавать эффективные результаты обработки экспериментальных данных от неэффективных	***зачета:*** 1. Вычислите пределы: а) $\lim\limits_{x\to\infty}\frac{1+4x-x^4}{x+3x^2+2x^4}$; б) $\lim\limits_{x\to 0}\frac{3x\cdot\arcsin 2x}{\cos x-\cos^3 x}$; в) $\lim\limits_{x\to 3}\frac{\sqrt{2x-1}-\sqrt{5}}{x-3}$. 2. Найдите $\frac{dy}{dx}$ для функций: а) $y=e^{4x-x^2}$. б) $\begin{cases}x=ctg2t,\\ y=\ln(\sin 2t).\end{cases}$ 3. Вычислить: а) $\sqrt[3]{-\sqrt{3}+i}$, б) $(-i)^{28}$. 4. Найти неопределённый интеграл: а) $\int\sin 3x\cdot\cos 5x dx$, б) $\int\frac{1-\cos x}{(x-\sin x)^2}dx$. в) $\int(2x+5)\cdot e^x dx$. 5. Вычислить определенный интеграл $\int\limits_2^{\sqrt{20}}\frac{xdx}{\sqrt{x^2+5}}$. 6. Вычислить определенный интеграл $\int\limits_0^1 4x\cdot\arcsin x dx$. 7. Найти площадь фигуры, ограниченной линиями: $x=4,\quad y^2=4x.$ 8. Изменить порядок интегрирования $\int\limits_{-2}^{-1}dy\int\limits_{-\sqrt{2+y}}^{0}fdx+\int\limits_{-1}^{0}dy\int\limits_{-\sqrt{-y}}^{0}fdx.$ 9. Вычислить $\iint\limits_D\frac{dxdy}{\sqrt{x^2+y^2}}$, $D: x\le y\le\sqrt{1-x^2}$, $x\ge 0$. 10. Найти и построить область определения функции $u=\sqrt{9-x^2-y^2}+(x-y)^3$. 11. Найти полный дифференциал функции: $z=x^3\ln y-\sin 2xy.$ 12. Найти частные производные первого порядка	

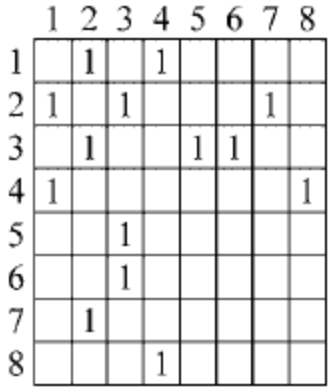
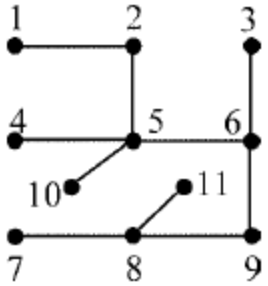
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		функции: $z = 5x^2y^3 + ln(x+4y).$ 13. Написать уравнение касательной плоскости и нормали к поверхности $z = \sqrt{x^2+y^2}$ в точке (3, 4, 5). 14. Исследовать на экстремум функцию $z = x^2 - 2xy + 4y^3$ 15. Решите задачу Коши: $y\cos^2 x\,dy = (y^2+1)\,dx$, $y(0) = 0$. 16. Найдите общее решение дифференциального уравнения . 17. Решить однородную систему дифференциальных уравнений: $\begin{cases} x' = 6x - y, \\ y' = x + 4y. \end{cases}$ 18. Исследовать на сходимость ряд: $\sum_{n=1}^{\infty} \frac{n!(2n+1)!}{(3n)!}$. 19. Разложить в ряд Фурье функцию, периодическую с периодом 4, заданную на отрезке $[-2,2]$ формулой $f(x) = \begin{cases} x^2, -2 \le x \le 0 \\ x, \quad 0 \le x \le 2 \end{cases}$. 20. Вычислить: $\arcsin i$.	
Владеть	- практическими навыками использования математических понятий и методов (изучаемых разделов математики) при решении прикладных задач; - способами оценивания значимости и практической пригодности полученных результатов; -навыками построения и решения математических моделей прикладных задач	***Примерные прикладные задачи и задания*** **Задача 1.** Зависимость пути от времени при прямолинейном движении точки задается уравнением $s = \frac{1}{3}t^3 + 2t^2 - 3$, где s — путь в м, а t — время в с. Вычислите ее скорость и ускорение в момент времени $t = 4c$. **Задание 2.** Составьте алгоритм решения линейного однородного дифференциального уравнения с постоянными коэффициентами.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Задача 3. К графику функции $f(x)=3-x^2$ в его точке с абсциссой $x_0=1$ проведена касательная. Найти площадь треугольника, образованного касательной и отрезками, отсекаемыми ею на осях координат**.** **Задача 4.** Найти центр масс однородного тела $\gamma=1$, ограниченного поверхностями $y^2+z^2\le x\le 2$. **Задача 5.** Найти наибольшее и наименьшее значения функции $z=5x^2+8y-2x+1$ в замкнутой области Д, ограниченной линиями $x=4,\quad y^2=4x.$ **Задание 6.** Подумайте, с помощью средств какого раздела математики можно решить следующую задачу. «Для уборки снега на улицах города используются снегоуборочные машины. Они работают в течение светлого времени суток с 6 до 18 часов с постоянной скоростью уборки снега 400 ($м^3$/ч). Изменение объема снега, выпадающего на улицы города в городе в течение суток, можно описать уравнением $\frac{dS}{dt}=120t-5t^2$, где $S(t)$ – объем снега (в $м^3$), выпавшего за время t (в часах), $0\le t\le 24.$ В момент времени $t=0$ на улицах города лежит 1000 $м^3$ снега. Установите соответствие между временем t и объемом снега, лежащего на улицах города $S(t)$. » Составьте математическую модель этой задачи и решите её.	
Знать	Основные методы исследований, используемых в теории вероятностей и математической статистике Основные законы, правила и определения процессов	Случайные события. Предмет теории вероятностей. Классическое определение вероятности. Геометрическая вероятность. Закон устойчивости относительных частот. Статистическая вероятность. Пространство элементарных событий. Алгебра событий. Аксиомы Колмогорова и следствия из них. Полная группа несовместных событий. Принцип практической уверенности. Теоремы сложения. Условная вероятность. Зависимые и независимые события. Теоремы умножения. Формула полной вероятности. Формула Бейеса. Схема Бернулли. Случайная величина. Закон распределения случайной величины. Дискретные случайные величины, их законы, функции распределения. Плотность	Б1.Б.13Теория вероятностей, математическая статистика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		вероятности непрерывных случайных величин. Свойства плотности вероятности. Математическое ожидание и его свойства. Определение дисперсии, формула для вычисления. Свойства дисперсии. Мода, медиана, асимметрия и эксцесс. Нормальный закон распределения. Правило «трех сигм». Корреляционный момент и его свойства. Коэффициент корреляции и его свойства. Закон больших чисел. Теорема Бернулли. Неравенство Чебышева. Теорема Чебышева и ее применения. Задачи математической статистики. Генеральная совокупность и выборка. Статистическое распределение. Полигон и гистограмма. Эмпирическая функция распределения. Точечные оценки неизвестных параметров распределения. Требования, предъявляемые к точечным оценкам. Статистические проверки статистических гипотез. Ошибки первого и второго рода. Критери проверки статистических гипотез. Критерии значимости и критерии согласия. Критерий согласия Пирсона для проверки гипотезы о нормальном распределении. Выборочный коэффициент корреляции. Корреляционная зависимость, выборочные прямые регрессии. Определение параметров линейной регрессии методом наименьших квадратов	
Уметь	Выделять главное, существенное при решении поставленных задач Обсуждать способы эффективного решения поставленных задач Распознавать эффективное решение от неэффективного Объяснять (выявлять и строить) типичные модели поставленных задач	**1.Тема: Комбинаторика** **Задача 1.** Предприятие может предоставить работу по одной специальности 4 женщинам, по другой - 6 мужчинам, по третьей - 3 работникам независимо от пола. Сколькими способами можно заполнить вакантные места, если имеются 14 претендентов: 6 женщин и 8 мужчин? **2.Формула Бернулли** **Задача 2:** Устройство, состоящее из пяти независимо работающих элементов, включается за время Т. Вероятность отказа каждого из них за это время равна 0,2. Найти вероятность того, что откажут: а) три элемента; б) не менее четырех элементов; в) хотя бы один элемент. **3.Формула полной вероятности** **Задача 3.** Из 1000 ламп 380 принадлежат к 1 партии, 270 – ко второй партии, остальные к третьей. В первой партии 4% брака, во второй - 3%, в третьей – 6%. Наудачу выбирается одна лампа. Определить вероятность того, что выбранная лампа – бракованная.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4.Нормально распределенная случайная величина **Задача 4.** Автоматический токарный станок настроен на выпуск деталей со средним диаметром 2.00 см и со средним квадратическим отклонением 0.005 см. Действует нормальный закон распределения. Компания технического сервиса рекомендует остановить станок для технического обслуживания и корректировки в случае, если образцы деталей, которые он производит, имеют средний диаметр более 2.01 см, либо менее 1.99 см. 1) Найти вероятность остановки станка, если он настроен по инструкции на 2.00 см. 2) Если станок начнет производить детали, которые в среднем имеют слишком большой диаметр, а именно, 2.02 см, какова вероятность того, что станок будет продолжать работать? 3) Производится измерение некоторой физической величины. Случайные ошибки измерения подчинены нормальному закону распределения со среднеквадратическим отклонением, равным 10. Систематические ошибки измерения отсутствуют. (Это означает, что математическое ожидание ошибки равно нулю.) Найти вероятность того, что модуль ошибки измерения меньше 15.	
Владеть	Способностью корректно применять при решении профессиональных задач соответствующий математический аппарат теории вероятностей, математической статистики, в том числе с использованием вычислительной техники.	ЗАДАНИЕ 1. Дан следующий вариационный ряд i 1 2 3 4 5 6 7 8 9 10 x 1 1 2 2 4 4 4 5 5 5 Требуется 1) Построить полигон распределения 2) Вычислить выборочную среднюю, дисперсию, моду, медиану. 3) Построить выборочную функцию распределения 4) Найти несмещенные оценки математического ожидания и дисперсии. Задание 2. Используя критерий Пирсона, при уровне значимости 0,05 проверить, согласуется ли гипотеза о нормальном распределении генеральной совокупности X по результатам выборки: X 0,3 0,5 0,7 0,9 1,1 1,3 1,5 1,7 1,9 2,1 2,3 N 7 9 28 27 30 26 21 25 22 9 5 Задание 3. Имеются данные средней выработки на одного рабочего Y (тыс. руб.) и товарооборота X (тыс. руб.) в 20 магазинах за	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		квартал. На основе указанных данных требуется 1) определить зависимость (коэффициент корреляции) средней выработки на одного рабочего от товарооборота, 2) составить уравнение прямой регрессии этой зависимости. Задание 4. На основании 18 наблюдений установлено, что на 64% вес X кондитерских изделий зависит от их объема Y. Можно ли на уровне значимости 0,05 утверждать, что между X и Y существует зависимость?	
Знать	Основные понятиятеории множеств, булевой алгебры, теории конечных автоматов и графов	Понятие выборки. Выборки упорядоченные и неупорядоченные. Размещения, сочетания, перестановки. Формула бинома Ньютона и следствие из нее. Алгоритм «Сочетания», алгоритм «Сочетания добавлением/изъятием одного элемента». Алгоритмы порождения перестановок: «Индуктивный» и «Транспозиция». Понятие линейного кода. Теорема о числе слов линейного кода. Порождающая и проверочная матрицы линейного кода и их связь. Кодирование линейным кодом. Понятие циклического кода. Порождающая и проверочная матрицы циклического кода. Диодно-резисторные схемы. Контактные структуры: элементы, операции И, ИЛИ, НЕ. Мостиковые и симметрические структуры. Примеры. Структура «чет-нечет». Примеры. Однотактные и многотактные автоматы. Триггеры. Определение графа. Части графа. Подграфы, остовы. Задание неориентированного графа с помощью матриц. Задание ориентированного графа с помощью матриц. Изоморфизм графов. Маршруты, цепи, циклы связного графа. Расстояния в графе. Эйлеровы графы. Критерий эйлеровости. Гамильтоновы графы. Теорема Дирака. Лес и деревья.	Б1.Б.14Дискретная математика
Уметь	Выбирать и применять методы дискретной математики и средства вычислительной техники для решения практических задач	1.По заданной матрице смежности постройте граф и дайте ответы на вопросы. а) укажите степени вершин 3 и 6; б) укажите вершины, степень которых равна 3; в) сколько четных вершин в графе? Укажите ихномера; г) укажите висячие вершины; д) сколько ребер содержит дополнение графа? е) укажите вершины, смежные относительно вершины 4; ж) из заданного графа удалили вершину	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		 1. Сколько в получившемся подграфе ребер? 2.Найдите код дерева методом Пруфера:  3. Используя вычисление идеалов Is, найдите минимальное расстояние для кода Хэмминга [7, 4]2. 4. Пусть F – произвольное поле и f(x) – многочлен положительной степени над F. Докажите, что в кольце F[x]/(f(x)) все идеалы являются главными и порождаются делителями многочлена f(x).	
Владеть	Навыками применения математического аппарата дискретной математики для формализации, анализа и выработки решения профессиональных задач с использованием вычислительной техники	1.Найдите минимальные конъюнктивные нормальные формы булевой функции, зависящей от четырех аргументов и заданной наборами минтермов. В квадратных скобках указаны неопределенные состояния. В ответе укажите число вхождений аргументов минимальной КНФ и число знаков дизъюнкции: $\boldsymbol{f} = (0, 8, 9, 10, 11, 12, 13, 14), [1, 2, 7, 15].$ 2.Построить диаграмму Венна для множеств вида $\boldsymbol{A}$ = {0, 1, 2, 4, 5, 8}; $\boldsymbol{B}$ = {1, 2, 3, 4, 7, 9};	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		C* ={2, 3, 4, 5, 6, 9}; *I = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. При помощи полученной диаграммы найдите элементы множества ***P***. а) $P = \bar{A} \cap B \cap C \cup \bar{A} \cap \bar{B} \cap C \cup \bar{A} \cap B \cap \bar{C} \cup \bar{A} \cap \bar{B} \cap \bar{C}$; б) $P = \bar{A} \cap \bar{B} \cap \bar{C} \cup \bar{A} \cap \bar{B} \cap C \cup \bar{A} \cap B \cap \bar{C} \cup A \cap \bar{B} \cap \bar{C}$. 3.Изобразите схему синхронного автомата на шести ***JK***-триггерах. Комбинационная схема, управляющая входами триггеров, реализует систему функций вида: ***JA = B*** 4.Выпишите явно порождающую и проверочную матрицы циклического кода, отвечающего делителю g(x) многочлена x m − 1 над Fq. 5.Задача 4. Разложите многочлен x 7 − 1 на неприводимые множители над полем F2. С помощью циклического кода, отвечающего делителю g(x) = x 3 + x + 1 многочлена x 7 − 1, закодируйте сообщение 1010. Докажите, что данный циклический код эквивалентен коду Хэмминга [7, 4, 3]2. 6. Пусть n = 2m − 1. Докажите, что [n, n − m]2-код Хэмминга эквивалентен бинарному циклическому коду, порождающий многочлен которого является минимальным многочленом некоторого примитивного элемента поля F2m над F2.	
Знать	способы представления и обработки информации с помощью алгоритмов (в том числе, реализованных на современных языках логического программирования), методологию построения математических алгоритмов, методы математического моделирования	1. Формулы алгебры высказываний: определение, примеры, классификация. 2. Логическое следование в логике высказываний. Правила пропозиционального вывода. 3. Логическая равносильность формул: определение, примеры, основные теоремы. 4. Нормальные формы: определения и алгоритмы отыскания ДНФ и КНФ. 5. Совершенные нормальные формы: определения и алгоритмы отыскания СДНФ и СКНФ. 6. Минимизация булевых функций. Метод логического куба. 7. Минимизация булевых функций. Метод Карно. 8. Булевы функции *n* аргументов.	Б1.Б.15Математическая логика и теория алгоритмов

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		9. Логическое следование формул. 10.Замкнутые классы булевых функций. Примеры. 11.Представление булевых функций полиномом Жегалкина 12.Классы булевых функций. Полные системы Условие полноты булевых функций. Безизбыточные системы. Примеры 13.Системы булевых функций. Базис булевых функций. Универсальный базис. 14.Понятие предиката. Классификация предикатов. Множество истинности предиката. 15.Понятие предиката. Равносильность и следование предикатов. 16.Синтаксис логики предикатов. Кванторы. Связанные и свободные переменные. 17.Формулы логики предикатов Логические операции над предикатами. 18.Кванторные операции над предикатами. взаимосвязь кванторов отрицания и квантора всеобщности 19.Нормальная форма предиката. Предваренная нормальная форма предиката. Пример приведения предиката к нормальной форме 20.Метод резолютивного вывода. Использование метода в языках логического программирования. Примеры 21.Алгоритмическая разрешимость. Теорема Тьюринга. Алгоритмически неразрешимые задачи 22.Машины Тьюринга: определение, применение к словам. 23.Нормальные алгоритмы Маркова. 24.Классификация задач по степени сложности. Примеры 25.Примитивно рекурсивные функции. Примеры. Определение вычислимости через представление функции в виде примитивной рекурсии. Общерекурсивные функции 26.Частично рекурсивные функции. Базисные функции. Формализация Геделя и Клини 27.Связь между общерекурсивными и частично рекурсивными функциями 28.Алгоритмические механизмы представления функции в рекурсивном виде. 29.Детерминированная машина Тьюринга. Представление алгоритмов : графы, таблицы перехода, списки перечисления состояний.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		30.Принцип резолюций в логике высказываний. 31.Формальные языки и грамматики. Классификация. 32.Неклассические логики. Истокивозникновения. 33.Нечеткая логика. Основные определения. Область применения. 34.Понятие алгоритма. Основные свойства алгоритмов. Эффективные алгоритмы. 35.Машины Тьюринга. Диаграммы Тьюринга. 36.Нормальные алгоритмы Маркова. Тезис Черча. 37.Примитивно-рекурсивные функции. Схемы рекурсии. 38.Примеры рекурсивных функций. Рекурсивное описание. 39.Примитивно-рекурсивные множества и предикаты. 40.Меры сложности алгоритмов. 41.Верхние и нижние оценки сложности алгоритмов. 42.Классы задач P и NP. 43.Влияние теории алгоритмов на практику	
Уметь	корректно применять аппарат математической логики для формализации и решения задач в сфере профессиональной деятельности строить математические алгоритмы, используемые при решении задач в конкретных областях знаний. формулировать полученные результаты в терминах предметной области изучаемого объекта. Применять методы верификации программного обеспечения	**Тема 1.2. Задание 2.** Найдите ***СДНФ*** и ***СКНФ*** двумя способами: (↔)→(∧) **Тема 1.3. Задание 3.** Для следующих булевых функций найдите представляющий их полином Жегалкина: ′(′∨ ′)	
Владеть	основными методами математического и алгоритмического моделирования; навыками применения вычислительных методов для решения задач профессиональной деятельности навыками построения эффективных алгоритмов с точки зрения теории вычислимости	1. Используя синтаксис языка Prolog составить предикаты для описания модели «генеалогическое древо» (задать разные имена). Написать предикаты для определения: - Ближайших родственников(дети,родители) - Родственники во втором поколении(внуки, дедушка/бабушка) - Дальние родственники(племянники, дядя/тетя) 2. Составить программу на языке Prolog для решения следующей задачи. Даны два списка целых чисел A1, A2, ..., An и B1, B2, ..., Bn. Объединить эти списки в один, исключить все повторения чисел и упорядочить их по возрастанию.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Знать	- основы теории информации; - способы измерения количественных характеристик информации; - способы измерения качественных характеристик информационных систем; - основные методы эффективного кодирования; - основные методы помехозащищенного кодирования; - основные методы криптографического кодирования.	1. Возникновение теории информации. 2.Системы передачи информации. Основные понятия. 3.Задачи и постулаты прикладной теории информации. 4. Количественная оценка информации. Энтропия . Свойства энтропии. 5. Энтропия при непрерывном сообщении. 6. Условная энтропия. Взаимная энтропия. 7.Избыточность информации. Коэффициенты сжатия и избыточности. 8. Методы архивации. Кодирование символами переменной длинны(алгоритм Хаффмана). 9.Кодирование изображения ,звука и видео (метод Лемпеля - Зива). 10. Эффективное кодирование . Двоично-десятичные коды . Метод Шеннона-Фано. 11. Метод Хаффмана. 12.Кодирование информации для канала с помехами. 13. Разновидность помехоустойчивых кодов . 14. Общие причины использования избыточности . Разрешенные и запрещенные кодовые комбинации. 15. Кодовое расстояние. Матрица расстояний. 16.Исправление одиночных ошибок. Контроль по нечетности (четности). 17. Контроль арифметических операций схемы свертки. 18.Понятие оптимальных кодов. Плотноупакованные коды. 19.Линейные коды. Основные определения. 20. Построение двоичного группового кода. 21.Таблицы опознавателей. Коды Хемминга. 22. Определение проверочных равенств. 23.Максоритарное декодирование групповых кодов. 24.Матричное представление линейных кодов. 25.Технические средства кодирования и декодирования для групповых кодов. 26.Построение циклических кодов. Порождающий многочлен. 27.Обнаружение одиночных ошибок. Исправление одиночных или обнаружение двойных ошибок. 28. Обнаружение ошибок краткости 3.Обнаружение и исправление	Б1.Б.16Теория информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		пачек ошибок. 29. Методы образования циклического кода. 30.Технические средства кодирования и декодирования для циклических кодов.	
Уметь	- применять основные постулаты теории информации; - применять современные методы теории информации для решения практических задач; - применять знания, полученные в ходе освоения дисциплины при работе над междисциплинарными и инновационными проектами; - применять методы эффективного кодирования; - применять методы помехозащищенного кодирования;	1. Выполнять преобразование десятичного числа 56410 в двоично-десятичный код. 2. Выполнять преобразование десятичного числа 22210 в двоичный обратный код. 3. Выполнять преобразование десятичного числа -10010 в двоичный дополнительный код. 4. Получить двоичную запись вещественного числа -333,6610 в формате double-precision IEEE 754. 5. Получить двоичную запись вещественного числа -345,2610 в формате single-precision IEEE 754. 6. Получить 10ти битный код Грея десятичного числа 24210.	
Владеть	- профессиональным языком предметной области знания; - современными методиками кодирования; - навыками создания программ осуществляющих эффективное кодирование текстовой информации; - навыками создания программ осуществляющих помехозащищенное кодирование информации;	1. Закодировать сообщение ABRACATABRA кодом Шеннона. 2. Закодировать сообщение ABRACATABRA кодом Шеннона-Фано 3. Закодировать сообщение ABRACATABRA кодом Хаффмана. 4. Закодировать сообщение ABRACATABRA при помощи арифметического кодирования. 5. Закодировать сообщение ABRACATABRA при помощи динамического алгоритма Хаффмана. 6. Закодировать сообщение ABRACATABRA при помощи адаптивного арифметического алгоритма. 7. Закодировать сообщение ABRACATABRA при помощи алгоритма LZ77. 8. Закодировать сообщение ABRACATABRA при помощи алгоритма LZ78. 9. Закодировать сообщение ABRACATABRA при помощи алгоритма LZSS. 10. Закодировать сообщение ABRACATABRA при помощи алгоритма LZW. 11. Определить значение бита контроля четности при передаче сообщения 10001111002.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		12. Построить код Хэмминга для 8 информационных бит.	
Знать	─ Классификацию современных компьютерных систем; ─ Классификацию системного и прикладного программного обеспечения; ─ Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера.	Вопросы: 1. Перечислите основные классы компьютерных систем и их отличия. 2. Настольные и портативные компьютеры. Основные отличия 3. Распределенные системы и системы реального времени. 4. Системное ПО. Драйверы, утилиты, средства обеспечения компьютерной безопасности. 5. Прикладное ПО. Назначения, категории, требования к операционных системам. 6. Инструментальное ПО. Уровни языков программирования 7. Применения современных редакторов электронных таблиц. Функциональные возможности для проведения исследований 8. Применение современных редакторов текстовых документов. Функциональные возможности для формирования отчетов по проведенным исследованиям 9. Создание макросов. Автоматизированное заполнение таблицы, автоматизированные расчеты. Сохранение документа с поддержкой макроса (MS Excel). 10. Защита данных (MS Access или MS Excel). 11. Информационные системы. Виды ИС. Базы данных. СУБД. Основные понятия реляционных баз данных. Объекты СУБД MS Access. 12. Этапы проектирования базы данных и их процедуры 13. Модель "сущность-связь". Сущность, атрибут, экземпляр сущности, связь, мощность связи, показатель кардинальности, класс принадлежности сущности. 14. Общая характеристика СУБД MS Access. Объекты базы данных MS Access.	Б1.Б.17Информатика
Уметь	─ Пользоваться расчетными формулами, таблицами, компьютерными программами при решении профессиональных задач; ─ Применять офисные приложения (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов) в профессиональной деятельности;	Задания: 1. Построить график функции при заданном коэффициенте a. $z(x)=\begin{cases}\sin(x-a), \textit{если} & x\in[-5;5]\\ \ln(2)-a, \textit{если} & x\in(5;8]\\ \sqrt{\lvert a-x\rvert}, \textit{иначе}\end{cases}$	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	─ Эффективно использовать современные компьютерные технологии для решения профессиональных задач.	2.Дан список средств защиты информации(инв.номер, наименование, стоимость, дата закупки). Произвести амортизацию стоимость на 10% для средств, которые в использовании более 5 лет, на 5% более 2 лет. 3. В таблице представлен список ПК работников организации, ФИО пользователя и кол-во инцидентов информационной безопасности. Определить компьютер с наибольшим кол-вом инцидентов и вывести в отдельную ячейку ФИО пользователя этого ПК используя встроенные библиотеки MS Excel. Произвести расчет среднего кол-ва инцидентов информационной безопасности организации 4. Построить в электронной таблице Excel графики параметрически заданной функции при разных значениях констант a, b, λ. $x = a \cdot cos(\lambda \cdot t) - b \cdot cos(t + \lambda \cdot t)$ $y = a \cdot sin(\lambda \cdot t) - b \cdot sin(t + \lambda \cdot t)$ $t \in 0 \div 10 \cdot \pi$, Шаг 0,5 $a = 0; 1; 2; 3; 10; 15$, $b = 2$, $\lambda = 0.25$. 5. Вычислить определенный и неопределенный интегралы. $\int_{1,2}^{2} \frac{\lg(x+2)}{x} dx$ 6. Решить систему линейных уравнений $\begin{cases} 3{,}21x_1 - 4{,}25x_2 + 2{,}13x_3 = 5{,}03 \\ 7{,}09x_1 + 1{,}17x_2 - 2{,}23x_3 = 4{,}75 \\ 0{,}43x_1 - 1{,}4x_2 - 0{,}62x_3 = -1{,}05 \end{cases}$ 7. Решить систему нелинейных уравнений $\begin{cases} \sin(x+1) - y = 1{,}2 \\ 2x + \cos y = 2 \end{cases}$	
Владеть	─ Навыками работы с реляционными системами управления базами данных при решении профессиональных задач; ─ Навыками проектирования и реализации алгоритмов для решения профессиональных задач;	Задания: 1. Создать базу данных статистики отдела информационной безопасности в СУБД MS Access содержащую информацию об отделах, работниках, персональных ПК и кол-ве инцидентов. Создать запрос для вычисления общего количества инцидентов по	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	─ Навыками создания, отладки и выполнения программ интегрированных сред разработки офисных приложений.	каждому отделу. Определить работника, наиболее часто подвергающего информационную систему предприятия атакам. 2. Дана таблица о количестве атак на серверы предприятия за каждый месяц в течение года. Создать макрос позволяющий выполнить следующее: - Отсортировать серверы в порядке возрастания общего количества атак за год; - Найти месяц с наибольшим средним количеством атак на все серверы. 3. Создать базу данных магазина технических средств защиты информации в СУБД MS Access содержащую информацию заказчиках, оборудовании, продажах. Создать запрос для определения общей суммы продаж указанного оборудования. Вывести список всех заказов указанного заказчика	
Знать	Основные методы исследования операций и теории игр Определения основных понятий, называет их структурные характеристики Основные законы, правила и определения процессов	1. Исследование операций. Примеры задач исследования операций. Основные определения (операция, цель операции, ЛПР, факторы). 2. Исследование операций. Классификация задач исследования операций в зависимости от наличия неконтролируемых факторов. Основные трудности, возникающие в процессе принятия решений. 3. Основные понятия теории игр. Классификация игр. 4. Антагонистические игры. Седловая точка, цена игры, решение антагонистической игры, оптимальные стратегии игроков. Теорема о значении функции выигрыша в ситуациях равновесия. 5. Верхняя и нижняя цены игры. Теорема о верхней и нижней ценах антагонистической игры. 6. Теорема о необходимых и достаточных условиях существования седловой точки. Формулировка теоремы о достаточных условия существования седловой точки для антагонистических игр с выпукло-вогнутой функцией выигрыша. 7. Матричные игры. Ситуации равновесия в матричных играх. Оптимальные смешанные стратегии игроков. Теорема о существовании решения матричной игры в смешанных стратегиях. 8. Критерий решения матричной игры. 9. Активные стратегии. Доминирование стратегий. Теорема о доминировании. 10. Теорема о цене и стратегиях матричной игры, полученной линейным преобразованием исходной. 11. Решение матричных игр 2 □ 2. 12. Решение матричных игр 2 □ m и n □ 2. 13. Сведение матричной игры к задаче линейного программирования. 14. Принятие решения	Б1.Б.18Исследование операций и теория игр

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		в условиях неопределенности. Игры с природой. Критерии Вальда, крайнего оптимизма, Гурвица, Лапласа, Сэвиджа в случае, когда ЛПР максимизирует значение критерия. 15. Принятие решения в условиях неопределенности. Игры с природой. Критерии Вальда, крайнего оптимизма, Гурвица, Лапласа, Сэвиджа в случае, когда ЛПР минимизирует значение критерия. 16. Принятие решений в условиях риска. Критерий математического ожидания, критерий математического ожидания-дисперсии. Использование дерева решений. 17. Основные определения из теории графов. Основные понятия, применяемые в методах сетевого планирования (работа, событие, сетевой график). Правила построения сетевых графиков. Разбивка на слои. 18. Время окончания проекта. Критический путь. Резерв времени событий.	
Уметь	Выделять главное, существенное при решении поставленных задач Обсуждать способы эффективного решения поставленных задач Распознавать эффективное решение от неэффективного	2.Зная платежную матрицу $\begin{Vmatrix} 4 & 5 & 6 & 7 & 9 \\ 3 & 4 & 6 & 7 & 6 \\ 7 & 6 & 10 & 8 & 11 \\ 8 & 5 & 4 & 7 & 3 \end{Vmatrix}$ определить нижнюю и верхнюю цены игры и найти решение матричной игры. 3.Найти оптимальный вариант электростанции по критериям Лапласа, Вальда, Гурвица с показателями 0,8 и 0,3 и Сэвиджа по заданной таблице эффективностей.	
Владеть	Методами исследования операций и теории игр при разработке и исследования моделей информационно-технологических ресурсов Методиками обобщения результатов решения, экспериментальной деятельности	1. Пусть эксперт упорядочивает 5 результатов x1>x2>…..>xn приписав им следующие оценки U0 (x1) □ 7 , U0(x2) □ 4 , U0(x3) □ 2, U0(x4) □1.5, U0 (x5) □1. Рассмотрев возможные варианты выбора, он высказал следующее суждение относительно ценности тех или иных комбинаций результатов: 1) x1 > x2 + x3+ x4 + x5 ; 5) x2 < x3+ x4 + x5 ; 7) x3>x4 + x5 2) x1 < x2 + x3+ x4 ; 6) x2>x3+ x4 ;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		3) x1 < x2 + x3+ x5 ; 4) x1 > x2+x3 Необходимо произвести оценку полезности результатов так, чтобы удовлетворить всем неравенствам, начиная с самого последнего. 2. Дайте геометрическую интерпретацию решения игры для двух игроков. Для проверки геометрического решения проведите также алгебраические расчеты и сравните результаты с полученными геометрическим способом. $A = \begin{matrix} 5 & 8 \\ 9 & 3 \end{matrix}$	
Знать	-Основы применения теории графов при решении задач на ЭВМ Способы классификации и виды графов направления развития теории графов -Новые технологии применения теории графов в моделировании предметных областей -связи теории графов с другими предметами, различные информационные технологии, используемые в теории графов	**Вопросы к зачету** 1. Типы графов. 2. Матрица смежностей. 3. Матрица инцинденций. 4. Как связаны между собой различные способы представления графов? 5. Как от вида или представления графа зависит временная сложность алгоритмов поиска в глубину и в ширину? 6. Как при реализации в коде выполняется возвращение из тупиковых вершин при обходе графа? 7. Как выполняется обход в несвязном графе? 8. Распространяются ли понятия "поиск в глубину" и "поиск в ширину" на несвязный граф? 9. Охарактеризуйте трудоемкость рекурсивного и нерекурсивного алгоритмов обхода графа. 10. Как от представления графа зависит эффективность алгоритма его обхода? 11. За счет чего поиск в ширину является достаточно ресурсоемким алгоритмом? 12. В чем преимущества алгоритмов обхода графа в ширину? 13. Каким образом в алгоритме перебора с возвратом при обходе графа обрабатывается посещение тупиковых вершин? 14. Примеры прикладных задач, реализуемых на основе алгоритма поиска в глубину. 15. Плоские и планарные графы.	Б1.Б.19Теория графов и ее приложения

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		16. Проблемы визуализации графов. 17. Характеризации планарных графов. 18. С какими видами графов работают алгоритмы Дейкстры, Флойда и переборные алгоритмы? 19. Примеры прикладных задач, реализуемых на основе алгоритма поиска в ширину. 20. Каркас графа. Вычисление количества каркасов графа. Матрица Кирхгофа. 21. Фундаментальное множество циклов графа. 22. Маршруты и связность. 23. Экстремальные графы. 24. Операции над графами. 25. Точки сочленения, мосты и блоки. 26. Разбиения. 27. Графические разбиения. 28. Эйлеровы графы. 29. Гамильтоновы графы. 30. Покрытия и независимость.	
Уметь	-Применять методы теории графов при решении задач на ЭВМ -Самостоятельно приобретать знания и применять теорию графов при решении задач на ЭВМ -Классифицировать задачи теории графов по степени сложности и применять соответствующие алгоритмы для решения задач	Задача: 1. Написать программу (C++, Java, Delphi, C#- на выбор), реализовать алгоритмы обхода графа на основе поиска в глубину. 2. На основании приведенной в лекции 1 функции реализуйте программу, в которой выполняется алгоритм обхода графа на основе поиска в ширину.	
Владеть	-Методологическими основами формирования изучения графов и их свойств при исследовании и построении систем -Приемами исследования проблем области теории графов, возникающих в различных сферах человеческой деятельности -Навыками разработки и реализации наилучшего решения для поставленной задачи	Задача: 1. Написать программу (C++, Delphi, Java, C#- на выбор), реализовать алгоритмы *обход графа* в ширину для определения всех *вершин графа*, находящихся на фиксированном расстоянии d от данной вершины. 2. Составить списки смежности для представления заданного неориентированного графа.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	-Навыками решения оптимизационных задач теории графов и задач сетевого планирования		
Знать	• математический аппарат теории информации, теории алгоритмов • процессы генерации простых чисел для систем ассиметричного шифрования • процессы постановки и верификации ЭЦП • математический аппарат шифра скользящей перестановки • принцип работы сети Фейстеля как базовым преобразованием симметричных блочных криптосистем	**Вопросы для зачета** 1. Виды информации, подлежащие закрытию, их модели и свойства. 2. Блочные и поточные шифры. 3. Понятие криптосистемы. 4. Ручные и машинные шифры. 5. Основные требования к шифрам. 6. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок 7. Поточные шифры. Шифры замены. Одноалфавитные и многоалфавитные замены. 8. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. 9. Вопросы криптоанализа простейших шифров замены. 10. Описать процесс работы четырехбитового регистра сдвига с линейной обратной связью.	Б1.Б.27 Криптографические методы защиты информации
Уметь	• корректно применять при решении профессиональных задач математический аппарат теории алгоритмов, теории информации, в том числе с использованием вычислительной техники • реализовывать методы генерации простых чисел средствами вычислительной техники • проводить дешифрование шифра простой перестановки при помощи метода биграмм	• Провести тест Ферма для проверки на простоту больших чисел • Провести тест на простоту с использованием пробных делений • Вычислить 1812 (mod 13); 127(mod 7). • Описать процесс работы четырехбитового регистра сдвига с линейной обратной связью.	
Владеть	• навыками использованием вычислительной техники для реализации криптографических алгоритмов	**Подготовить курсовую работу на тему:** 1. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра маршрутной перестановки. 2. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра двойной перестановки. 3. Разработать программное обеспечение для шифрования и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		дешифрования текста на основе алгоритма Диффи-Хэлмана. 4. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра Цезаря. 5. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра табличной маршрутной перестановки. 6. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра вертикальной перестановки. 7. Разработать программное обеспечение для шифрования и дешифрования текста на основе одноалфавитного шифра подстановки с использованием кодового слова. 8. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра Виженера. 9. Разработать программное обеспечение для шифрования и дешифрования текста на основе алгоритма RSA.	
Знать	Общие положения теории оптимизации; - Основные понятия и методы решения задач оптимизации ─ Способы применения теоретических положений и методов теории оптимизации для постановки и решении профессиональных задач.	Теоретические вопросы 1. Что такое допустимое множество? 2. Что такое критерий оптимизации и целевая функция? 3. Постановка задачи безусловной оптимизации. 4. Необходимые и достаточные условия локального экстремума безусловной оптимизации. 5. Численные методы решения задачи безусловной оптимизации. 6. Постановка гладкой задачи с ограничениями равенствами и неравенствами . 7. 5Необходимые и достаточные условия локального экстремума нелинейного программирования. Принцип Лагранжа. Элементы теории двойственности. Седловая точка.	Б1.В.ДВ.02.01 Основы теории оптимизации
Уметь	Проводить теоретические исследования применения общих положений и методов теории оптимизации; ─ Определять возможности применения теоретических положений и методов теории оптимизации для постановки и решения конкретных прикладных задач; ─ Эффективно использовать и оптимизировать	Решить задачу методом потенциалов с учетом дополнительных ограничений на пропускную способность сети	

<table>
<tr><th>Структурный элемент компетенции</th><th>Планируемые результаты обучения</th><th>Оценочные средства</th><th>Структурный элемент образовательной программы</th></tr>
<tr><td></td><td>свою работу за счет применения общих положений и методов теории оптимизации</td><td>$x_{24} \le 500;\ x_{32} \ge 500$
<table><tr><td>a_i \ b_j</td><td>500</td><td>1000</td><td>500</td><td>1500</td></tr><tr><td>500</td><td>1</td><td>3</td><td>1</td><td>2</td></tr><tr><td>1500</td><td>1</td><td>6</td><td>4</td><td>3</td></tr><tr><td>1000</td><td>2</td><td>5</td><td>3</td><td>4</td></tr><tr><td>1500</td><td>3</td><td>5</td><td>4</td><td>3</td></tr></table></td><td rowspan="2"></td></tr>
<tr><td>Владеть</td><td>Приемами использования соответствующего математического аппарата при решении профессиональных задач;
─ Навыками повышения эффективности работы за счет применения общих положений и методов теории оптимизации.</td><td>Графический метод решения ЗЛП
Минимизируйте функцию $z = -2x_1 - x_2$
при ограничениях $x_1 \ge 0$, $x_2 \ge 0$,
$x_1 + 2x_2 \le 11$,
$x_1 + x_2 \le 6$,
$x_1 - x_2 \le 2$,
$2x_1 - 4x_2 \le 3$.

Решить ЗЛП Симплекс- методом
Найти максимум функции:
$F(x) = -6x_1 - 4x_2 + 4x_3$
при ограничениях:
$\begin{cases} x_1 + x_2 + x_3 \ge -1 \\ -2x_1 - x_2 + x_3 \le 1 \\ x_1 \ge 0, x_2 \ge 0, x_3 \ge 0 \end{cases}$</td></tr>
</table>

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Знать	– теоретические основы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов; – основные принципы и схемы автоматического управления; – основные типы систем автоматического управления, их математическое описание и основные задачи исследования систем с распределенными параметрами.	1. Моделирование зависимости коэффициента нелинейных искажений емкостного микрофона от уровня звукового давления. 2. 2Структурная модель автоматической системы управления интерферометра Фабри-Перо. Исследование с помощью модели переходных процессов и частотных характеристик системы. Анализ устойчивости. 3. Моделирование зависимости интерференционной картины двухщелевого интерферометра от расстояния между щелями и ширины спектральной линии источника света; 4. Моделирование как метод научного исследования. Типы моделей. 5. Особенности имитационного моделирования. Этапы имитационного моделирования. 6. Подходы к построению моделей сложных систем. 7. Экономические системы как пример сложных систем. Особенности моделей экономических систем, цели и задачи их моделирования. 8. Понятие псевдослучайности. Псевдослучайные объекты, используемые в практике моделирования экономических систем. 9. Базовый датчик: критерии качества, используемые методы. Генерация непрерывных случайных величин: метод отбраковки и метод обратной функции. 10. Специальные методы генерации нормально распределённых случайных величин 11. Генерация дискретных случайных величин, выборка с возвращением и выборка без возвращения. 12. Генерация случайных процессов: основные подходы. Генерация Гауссовских процессов.	Б1.В.ДВ.02.02 Математическое моделирование распределенных систем
Уметь	– применять математические методы для анализа общих свойств линейных распределенных систем; – применять методы расчета и исследования систем автоматического управления	1. Воссоздать структурную модель автоматической системы управления интерферометра Фабри-Перо. 2. Произвести исследование с помощью модели переходных процессов и частотных характеристик системы. Выполнить	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	объектами с распределенными параметрами; – применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами на базе современной вычислительной техники и средств автоматизации исследований.	анализ устойчивости. 3. Произвести моделирование зависимости интерференционной картины двухщелевого интерферометра от расстояния между щелями и ширины спектральной линии источника света; 4. Произвести моделирование доски Гальтона (аппроксимации биномиального закона нормальным законом распределения вероятностей). 5. Выполнить генерацию дискретных случайных величин. Сделать выборку с возвращением и выборку без возвращения. 6. Выполнить генерацию случайных процессов. Выполнить генерацию Гауссовских процессов. 7. Выполнить генерацию случайных графов с заданными свойствами. Использовать метод допустимого выбора. 8. Произвести нахождение минимального набора переменных состояния, необходимых для однозначного воспроизведения поведения модели.	
Владеть	– методами преобразования структурных схем распределенных систем управления; – методами преобразования структурных схем распределенных систем управления; – методами и навыками преобразования структурных схем распределенных систем управления.	1. Выполнить моделирование собственных частот и форм (мод) колебаний подвижной системы консольного акселерометра. 2. Выполнить моделирование электростатического поля (скалярного поля потенциала и векторного поля напряженности), создаваемого системой точечных или линейных зарядов. 3. Выполнить моделирование топологии магнитного поля системы линейных токов, например, линий электропередачи 4. Произвести моделирование и оптимизацию потоков в случайных сетях. 5. Произвести решение задачи анализа и оптимизации экономических систем, которые удобно решать на моделях, представленных случайными графами и сетями. 6. Выполнить построение сети Петри для простейшей модели управления запасами на складе готовой продукции. 7. Выполнить построение и анализ графа событий для модели малого производственного предприятия. 8. Произвести генерация случайных графов из заданного класса,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		соответствующего одной из моделей деятельности производственного предприятия.	
ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности			
Знать	Общие принципы построения современных языков программирования высокого уровня. Общие принципы использования современных языков программирования высокого уровня. Язык программирования высокого уровня (объектно-ориентированное программирование).	Теоретические вопросы к экзамену: 1. Компоненты среды программирования. 2. Понятие компилятора. 3. Классификация языков программирования. 4. Виды динамических структур данных. Особенности работы с ними. 5. Универсальная обработка особых ситуаций. 6. Технология работы с файлами в C#. 7. Основные понятия класса. Создание классов.	Б1.Б.20 Языки программирования
Уметь	Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования. Проводить комплексное тестирование и отладку программных систем. Работать с интегрированной средой разработки программного обеспечения. Использовать шаблоны классов и средства макрообработки. Использовать динамически подключаемые библиотеки. Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения. Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования.	1. Создайте приложение под Windows с удобным интерфейсом для организации работы пользователя. 2. В созданном приложении организовать диалог закрытия приложения с сохранением изменения в текстовом редакторе в файл перед закрытием приложения. 3. Заполнить таблицу, в созданном приложении, данными из текстового файла. Размеры таблицы определяются автоматически по количеству записей в файле. Данные в файле хранятся в виде ФИО, данные о количестве продаж в день в течение четырех дней, данные на следующего человека отделяются звездочкой. Вывести Фамилии в порядке возрастания суммарного количества продаж. Вывести суммарные продажи по людям в виде диаграммы. 4. В программе создать класс «Автомобиль», хранящий данные о номере двигателя, заводской цене и марке автомобиля и массив объектов этого класса «Автосалон». Определить метод класса «Автомобиль», увеличивающий заводскую цену на заданные проценты предпродажной подготовки и транспортных издержек. Перегрузив операции «< и >» найти авто с самой высокой ценой. Определить метод для поиска авто по заданным характеристикам. Определить метод, для подсчета количества машин заданной марки. Определить класс с заданными параметрами и создать динамический массив объектов этого	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		класса. Определить свойства доступа к полям и методы класса в соответствии с заданием. Определить перегрузки операторов. Создать статические методы класса Program для заполнения, печати массива объектов и решения заявленных задач.	
Владеть	Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования. Навыками работы с интегрированной средой разработки программного обеспечения. Навыками проектирования программного обеспечения с использованием средств автоматизации.	Задание: Создать Windows-приложение для расчета индекса цифровой грамотности населения (ИЦГН) на основе обработки данных опроса населения (вопросы для опроса необходимо придумать так, чтобы по ним можно было вычислить ИЦГН по 10-ти бальной шкале). ИЦГН рассчитывать как зависимость между 3 показателями: уровень цифровых компетенций, уровень цифрового потребления и уровень цифровой безопасности. Анкету пользователь заполняет с формы приложения. В первом окне пользователь вводит свои данные. Затем появляются вопросы. Вопросы в анкете должны предполагать различные виды ответов: текстовый ответ, выбор, логический выбор, сопоставление.	
Знать	Язык программирования высокого уровня (объектно- ориентированное программирование); Современные технологии и методы программирования; Показатели качества программного обеспечения; Методологии и методы проектирования программного обеспечения; Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; Принципы организации документирования разработки, процесса сопровождения программного обеспечения.	Теоретические вопросы: 1. Жизненный цикл программных средств. Модели жизненного цикла. 2. Поддержка технологии объектно-ориентированного программирования средствами языка Python. 3. Кортежи. Базовые операции. 4. Множества. Базовые операции. Генераторы множеств. 5. Словари. Создание, базовые операции. Методы словарей. 6. Функции. Передача параметров в функцию. Области видимости переменных в Python. 7. Дополнительные возможности при работе с функциями.	Б1.Б.21Технологии и методы программирования
Уметь	Работать с интегрированной средой	1. Реализовать алгоритмы сортировки и поиска	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	разработки программного обеспечения; Использовать динамически подключаемые библиотеки; Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; Использовать шаблоны классов и средства макрообработки; Проводить комплексное тестирование и отладку программных систем; Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; Проводить выбор эффективных способов реализации профессиональных задач; Планировать разработку сложного программного обеспечения; Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; автоматизированных систем;	экстремальных значений в массивах. 2. Определите класс «Решение квадратного уравнения» Класс содержит: Закрытые поля: коэффициенты квадратного уравнения; Открытые: функции-свойства для заполнения полей; Функции-методы: вычисления дискриминанта вычисления корней распечатка количества корней распечатка корней.	
Владеть	Основными навыками проектирования программного обеспечения с использованием средств автоматизации. Навыками программирования различными стилями. Навыками разработки программной документации. Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов. Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.	Написать приложение для реализации следующих задач: 1. Графический редактор “Схемы алгоритмов”. 2. Система представления табличной информации в графическом виде. 3. Специализированный текстовый редактор. 4. Система расчета простейших электрических схем. 5. Разработка обучающего web-ориентированного документа на тему «Язык XML».	
Знать	Виды аутентификации и принципы, на которых	Вопросы для зачета:	Б1.Б.25Безопасность

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	они основаны. Принципы программирования различных видов карт и ключей доступа. Типы атак на системы данных, использующих различные виды аутентификации	1. Процедуры, выполняемые при регистрации пользователя в системе. 2. Перечислить элементы аутентификации. 3. Привести примеры факторов аутентификации. 4. Для чего служит механизм управления доступом? 5. Структура команд APDU. Примеры команд APDU. 6. Для чего необходимы парольные политики? 7. Методы парольной аутентификации. 8. Описать принципы работы биометрических систем. 9. Описать принцип работы OTP-токена. 10. Способы аутентификации пользователя при использовании OTP-токена.	систем баз данных
Уметь	Настраивать систему организации и контроля доступа различного вида. Анализировать и находить решения по защите от атак на системы данных, использующих различные виды аутентификации. Устанавливать средства защиты БД.	1. Провести анализ атак на системы данных, в которых используется аутентификация на основе пароля, и найти способы защиты от них. 2. Провести анализ атак на системы данных, использующие аутентификацию с помощью биометрических характеристик, и найти способы защиты от них. 3. Провести анализ атак на системы данных, использующие аутентификацию с помощью OTP-токенов, и найти способы защиты от них.	
Владеть	Навыками настройки и администрирования средств защиты БД. Навыками разработки системы защиты с учетом особенностей защиты информации, обрабатываемой в СУБД. Навыками анализа критериев оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.	1. Запрограммировать смарт карту. 2. Внести в БД биометрической системы аутентификации 2х администраторов. В качестве идентификаторов использовать отпечаток пальца и модель лица. 3. Внести в БД биометрической системы аутентификации 2х пользователей. В качестве идентификаторов использовать отпечаток пальца или пароль. 4. Запрограммировать 2 ключа iButton на блокировку входа. 5. Запрограммировать 2 ключа iButton на администрирование системы.	
Знать	Основные принципы организации программных и программно-аппаратных СЗИ. Основные подходы создания программных и программно-аппаратных СЗИ.	Вопросы к экзамену: 1. Основные принципы организации программных и программно-аппаратных СЗИ. 2. Обзор рынка имеющихся сертифицированных	Б1.Б.36Информационная безопасность распределенных информационных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	Основные подходы и способы реализации СКЗИ.	программных и программно-аппаратных СЗИ. 3. Обзор рынка имеющихся сертифицированных СКЗИ.	
Уметь	Проводить комплексное тестирование и отладку программных и программно-аппаратных СЗИ. Администрировать программные и программно-аппаратные СЗИ. Проводить комплексное тестирование и отладку СКЗИ. Администрировать СКЗИ.	1. Провести тестирование работоспособности СЗИ «Страж NT». 2. Провести тестирование работоспособности СКЗИ «КриптоПро CSP». 3. Провести тестирование работоспособности СКЗИ «КРИПТОН-ЗАМОК».	
Владеть	Навыками комплексного тестирования и отладки программных и программно-аппаратных систем защиты информации. Навыками администрирования программных и программно-аппаратных СЗИ. Навыками комплексного тестирования и отладки СКЗИ. Навыками администрирования СКЗИ.	1. Произвести снятие СКЗИ «КРИПТОН-ЗАМОК». Затем восстановить работоспособность и настроить СКЗИ. 2. Произвести аварийное снятие СЗИ. Затем восстановить подсистему идентификации и работоспособность основных служб СЗИ «Страж NT».	
Знать	- способы организации обмена данными по схеме «peer-to-peer»; - способы организации обмена данными при помощи технологии Socket - базовый синтаксис C#; - базовый функционал LabVIEW; - способы обработки ошибок; -способы организации многопоточности;	1. Определение распределенной системы. 2. Классификация распределённых приложений. 3. Прозрачность в распределенных приложениях. 4. Открытость в распределенных приложениях. отделение правил от механизмов. 5. Масштабируемость в распределенных системах. Проблемы масштабируемости. Технологии масштабирования. 6. Мультипроцессоры. 7. Гомогенные мультикомпьютерные системы. 8. Гетерогенные мультикомпьютерные системы. 9. Мультипроцессорные операционные системы. 10. Мультикомпьютерные операционные системы. 11. Системы с распределенной памятью.	Б1.Б.38Технология построения защищенных распределенных приложений

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	- применять язык программирования C# для построения консольных клиент/серверных приложений для однократной передачи данных; - применять язык программирования LabVIEW для построения простейших клиент/серверных приложений для однократной передачи данных; - согласовывать формат передаваемых данных и логику обмена информацией.	На языке C# разработать алгоритм подключения к удаленному серверу. На языке C# разработать алгоритм передачи данных удаленному серверу. На языке C# разработать алгоритм приема данных от удаленного сервера. В среде LabVIEW разработать блок-диаграмму подключения к удаленному серверу. В среде LabVIEW разработать блок-диаграмму передачи данных удаленному серверу. В среде LabVIEW разработать блок-диаграмму приема данных от удаленного сервера.	
Владеть	- навыками разработки приложений на языке C# с применением многопоточности; - навыками разработки приложений на языке LabVIEW с применением многопоточности;	На языке C# реализовать алгоритм создания отдельного потока при подключении к серверу очередного клиента. На языке C# реализовать алгоритм передачи данных между потоками. На языке C# реализовать алгоритм рассылки сообщения всем подключенным клиентам. В среде LabVIEW разработать блок-диаграмму создания отдельного потока при подключении к серверу очередного клиента. В среде LabVIEW разработать блок-диаграмму передачи данных между потоками. В среде LabVIEW разработать блок-диаграмму рассылки сообщения всем подключенным клиентам.	
Знать	−базовые понятия и терминологию Big Data; −возможности инструментальных средств программирования для обработки Big Data; −основные алгоритмы и структуры для работы с Big Data; основные понятия распределённых систем	**Перечень теоретических вопросов:** 1. Основные понятия Big Data 2. Технологии, используемые для обработки и хранения Big Data. 3. Инструментальные системы программирования для обработки больших массивов данных. 4. Аналитические процессы обнаружения и обработки ошибок данных. 5. Системы управления потоками данных. 6. Обработка данных в реальном времени. 7. ЦОДы, хранилища данных, витрины данных.	Б1.Б.43 Основы Data инжиниринга

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		8. Теорема CAP и возможность ее обеспечения в реализации распределѐ нных вычислений. 9. Масштабируемость баз данных NoSQL 10. Основные модели параллельных вычислений. 11. Модель вычислений MapReduce. 12. Архитектура платформы Apache Hadoop 13. Устройство распределенной файловой системы HDFS. 14. Технологии поиска Big data: обычный, полнотекстовый и интеграции. 15. Параллельные запросы. 16. Интеграция данных из различных источников. 17. Основные алгоритмы и структуры для работы с Big Data Основные функции Python, применяемые для синтаксического анализа Big Data	
Уметь	– применять инструментальные средства программирования для обработки Big Date; выявлять скрытые аномалии в данных.	**Задание**. Используя основные функции библиотеки Pandas провести комбинаторный синтаксический анализ записей файла больших размеров (>30 Гб) вида: X 45.2121 Y 12.7711 Z -2.2141 **Задание.** С помощью алгоритмов и инструментальных средств Питона провести синтаксический анализ записей файла больших размеров (>100 Гб) и произвести подсчет частоты встречаемости слов в наборе данных. **Задание.** Укажите, какие аналитические процессы обнаружения и обработки ошибок данных применимы для указанной структуры документа.	
Владеть	– современными технологиями обслуживания Big Data; – алгоритмами и методами для обработки Big Date; – инструментальными средствами программирования для обработки Big Date	**Задание. З**апустите Hadoop кластер из трех нод – 1 главной и 2 подчиненных **Задание.** Создайте программу с реализацией функций Map и Reduce на платформе Apache Hadoop **Задание.** Создайте программу для реализации взаимных блокировок. **Задание.** Имеется набор документов (например, архив новостей). Необходимо для каждого слова, встречающегося в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		наборе документов, посчитать, сколько раз встречается слово в наборе. Для подсчета используйте технологию MapReduce. Для запуска MapReduce используйте streaming-интерфейс Hadoop. Программы Mapper и Reducer (для выполнения функций Map и Reduce) реализовать на python. **Задание.** Проведите тест по производительности Hadoop MapReduce.	
Знать	– средства моделирования угроз информационной безопасности	Перечень вопросов к экзамену 1. Средства моделирования угроз 2. Средства для вычисления вероятности возникновения отдельных угроз. 3. Назовите основные законы распределения вероятностей для статистического моделирования угроз.	Б1.В.03 Моделирование угроз информационной безопасности
Уметь	– применять языки, системы и инструментальные средства программирования для моделирования угроз информационной безопасности.	Определить вероятность возникновения угрозы по полученным данным	
Владеть	– навыками применения инструментальных средств программирования для моделирования угроз.	Провести прогнозирование атак на сервер объекта информатизации	
Знать	- Синтаксис языков программирования высокого уровня (объектно- ориентированное программирование); - Современные технологии и методы программирования; - Показатели качества программного обеспечения; - Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; - Принципы организации документирования разработки, процесса сопровождения программного обеспечения.	***индивидуальное задание на производственную практику:*** *Список индивидуальных тем* 55. Современные средства защиты информации 56. Современные системы компьютерной безопасности 57. Современные криптографические системы 58. Криптоанализ, современное состояние 59. Правовые основы защиты информации 60. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними 61. Технические аспекты обеспечения защиты информации. 62. Атаки на систему безопасности и современные методы защиты 63. Современные пути решения проблемы информационной безопасности РФ 64. Организация центра мониторинга событий на основе	Б2.Б.01(У) Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	- Работать с интегрированной средой разработки программного обеспечения; - Реализовывать основные структуры данных и базовые алгоритмы средствами языков		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	программирования; - Проводить комплексное тестирование и отладку программных систем; - Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; - Проводить выбор эффективных способов решения профессиональных задач; - Планировать разработку сложного программного обеспечения; - Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; автоматизированных систем;	современных систем анализа информационной безопасности 65. Информационная безопасность в условиях цифровой экономики Российской Федерации 66. Безопасность сетей беспроводной передачи данных 67. Использование хэш-функций в современном мире и их криптостойкость 68. Проблемы применения средств защиты информации в операционной системе Windows 69. Алгоритмы тестирования генераторов псевдослучайных чисел 70. Система накопления и анализа данных для контроля за инцидентами в сфере информационной безопасности с учетом поведенческого подхода 71. Анализ законодательства в области размещения и использования ИТСНК на территории Российской Федерации 72. Анализ угроз безопасности информации. Возможные организационные меры, применяемые для нейтрализации ряда угроз безопасности информации 73. Актуальность обеспечения информационной безопасности на промышленных предприятиях 74. Безопасность в мире «Интернета вещей» 75. Безопасность распознавания личности по отпечаткам пальцев 76. Применение искусственных нейронных сетей для выявления инцидентов информационной безопасности 77. Угрозы информационной безопасности при «оплате в одно касание». 78. Анализ нормативной документации, регламентирующей ответственность за утечку сведений, составляющих государственную тайну 79. Математические модели в информационной безопасности 80. Обзор нормативно-правовой базы в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации	
Владеть	- Навыками программирования различными стилями. - Навыками разработки программной документации. - Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов. - Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		81. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований Cookie: принципы работы и безопасность использования	
Знать	Общие принципы построения современных языков программирования высокого уровня. -Язык программирования высокого уровня (объектно- ориентированное программирование).	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-Работать с интегрированной средой разработки программного обеспечения. -Использовать шаблоны классов и средства макрообработки. -Использовать динамически подключаемые библиотеки. -Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.		
Владеть	-Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования. -Навыками работы с интегрированной средой разработки программного обеспечения.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 45) Род деятельности предприятия, на котором проходила практика. 46) Какие способы защиты информации используются на предприятии? 47) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 48) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 49) Какая топология используется в локальных сетях на предприятии? 50) Как обеспечивается безопасность беспроводных сетей? 51) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 52) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 53) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 54) Опишите способы контроля трафика по локальным сетям предприятия. 55) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 56) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 57) При помощи, каких программных средств	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		осуществляется администрирование ПК персонала предприятия? 58) Какие операционные системы используются на ПК персонала предприятия? 59) Какие операционные системы используются на серверах предприятия? 60) Понятие и виды защищаемой информации по законодательству РФ. 61) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 62) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 63) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 64) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 65) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 66) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 67) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 68) Основное содержание разработки Политики безопасности предприятия (организации). 69) Принципы, основные задачи и функции обеспечения информационной безопасности. 70) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 71) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		сведений, составляющих государственную тайну. 72) Ответственность за нарушение законодательства в информационной сфере. 73) Основные мероприятия по защите информации при проведении совещаний и переговоров. 74) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 75) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 76) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 77) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 78) Сформулировать основные правила безопасной работы в компьютерной системе. 79) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 80) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 81) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 82) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 83) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 84) Рассмотреть особенности разграничения доступа и аудита в СЗИ 85) Особенности реализации метода «разграничения доступа» в системах защиты информации от	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		несанкционированного доступа. 86) Раскрыть особенности образования электромагнитных каналов утечки информации. 87) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	Общие принципы построения современных языков программирования высокого уровня. -Язык программирования высокого уровня (объектно- ориентированное программирование).	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	-Работать с интегрированной средой разработки программного обеспечения. -Использовать шаблоны классов и средства макрообработки. -Использовать динамически подключаемые библиотеки. -Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.		
Владеть	-Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования. -Навыками работы с интегрированной средой разработки программного обеспечения.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах			
Знать	– Основные понятия информатики; – Основные способы хранения, обработки и передачи информации; – Основы технологии поиска в современных информационно- поисковых системах; – Значение информации в развитии современного общества.	Перечень вопросов: 1. Понятие информации и ее свойства 2. Понятие информатизации общества. Роль вычислительной техники в информатизации 3. Принципы построения и классификация технических средств информатизации 4. Технологии сбора и хранения информации 5. Технологический процесс обработки информации 6. Способы обработки информации 7. Режимы обработки информации на компьютере 8. Технологии передачи и представления информации 9. Значение информации в развитии современного общества. 10. Процесс информатизация. Технологии и информационное поле 11. Информационное воздействие и информационная безопасность 12. Информационные технологии для поиска информации 13. Запросы в поисковых системах. Специальные символы поискового запроса 14. Безопасный поиск информации в сети Интернет	Б1.Б.17Информатика
Уметь	– Пользоваться сетевыми средствами для обмена данными, с использованием глобальной	Задания: 1. С помощью информационно-поисковых систем	

<table>
<tr><td>Структурный элемент компетенции</td><td>Планируемые результаты обучения</td><td>Оценочные средства</td><td>Структурный элемент образовательной программы</td></tr>
<tr><td></td><td>информационной сети Интернет;
– Применять функции офисных приложений для организации поиска информации по заданным критериям;
– Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач.</td><td>произвести поиск информации по заданной тематике с учетом основных требований информационной безопасности.
Произвести форматирование многостраничного документа (обзора, реферата и библиографии) в соответствии с стандартами учебного заведения в текстовых редакторах (MS Word или Open Writer).
Обосновать необходимость использования и создания внутри документа нескольких разделов. Подготовить отчет с заданной структурой.
2. Работники отдела удостоверяющего центра производят выдачу электронно-цифровых подписей. На расчет зарплаты выделяется фонд размером 300т.р., каждый работник имеет фиксированный оклад, остатки фонда распределить поровну между работниками, у которых объем выполненной работы превысил среднее значение по отделу.
3. На листе 1 представлен список закупленных средств защиты информации(инв.номер, наименование, производитель, стоимость, № договора, производитель, гарантия). На втором листе по инвентарному номеру определить гарантию(действует/истекла)
4. Реселлер производит поставки набора «Антишпион» от изготовителей до магазинов. Наличие на складах производителей, потребности магазинов и стоимость доставки от производителя до магазинов известны. Использую надстройку «Поиск решения» произвести оптимизацию поставок, с целью снижения общей стоимости доставки.
Стоимость доставки представлены в таблице:
<table>
<tr><td>Магазин\ Производитель</td><td>Производитель 1</td><td>Производитель 2</td><td>Производитель 3</td><td>Потребность, шт</td></tr>
<tr><td>Магазин 1</td><td>2000</td><td>1500</td><td>800</td><td>160</td></tr>
<tr><td>Магазин 2</td><td>900</td><td>1100</td><td>1300</td><td>170</td></tr>
<tr><td>Магазин 3</td><td>1400</td><td>800</td><td>1100</td><td>90</td></tr>
</table>
</td><td></td></tr>
</table>

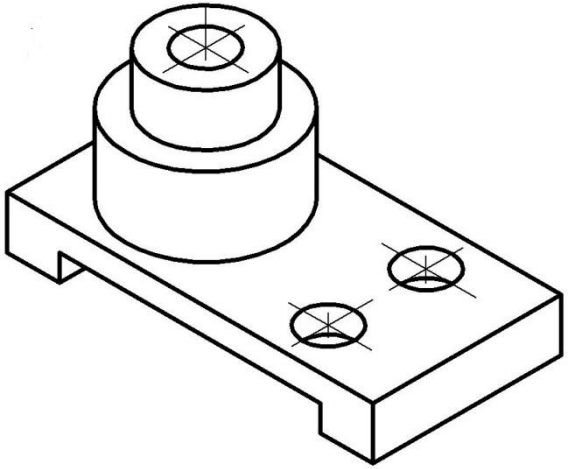
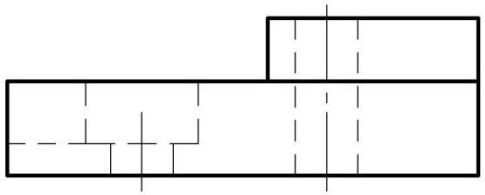
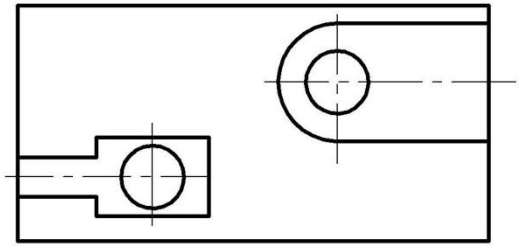
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Склад, шт | 150 | 130 | 140 |	
Владеть	– Навыками использования современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах при решении профессиональных задач; – Навыками построения запросов для организации поиска информации в компьютерных системах, сетях, библиотечных фондах.	Задания: 1. С помощью информационно-поисковых систем найти количество кибератак на информационные системы стран. Составить таблицу количества атак, в которой указать 5 стран и 4 вида атак. Используя язык программирования VBA найти страну с наименьшим средним количеством атак. 2. С помощью информационно-поисковых систем найти количество кибератак на информационные системы стран. Составить таблицу количества атак, в которой указать 3 стран и 5 видов атак. Используя язык программирования VBA найти самую распространенный вид атак. 3. С помощью информационно-поисковых систем найти количество кибератак на информационные системы стран. Создать базу данных в СУБД MS Access содержащую информацию о странах, видам атак, статистику по дням. Создать запрос для вычисления общего количества атак по каждому виду для определенной страны за указанный период.	
Знать	– основные направления развития, значение Big Data и их роль в современном обществе; основные возможности ИКТ для поиска Big Data из различных источников информации.	**Теоретические вопросы:** 1. Значение Big Data в развитии современного общества 2. Основные направления развития технологий Big Data. 3. Современные аппаратные решения для обработки Big Data. 4. Основные методы поиска Big Data из различных источников. 5. Основные понятия о способах хранения информационных массивов. 6. Отличительная особенность NoSQL. 7. Назовите основные пять характеристик, присущие Big Data. 8. Какие задачи может решать анализ Big Data? 9. Назовите принципы разработки параллельных алгоритмов. 10. Свойства больших данных и ограничения RDBMS. 11. Какие существуют базовые принципы обработки Big Data? 12. Дайте определение потоковым данным. Что является хранилищем для ключей?	Б1.Б.43 Основы Data инжиниринга

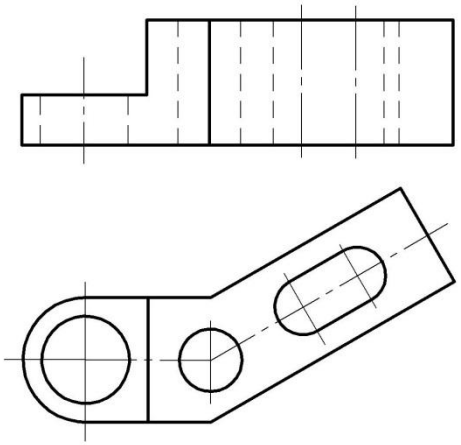
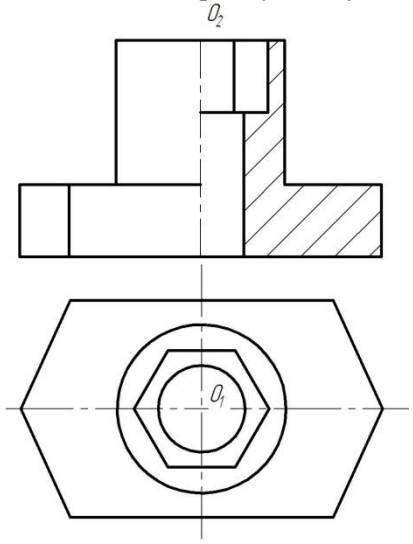
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	–организовывать поиск информации в компьютерных системах, сетях и библиотечных фондах. – автоматизировать работу с большими массивами данных, получать данные из внешних источников.	**Задание.** С помощью информационно-поисковых систем произведите поиск по заданной тематике в структурированных и полуструктурированных данных большого объема (> 5 Гб) из внешних источников с использованием любой из облачных технологий (Cloud Dataflow, AWS, EMR, Azure). Опишите возможные модели и методы для хранения полученных массивов данных большого объема. **Задание.** Создать программу, которая производит поиск неструктурированных данных в указанной предметной области и создает отчет в соответствии с установленными требованиями.	
Владеть	– методами поиска, хранения и обработки Big Data из различных источников баз данных, библиотечных фондов; – методами представления Big Data с использованием информационных, компьютерных и сетевых технологий	**Задание**. Создайте программу обмена сообщениями между распределенными процессами. В виде распределенной среды выполнения используйте ApacheHadoop. **Задание**. Создайте программу с параллельной сортировкой. **Задание.** Каждый месяц в сети Facebook выкладывается в открытый доступ 30 млрд новых источников информации. Определите, какой необходим объем для хранения полученных данных за год. Используйте технологию MapReduce. **Задание.** Создать программу, которая производит поиск Big Data из Internet сайтов и создает отчет в соответствии с установленными требованиями.	
Знать	─ Основные понятия информатики; ─ Основные способы хранения, обработки и передачи информации; ─ Основы технологии поиска в современных информационно- поисковых системах; ─ Значение информации в развитии современного общества.	***индивидуальное задание на производственную практику:*** *Список индивидуальных тем* 1. Современные средства защиты информации 2. Современные системы компьютерной безопасности 3. Современные криптографические системы 4. Криптоанализ, современное состояние 5. Правовые основы защиты информации 6. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними 7. Технические аспекты обеспечения защиты информации. 8. Атаки на систему безопасности и современные методы защиты	Б2.Б.01(У) Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	─ Пользоваться сетевыми средствами для обмена данными, с использованием глобальной информационной сети Интернет; ─ Применять функции офисных приложений для организации поиска информации		

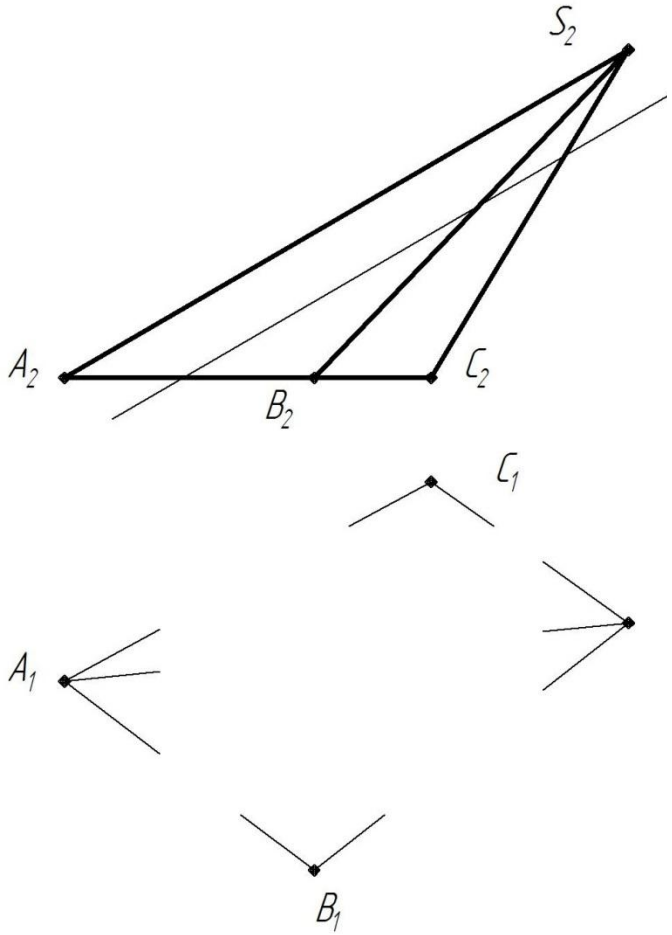
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	по заданным критериям; – Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач.	9. Современные пути решения проблемы информационной безопасности РФ 10. Организация центра мониторинга событий на основе современных систем анализа информационной безопасности 11. Информационная безопасность в условиях цифровой экономики Российской Федерации 12. Безопасность сетей беспроводной передачи данных 13. Использование хэш-функций в современном мире и их криптостойкость 14. Проблемы применения средств защиты информации в операционной системе Windows 15. Алгоритмы тестирования генераторов псевдослучайных чисел 16. Система накопления и анализа данных для контроля за инцидентами в сфере информационной безопасности с учетом поведенческого подхода 17. Анализ законодательства в области размещения и использования ИТСНК на территории Российской Федерации 18. Анализ угроз безопасности информации. Возможные организационные меры, применяемые для нейтрализации ряда угроз безопасности информации 19. Актуальность обеспечения информационной безопасности на промышленных предприятиях 20. Безопасность в мире «Интернета вещей» 21. Безопасность распознавания личности по отпечаткам пальцев 22. Применение искусственных нейронных сетей для выявления инцидентов информационной безопасности 23. Угрозы информационной безопасности при «оплате в одно касание». 24. Анализ нормативной документации, регламентирующей ответственность за утечку сведений, составляющих государственную тайну 25. Математические модели в информационной безопасности	
Владеть	– Навыками использования современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах при решении профессиональных задач; – Навыками построения запросов для организации поиска информации в компьютерных системах, сетях, библиотечных фондах.		

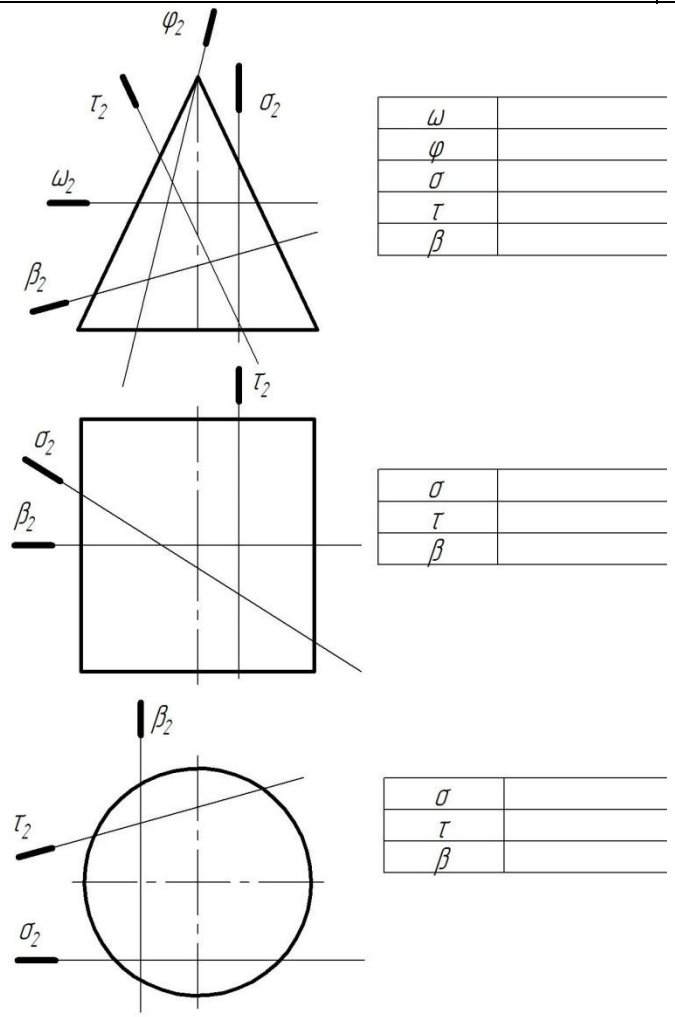
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		26. Обзор нормативно-правовой базы в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации 27. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований Cookie: принципы работы и безопасность использования	
ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами			
Знать	- основные определения и понятия инженерной графики; - основные правила выполнения чертежей; - основные положения ЕСКД; - нормативные и руководящие материалы, касающиеся выполняемых типов чертежей	***Перечень теоретических вопросов к зачету:*** 1. Единая система конструкторской документации (ЕСКД). ГОСТ 2.301-68 Форматы. ГОСТ 2.302-68 Масштабы. ГОСТ 2.303-68 Линии чертежа. ГОСТ 2.304-81 Шрифты чертежные. 2. ГОСТ 2.305 – 68. Изображения. Виды. Разрезы. Сечения. 3. ГОСТ 2.306-68 Обозначения графические материалов и правила их нанесения на чертежах. 4. ГОСТ 2.307-68. Нанесение размеров на чертежах и предельных отклонений. 5. Аксонометрические проекции. Условия наглядности. Свойства параллельного проецирования. 6. ГОСТ 2.317-69 Стандартные виды аксонометрических проекций. Коэффициенты искажения. Построение плоских фигур и окружностей в различных видах аксонометрических проекций. 7. Метод проецирования. Центральное и параллельное проецирование. Ортогональное и косоугольное проецирование. 8. Комплексный чертеж в трех проекциях. Свойства комплексного чертежа. 9. Проекции прямой линии. Точка на прямой линии. Взаимное расположение прямых линий. 10. Различные случаи положения прямой линии в пространстве. 11. Плоскость. Элементы, определяющие плоскость. 12. Различные положения плоскости в пространстве.	Б1.Б.35 Инженерная графика

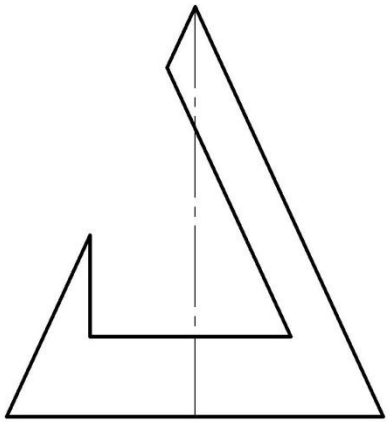
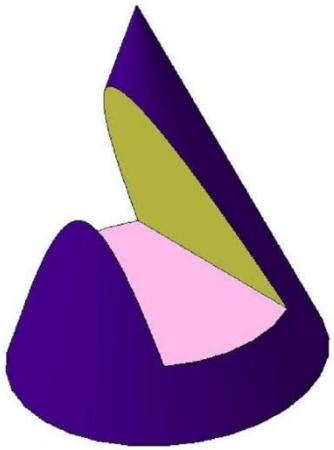
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		13. Поверхности. Классификация поверхностей и задание поверхности на чертеже. 14. Точка и линия, принадлежащие поверхности. 15. Сечение многогранников плоскостью. 16. Пересечение тел вращения плоскостью. Пересечение цилиндра проецирующей плоскостью. 17. Пересечение тел вращения плоскостью. Конические сечения. 18. Пересечение тел вращения плоскостью. Пересечение сферы проецирующей плоскостью. 19. Резьбовые соединения. Элементы резьбы. Типы резьб. Изображение и обозначение резьбы. 20. Сварные соединения. Типы сворных соединений. Изображение и обозначение их на чертеже. 21. Сборочный чертеж, чертеж общего вида. Условности и упрощения при выполнении СЧ. 22. Стандартные изделия. Соединения болтовое, винтовое, шпилечное. Особенности их изображения на сборочных чертежах. 23. ГОСТ 2.401-68. Спецификация. Разделы спецификации. Порядок составления. 24. Компьютерная графика. Выполнение чертежей средствами компьютерной графики и САПР. Основные методы и команды создания 2-д чертежа. 25. Компьютерная графика. Выполнение чертежей средствами компьютерной графики и САПР. Основные методы и команды создания трехмерной модели и получение чертежа. 26. Компьютерная графика. Выполнение чертежей средствами компьютерной графики и САПР. Основные методы и команды редактирования чертежей и 3D моделей.	
Уметь	- обсуждать способы эффективного решения задач (2D или 3D построения); - объяснять (выявлять и строить) типичные модели задач, чертежей и 3D моделей; - применять знания чтения и построения	Примерные практические задания для зачета: 1. По наглядному изображению построить комплексный чертеж детали.	

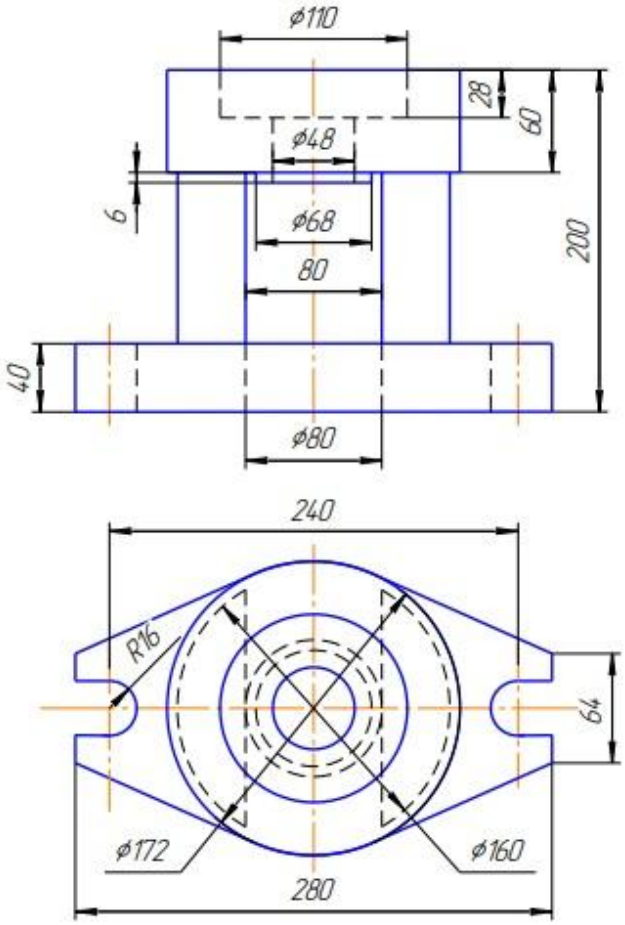
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	чертежей в профессиональной деятельности; - использовать знания чтения и построения чертежей и 3D моделей на междисциплинарном уровне	 2. Выполнить и обозначить сложный ступенчатый разрез   3. Выполнить и обозначить сложный ломаный разрез	

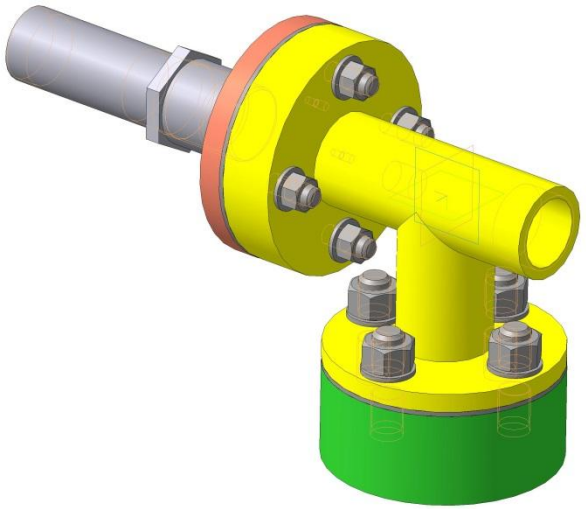
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		 4. Построить вид слева, прямоугольную изометрию детали  5. Достроить горизонтальную проекцию пирамиды, натуральную величину сечения пирамиды плоскостью и определить видимость ребер пирамиды. Построить развертку пирамиды.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		 6. Записать в таблицы названия кривых, полученных в сечениях заданных поверхностей вращения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		 7. Построить три проекции поверхности вращения со сквозным вырезом	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
			
Владеть	- практическими навыками использования элементов дисциплины для решения задач на других дисциплинах, на занятиях в аудитории и на производственной практике; - методами использования программных средств для решения практических задач; - основными методами решения задач в области инженерной графики; - возможностью междисциплинарного применения полученных знаний; - основными методами исследования в области инженерной и компьютерной графики, практическими умениями и навыками их использования	Примерные практические задания: 1. Построить 3D модель поверхности вращения со сквозным вырезом в КОМПАС 3D  1. По заданным видам построить 3D модель детали, создать ассоциативный комплексный чертеж детали в соответствии с требованиями ЕСКД	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		 2. По индивидуальным вариантам создать 3D модели деталей элеватора, создать 3D сборку элеватора.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		 3. Создать сборочный чертеж и спецификацию элеватора.	
Знать	Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Способы координирования деятельности подразделений по ЗИ на предприятии, в учреждении, организации. Подходы создания междисциплинарных и инновационных проектов.	Вопросы к экзамену: 1. Принципы построения информационно-логической модели. 2. Принципы разработки пакета планирующих документов по построению системы ИБ, с помощью и на основе которого реализуется принятая политика ИБ.	Б1.Б.36Информационная безопасность распределенных информационных систем
Уметь	Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации.	1. Составьте подробное описание прохождения критичной информации через все элементы выбранной СОИ и опишите все возможные точки атак.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации. Принимать участие в междисциплинарных и инновационных проектах.	2. Составить список ранжированных угроз для выбранного ОИ.	
Владеть	Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации. Навыками организации и реализации междисциплинарных и инновационных проектов.	1. Распределите работы по проведению аудита среди обучающихся группы с учетом их возможностей. Оцените результаты их работы. 2. Распределите работы для расследования компьютерного инцидента среди обучающихся группы с учетом их возможностей. Оцените результаты их работы. 2. Распределите работы по предпроектному диагностическому обследованию среди обучающихся группы с учетом их возможностей. Оцените результаты их работы.	
Знать	– средства и методы стимулирования сбыта продукции. Виды охранных документов интеллектуальной собственности – основные шаги и правила государственной системы регистрации результатов научной деятельности	*Теоретические вопросы:* 1. Организация и планирование продвижения товара и пути его совершенство-вания. 2. Средства и методы стимулирования сбыта продукции. 3. Изобретательство. Изобретение. 4. Изобретательство. Полезная модель. 5. Государственная регистрация научных результатов.	Б1.Б.40Продвижение научной продукции
Уметь	– составлять пакет документов для регистрации программы ЭВМ – составлять пакет документов для регистрации изобретения или полезной модели	*Практические задания:* 1. Определить 5 аналогов и прототип: - Заявка 2015127606/02 - Заявка 2015153533 - Заявка 2017116674 - Заявка 2017124014 2. Указать структурные элементы формулы изобретения в сравнении с аналогом для: - ДВС - Электродвигатель - Телевизор	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		- Технология производство стекла - Спортивный велосипед 3. Указать структурные элементы формулы полезной модели в сравнении с аналогом для : - ДВС - Электродвигатель - Телевизор - Технология производство стекла - Спортивный велосипед	
Владеть	– способами анализа патентной документации и проведения патентного поиска – способами совершенствования профессиональных знаний и умений путем использования возможностей информационной среды	*Творческие задания:* 1. Сравнить стабильный и инновационный производственные процессы. 2. Описать виды продвижения научной продукции на рынке.	
Знать	Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Этапы создания междисциплинарных и инновационных проектов.	*перечень вопросов на защите отчета НИР:* 1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР?	Б2.Б.02(Н) Научно-исследовательская работа
Уметь	Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации. Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации. Принимать участие в междисциплинарных и инновационных проектах		
Владеть	Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации. Навыками организации и реализации междисциплинарных и инновационных проектов		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Какие охранные документы были получены в ходе выполнения НИР?	
ОПК-6	**способностью применять нормативные правовые акты в профессиональной деятельности**		
Знать	– роль правовой информации в развитии современного общества и профессиональной деятельности; – виды источников права – систему законодательства Российской Федерации	**Примерные вопросы к зачету** 1. Понятие и сущность права 2. Источники права 3. Система законодательства Российской Федерации 4. Нормативно-правовые акты, их виды 5. Отрасли российского права.	Б1.Б.05Правоведение
Уметь	– находить и анализировать правовую информацию; – использовать правовую информацию при решении конкретных жизненных ситуаций.	**Примерные практические задания:** После расторжения брака родителей Андрюша Холкин был оставлен матери Гордеевой В.. Фактически же он проживал с бабушкой Холкиной Р., где был ранее прописан. Холкина Р. решила продать свою квартиру и попросила бывшую сноху прописать мальчика у себя и заняться, наконец, воспитанием сына, та никак не отреагировала. **Дайте правовую оценку ситуации. Аргументируйте свой ответ со ссылкой на статьи части 1 Гражданского кодекса РФ.**	
Владеть	– практическими навыками работы со справочно-поисковыми системами Консультант Плюс и Гарант	**Примерные практические задания:** 1. Используя, данные сети Интернет найдите официальные сайты справочно-поисковых систем Консультант Плюс и Гарант; 2. Используя, ресурсы справочно-поисковой системы Консультант Плюс найдите Конституцию Российской Федерации в последней редакции; 3. Используя, ресурсы справочно-поисковой системы Гарант найдите Уголовный кодекс Российской Федерации в последней редакции.	
Знать:	Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. Системы регулирования возникающих общественных отношений в информационной сферы. Составляющие информационной сферы, представляющей собой совокупность информации,	Вопросы для зачета: 1. Понятие информационной безопасности государства. 2. Источники угроз информационной безопасности для объекта информатизации. 3. Классификация угроз информационной безопасности для объекта информатизации. 4. Требования защиты информации. 5. Стратегия развития информационного общества в России.	Б1.Б.26Основы информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.		
Уметь:	Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. Использовать инфраструктуру единого информационного пространства РФ в личных целях. Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.	1. Найти перечень нормативно-правовых документов в области защиты информации автоматизированных систем. 2. Провести анализ нормативно-правовых документов в области защиты информации автоматизированных систем.	
Владеть:	Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. Способами использования информационной инфраструктуры в интересах общественного развития. Методами разработки проектов нормативных документов, регламентирующих работу по защите информации	1. На основе проведенного анализа нормативно-правовых документов в области защиты информации автоматизированных систем найти слабые места в системе управления безопасностью информации в автоматизированных системах на современном уровне развития общества.	
Знать	-виды тайн, закрепленные в российском законодательстве -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях	Теоретические вопросы 1. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима. 2. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. 3. Требования к помещениям и хранилищам, в которых	Б1.Б.31Организационное и правовое обеспечение информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	-основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности - нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях	ведутся закрытые работы. 4. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. 5. Защита информации в экстремальных ситуациях. 6. Виды информации, подлежащие защите в соответствии с законодательством Российской Федерации. 7. Государственная тайна. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. 8. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. 9. Лицензионные требования ФСТЭК России на деятельность по технической защите конфиденциальной информации. 10. Лицензионные требования ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. 11. Сертификация. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации	
Уметь:	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	Составить перечень нормативно правовых локументов для обеспечения режима гос.таайны Составить перечень нормативно правовых локументов для обеспечения режима конфиндециальности	
Владеть	-навыками работы с нормативными правовыми актами -навыками подготовки деловой корреспонденции	Подготовит инструкции по конфиндециальному делопросизводству выбраннойорганизации	
Знать	- основные нормативные правовые акты в области защиты информации;	Вопросы для зачета: 1. Понятия информация, информационные технологии и	Б1.Б.42 Основы безопасности цифрового

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- основные законы о цифровых правах граждан РФ;	защита информации. 2. Угрозы информационной безопасности для личных персональных данных. 3. Трансформация понятия информационная безопасность. 4. Понятие цифровые права гражданина РФ. 5. Понятие кибергигиены.	общества
Уметь	- находить нужные источники цифровой информации и цифровые данные; - воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными	1. Найти перечень основных нормативно-правовых документов по кибербезопасности и провести их анализ. 2. Найти перечень основных нормативно-правовых документов по цифровизации и провести их анализ.	
Владеть	способами эффективного использования полученной цифровой информации для решения профессиональных задач; - управлять цифровой информацией и данными;	1. На основе проведенного анализа нормативно-правовых документов в области цифровизации найти слабые места, требующие внимания. 2. Написать приложение на языке C# для определения уровня цифровой грамотности респондента.	
Знать	-основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности - нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности		
Владеть	-навыками работы с нормативными правовыми актами		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать:	-основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности - нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь:	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности		
Владеть:	-навыками работы с нормативными правовыми актами		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ОПК-7 способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций			
Знать	- основные понятия о приемах первой помощи; - основные понятия о правах и обязанностях граждан по обеспечению безопасности жизнедеятельности; - характеристики опасностей природного, техногенного и социального происхождения; - государственную политику в области подготовки и защиты населения в условиях	**Перечень теоретических вопросов к экзамену:** 1. Что такое чрезвычайная ситуация? 2. Классификация ЧС 3. Опасные факторы различных ЧС 4. Перечислите характеристики опасностей природного происхождения 5. Перечислите характеристики опасностей техногенного происхождения	Б1.Б.08Безопасность жизнедеятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	чрезвычайных ситуаций	6. Перечислите характеристики опасностей социального происхождения 7. Что такое безопасность жизнедеятельности? 8. Права и обязанности граждан по обеспечению БЖД 9. Принципы обеспечения безопасности. Методы и средства обеспечения безопасности 10. Что такое первая доврачебная помощь? 11. Основные приемы первой доврачебной помощи при различных случаях 12. Какова государственная политика в области подготовки и защиты населения в условиях ЧС?	
Уметь	- выделять основные опасности среды обитания человека; - оценивать риск их реализации	**Практические задания (тесты):** **1. Индивидуальный риск 3* относится к транспорту:** а) автомобильному б) водному в) железнодорожному г) воздушному **2. В организме человека радиоактивный плутоний и лантан концентрируются в:** а) в скелете б) в печени в) в мышцах г) в легких **3. Устройство, предназначенное для перевозки людей и (или) грузов – это ...** **4. Соотнесите вид излучения с коэффициентом относительной биологической эффективности:** 1. Рентгеновское и у-излучение 2. Нейтроны с энергией меньше 20кЭв 3. Протоны с энергией меньше 10 мэВ 4. Тяжелые ядра отдачи а) 1 б) 3 в) 10 г) 20 **5. Необходимые действия населения при экологической**	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		катастрофе ... а) отстаивание питьевой воды б) для снижения возможностей отравления следует дышать носом в) проверка газоснабжения, водопровода, канализации г) проветривать квартиру в городах следует только днём д) нельзя применять продукты, имевшие контакт с водой е) осторожное обращение с растворителями, ядохимикатами, моющими и чистящими средствами	
Владеть	- основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций	**Комплексные задания:** ЗАДАНИЕ 1 Произошел крупный пожар, который был вызван неосторожным применением пиротехники. По заключению следствия жертвы пожара погибли преимущественно из-за отравления угарным газом и продуктами горения, ожогов и давки. К какому виду ответственности должно быть привлечено руководство за нарушение правил пожарной безопасности? Укажите последовательность осуществления первой медицинской помощи при отравлении угарным газом. Как называется неконтролируемый процесс горения, причиняющий материальный ущерб, вред жизни и здоровью людей, интересам общества и государства? ЗАДАНИЕ 2 В результате схода лавины погибли четверо туристов. Двум участникам группы удалось спастись. Их попытки самостоятельно откопать пострадавших оказались безуспешными. По данным МЧС, ориентировочно в горном массиве сошло 2,1 тыс. $м^3$ снега: ширина лавины составила 7 метров, глубина – 3 метра и длина – 100 метров. Как называется удушье, обусловленное кислородным голоданием и избытком углекислоты в крови и тканях? Укажите последовательность осуществления первой медицинской помощи при сильном обморожении конечностей. Если скорость лавины составляет 200 км/ч, а дальность ее выброса – 1 км, то время (в секундах), за которое лавина сойдет с горного массива, составит …? ЗАДАНИЕ 3 В районе аэропорта потерпел катастрофу пассажирский	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		самолет. 44 человека погибло, 1 – пострадал. Официальное расследование катастрофы провел Межгосударственный авиационный комитет (МАК). Непосредственной причиной катастрофы названа ошибка пилотирования. Как называется уменьшение давления в салоне самолета? Укажите последовательность действий человека в случае возникновения аварийной ситуации в самолете. Если в 2011 году в России в авиакатастрофах погибло 120 человек, что составляет 24 % от общего количества всех погибших, то во всем мире за этот год в результате авиакатастроф погибло … человек.	
Знать	- основные понятия о приемах первой помощи; - основные понятия о правах и обязанностях граждан по обеспечению безопасности жизнедеятельности; - характеристики опасностей природного, техногенного и социального происхождения; - государственную политику в области подготовки и защиты населения в условиях чрезвычайных ситуаций	*Перечень теоретических вопросов к зачету:* 1. Организм. Его функции. Взаимодействие с внешней средой. Гомеостаз. 2. Регуляция функций в организме. 3. Двигательная активность как биологическая потребность организма. 4. Особенности физически тренированного организма. 5. Костная система. Влияние на неё физических нагрузок. 6. Мышечная система. Скелетные мышцы, строение, функции. 7. Напряжение и сокращение мышц. Изотонический и изометрический режим работы. 8. Сердечно-сосудистая система. Функции крови. Систолический и минутный объём крови. Кровообращение при физических нагрузках. 9. Работа сердца, пульс. Кровяное давление. 10. Дыхательная система. Процесс дыхания. Газообмен. Регуляция дыхания и его особенности. Дыхание при физических нагрузках. 11. Жизненная ёмкость лёгких. Кислородный запрос и кислородный долг. 12. Пищеварение. Его особенности при физических нагрузках. 13. Утомление и восстановление. Реакция организма на физические нагрузки.	Б1.Б.41Физическая культура и спорт
Уметь	- выделять основные опасности среды обитания человека; - оценивать риск их реализации	*Перечень заданий для зачета:* 1. Что такое здоровье? 2.Какое здоровье определяет духовный потенциал человека? 3. Какие факторы окружающей среды влияют на здоровье	

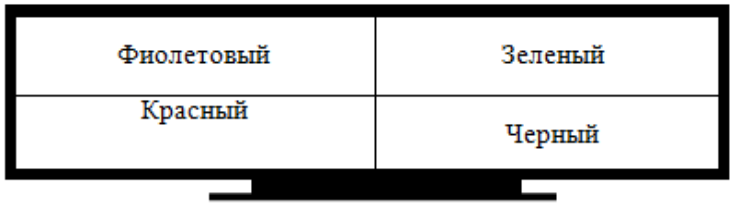
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		человека? 4. Какова норма ночного сна? 5. Укажите среднее суточное потребление энергии у девушек. 6. Укажите среднее суточное потребление энергии у юношей. 7. За сколько времени до занятий физической культурой следует принимать пищу? 8. Укажите в часах минимальную норму двигательной активности студента в неделю. 9. Укажите важный принцип закаливания организма.	
Владеть	- основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций	*Задания на решение задач из профессиональной области, комплексные задания:* 1. Дайте определение основным понятиям: работоспособность, утомление, переутомление, усталость, рекреация, релаксация, самочувствие. 2. Опишите изменение состояния организма студента под влиянием различных режимов и условий обучения 3. Как внешние и внутренние факторы влияют на умственную работоспособность? Какие закономерности можно проследить в изменении работоспособности студентов в процессе обучения? 4. Какие средства физической культуры в регулировании умственной работоспособности, психоэмоционального и функционального состояния студентов вы знаете? 5. «Физические упражнения как средство активного отдыха»,- раскройте это положение. 6. «Малые формы» физической культуры в режиме учебного труда студентов. 7. Учебные и самостоятельные занятия по физической культуре в режиме учебно-трудовой деятельности.	
ОПК-8	**способностью к освоению новых образцов программных, технических средств и информационных технологий**		
Знать	– основные определения и понятия, используемые в теории операционных систем; – современные подходы к организации и проведению научных исследований с использованием сетевых технологий; - принципы построения и современные	Перечень вопрос: 1. Принципы классификации операционных систем, их основные характеристики и функциональное назначение; 2. Основные структурные элементы и подсистемы операционной системы, их характеристики и функциональное назначение;	Б1.Б.23 Безопасность операционных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;	3. Принципы функционирования ядра, дисковой, файловой, сетевой подсистем операционной системы 4. Основные принципы построения подсистем безопасности операционных систем	
Уметь	- разрабатывать политику учетных записей пользователей ОС; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;	1. Провести сравнительный анализ различных операционных систем с точки зрения защищенности информации; 2. Обосновать выбор операционной системы при построении информационной системы на ее базе;	
Владеть	- навыками использования операционных систем семейств Unix и Windows в системах защиты информации ; - методами и технологиями исследования безопасности операционных систем.	1. Используя средства администрирования файловой подсистемы произвести настройку операционной систем семейств Windows 2. Используя средства администрирования произвести настройку подсистемы безопасности операционной системы семейств Windows 3. Разработать сценарий администрирования для операционных систем семейств Windows и UNIX/Linux 4. Произвести и обосновать выбор операционной системы для построения информационной системы на ее базе с точки зрения требований по защищенности информации	
Знать	─ Нормативные и правовые акты в области защиты информации передаваемой в сетях ЭВМ; ─ Современные технологии обеспечения информационной безопасности в сетях ЭВМ; ─ Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ.	Перечень вопросов: 1. Классифицируйте угрозы безопасности в современных вычислительных сетях. Какие угрозы безопасности в современных вычислительных сетях являются актуальными на сегодняшний день? Какие угрозы безопасности сетей ЭВМ будут, на Ваш взгляд, актуальными завтра? 2. Какие тенденции и подходы к обеспечению безопасности сетей ЭВМ Вы знаете? Охарактеризуйте их. 3. Дайте определение понятий «уязвимость сетевого оборудования» и «уязвимость вычислительной сети». Какие виды уязвимостей Вам известны? Перечислите и охарактеризуйте их. 4. Каким образом осуществляется поиск и устранение	Б1.Б.24Безопасность сетей ЭВМ

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		уязвимостей сетевого оборудования и вычислительной сети? Какие программные и аппаратные средства используются для поиска уязвимостей? 5. Назовите современные программные и аппаратные средства, позволяющие нейтрализовать угрозы безопасности вычислительной сети. 6. Классифицируйте современные технологии обеспечения безопасности сетей ЭВМ – назначение, область применения, принцип действия, достоинства и недостатки. 7. Дайте определение понятию «сетевая атака». Какие разновидности сетевых атак Вы знаете? Каким образом производится обнаружение и нейтрализация сетевых атак? 8. Назовите известные Вам системы обнаружения сетевых атак? Классифицируйте их (назначение, область применения, принцип действия). 9. Что, на Ваш взгляд, включает в себя понятие «комплексный подход к обеспечению сетевой безопасности»? 10. Дайте определения понятиям «базовая модель угроз» и «модель нарушителя» для сети ЭВМ.	
Уметь	- Производить анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей; - Выполнять подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности; - Выполнять установку и настройку средств защиты информации при эксплуатации их в современной вычислительной сети; - Разрабатывать и реализовать политику сетевой безопасности при настройке и конфигурировании сетевого оборудования.	1. Произвести анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей. 2. Разработать план нейтрализации выявленных уязвимостей вычислительной сети и сетевого оборудования. 3. Выполнить подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности. 4. Произвести настройку протоколов обеспечения сетевой безопасности на сетевом оборудовании. 5. Выполнять установку и настройку средств защиты информации при эксплуатации их в современной вычислительной сети. 6. Разработать политику безопасности вычислительной сети как комплексную методику обеспечения безопасности и нейтрализации уязвимостей вычислительной сети. 7. Реализовать разработанную политику сетевой безопасности при настройке и конфигурировании сетевого оборудования.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	- Навыками работы с современными программными сканерами сетевых протоколов и сетевых уязвимостей; - Навыками решения задач по поиску неисправностей вычислительных сетей с целью выявления уязвимостей вычислительных сетей и нейтрализации обнаруженных уязвимостей; - Навыками повышения уровня защищенности вычислительных сетей и оптимизации их работы.	При помощи сканеров сетевых протоколов и сетевых уязвимостей произвести обследование вычислительной сети и определить: • Каким образом организован доступ в глобальные сети из данной сети; • Системное программное обеспечение, применяемое для обеспечения функционирования сетевых узлов (операционные системы); • Модели и сетевые адреса активного сетевого оборудования в структуре вычислительной сети; • Схемы маршрутизации сетевого трафика; • Используемые сетевые протоколы; • Открытые сетевые порты; • Наличие или отсутствие устройств межсетевого экранирования, систем обнаружения вторжений, сетевых антивирусов и других средств обеспечения сетевой безопасности; • Наличие или отсутствие активных гостевых учетных записей и административных учетных записей с паролем по умолчанию на сетевом оборудовании; • Наличие или отсутствие известных уязвимостей сетевого оборудования и программного обеспечения на узлах сети. По результатам обследования сделать заключение о достаточности или недостаточности мер, принимаемых для обеспечения безопасности вычислительной сети.	
Знать	принципы построения и функционирования, примеры реализаций современных операционных систем; ─ принципы работы элементов и функциональных узлов электронной аппаратуры; ─ типовые схемотехнические решения основных	1. Общие принципы построения ОС 2. Современная ОС. Развитие ОС 3. Состав, взаимодействие основных компонентов ОС 4. Логическая организация файловой системы. 5. Физическая организация файловой системы.	Б1.Б.28Организация ЭВМ и вычислительных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	узлов и блоков электронной аппаратуры	6. Файловые операции, контроль доступа к файлам. 7. Причины нарушения целостности ФС 8. Организация хранения данных. Файловая система FAT 9. Организация хранения данных. Файловая система NTFS 10. Разбиение жесткого диска на разделы и их форматирование 11. Конфигурирование системы. Формат управлений 12. Диспетчер задач 13. Какие основные напряжения используются при питания материнской платы. 14. Допустимые токи при питании переферийных устройств с интерфейсом USB 15. Назначение, классификация цифро-аналоговых преобразователей, основные их характеристики. 16. Назначение, классификация аналого-цифровых преобразователей, основные их характеристики.	
Уметь	применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); ─ применять на работать с современной элементной базой электронной аппаратуры	1. Произвести анализ и выполнить оптимизацию диска с помощью встроенных средств дефрагментации ОС 2. Создать контрольную точку восстановления и произвести восстановление ОС к созданной точке 3. Произвести анализ канала Data интерфейса PS/2 Keyboard полученного с помощью осциллографа 4. Произвести анализ канала HSyns интерфейса SVGA полученного с помощью осциллографа 5. Выполнить оценку напряжений разъема ATX 24pin используя цифровой мультиметр.	
Владеть	принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; ─ навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы	1. По указанной схеме архитектуры ЭВМ указать основные элементы. 2. Оценить работу ПК с помощью системных программных средствам Windows диагностики ПК 3. Оценить комплектацию ПК. Составить рекомендацию на оптимизацию с применением модернизации компонентов. 4. По указанной схема материнской платы определить интерфейс для подключения аудиоразъема передней панели корпуса 5. Построить временную диаграму каналов CLK и DATA при нажатии клавиши «1» клавиатуры PS/2 (скан код клавиши «69»)	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		6. Нарисовать осциллограмму каналов R,G,B, HSync, VSync при передачи изображения по стандарту SVGA следующего изображения (разрешение 2x2): 	
Знать	Принципы построения вычислительных сетей; - Классификацию сетей ЭВМ; - Принципы передачи информации по телекоммуникационным каналам связи; - Классификацию сетевого оборудования; - Принципы функционирования и основные структурные и функциональные элементы различных классов сетевого оборудования; - Семиуровневую эталонную модель взаимодействия открытых систем (модель OSI) с твердым пониманием назначения каждого из уровней модели; - Принципы адресации в вычислительных сетях; - Принципы организации межсетевого взаимодействия и межсетевой передачи информации.	Перечень вопросов: 1. Какие разновидности сетей Вы знаете? Назовите их. 2. Каким образом осуществляется передача информации по телекоммуникационному каналу связи. Объясните основные принципы кодирования информации при ее передаче по каналу связи. 3. Коммутация в системах передачи информации. Организация систем связи по принципу коммутации каналов и по принципу пакетной коммутации. В чем отличия? 4. Назначение и область применения семиуровневой эталонной модели взаимодействия открытых систем. Охарактеризуйте подробно функциональное назначение каждого уровня модели. 5. Какие технологии построения локальных сетей Вы знаете? Охарактеризуйте их. Дайте определение понятию «сетевая топология». 6. Дайте классификацию современного сетевого оборудования – типы, назначение, область применения. 7. Дайте определение понятию «сетевой протокол». Какие современные сетевые протоколы Вы знаете? 8. Принципы адресации в вычислительных сетях. Каким образом реализуется сетевая адресация на различных уровнях семиуровневой эталонной модели межсетевого взаимодействия? 9. Что такое «маршрутизация» в вычислительных сетях? Назначение, принципы организации, основные алгоритмы. 10. Беспроводная передача информации и беспроводные сети. Назначение, область применения, основные принципы построения.	Б1.Б.30Сети и системы передачи информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	Выбирать требуемое сетевое и телекоммуникационное оборудование, необходимое для организации вычислительной сети с требуемыми характеристиками.	1. Самостоятельно выполнить подбор сетевого оборудования исходя из требуемых рабочих характеристик и планируемой производительности вычислительной сети; 2. Разработать физическую (топологию) и логическую (схему разбиения на подсети (сегментирования), план адресации, схемы маршрутизации) схемы вычислительной сети согласно поставленной задаче, определить возможности дальнейшего роста спроектированной вычислительной сети. 3. Выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, межсетевой экран) для построения разработанной топологии сети. 4. Реализовать разработанную логическую схему сети при настройке и конфигурированию сетевого оборудования.	
Владеть	Профессиональным языком и терминологией предметной области (сети ЭВМ); - Современным сетевым оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей (сетей ЭВМ).	1. Произвести работу с программными сканерами сетевых протоколов (например, свободно распространяемые сканеры WireShark и Ethereal) 2. Выполнить диагностику неисправностей и аномальных состояний вычислительных сетей 3. Выполнить задачу по поиску неисправностей вычислительных сетей и оптимизации их работы 4. Осуществить сбор и анализ информации в вычислительной сети при помощи сканера сетевых протоколов и определить: - Количество активных сетевых узлов; - Схему сетевой адресации; - Схему подключения сети к глобальным сетям общего пользования; - Адреса активного сетевого оборудования; - Наличие ошибок топологии сети (например, петли в структуре сети), ошибок в логической структуре сети (ошибки адресации, маршрутизации, сегментирования на подсети и т.д.)	
Знать	Классификацию современных программных и программно-аппаратных СЗИ.	Вопросы к экзамену: 1. Разновидности ключей Rutoken.	Б1.Б.32Программно-аппаратные средства

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ. Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.	2. Отличия ключей eToken от Rutoken. 3. Особенности ключей Guardant. 4. Методы защиты информации от НСД. 5. Классификация программных и программно-аппаратных СЗИ.	обеспечения информационной безопасности
Уметь	Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ и систем с применением современных информационных технологий. Основные принципы работы всех подсистем системы ИБ АС.	В СЗИ «Страж NT» создать пользователей user1 и user2. Присвоить пользователю user1 пароль, назначить допуск «Сов.секретно» и сформировать идентификатор типа Guardant ID. Не присваивать пользователю user2 пароль, назначить допуск «Секретно» и сформировать идентификатор типа ruToken. Сформировать ЗПС. Настроить управление защитными атрибутами ресурсов. Продемонстрировать различия в работе этих двух пользователей.	
Владеть	Навыками работы с подсистемами системы информационной безопасности автоматизированной системы. Навыками администрирования системы ИБ АС.	В СЗИ «Страж NT» создать иерархию ресурсов, назначить им разные дискреционные списки контроля доступа, назначить им разные грифы. Продемонстрировать различия в работе пользователей с различными правами доступа при осуществлении попытки доступа к созданным ресурсам.	
Знать	– типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ – способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы;	1. Назначение и возможности аппаратно-программных средств защиты информации 2. Выбор мер защиты информации для реализации в информационной системе. 3. Защита информационной системы, ее средств, систем связи и передачи данных 4. Защита от вредоносного программного обеспечения 5. Программно-аппаратные комплексы средств защиты информации от НСД	Б1.Б.33Разработка и эксплуатация защищенных автоматизированных систем
Уметь	– осуществлять сбор, обработку, анализ и систематизацию научно- технической информации в области программных и программно-аппаратных средств ЗИ; – применять средства и системы защиты информационно-технологических ресурсов	Определить перечень СЗИ согласно требованиям к функциям подсистемы обеспечения безопасности информации типовой модели угроз безопасности персональных данных при их обработке в системе обеспечения вызова экстренных оперативных служб по единому номеру «112»	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	автоматизированной системы; – применять новые информационные технологии в сфере защиты данных.		
Владеть	методами исследования новых образцов программных, технических средств и информационных технологий, применяемых в области информационной безопасности	**Задание.** Провести тестирование работоспособности СЗИ «Страж NT».	
Знать	- основные информационные ресурсы, содержащие актуальную информацию по проектированию распределенных систем. - концепции аппаратных решений при проектировании распределенных систем; - Концепции программных решений при проектировании распределенных систем - варианты архитектуры клиент-сервер;	1. Назовите современные паттерны проектирования распределенных информационных систем. 2. В чем отличия между гомогенными и гетерогенными мультикомпьютерными системами? 3. В чем отличия мультипроцессорных и мультикомпьютерных распределенных систем. 4. Назовите имманентные свойства сетевых операционных систем. 5. Укажите причины разделения программных компонент распределенных систем по функциональным уровням. 6. Укажите основные функциональные уровни программных компонент распределенной системы. 7. Программное обеспечение промежуточного уровня.	Б1.Б.37Методы проектирования защищенных распределенных информационных систем
Уметь	- разделять программные компоненты распределенных систем по функциональным уровням - разделять зоны ответственности программных компонент распределённой системы - применять SOLID принципы при проектировании распределенных систем	1. На примере службы доменных имен укажите функциональные уровни программных компонент. 2. В чем опасность увеличения зоны ответственности программной компоненты распределенной системы? 3. Как применение принципа единой ответственности влияет на структуру программных компонент распределенной системы? 4. Каким образом описывается интерфейс программной компоненты распределенной системы?	
Владеть	методами масштабирования распределенных систем. - методами интеграции готовых программных решений в проектируемую распределенную систему - навыками конфигурирования аппаратных средств входящих в состав распределенной системы	1. Укажите основные способы масштабирования распределенной системы. 2. Какие трудности могут возникнуть при масштабировании распределенной системы по размеру. 3. Укажите функционал пакетных менеджеров различных сред проектирования распределенных систем. 4. Укажите последовательность конфигурирования коммутаторов 2	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		и 3 уровней. 5. Назовите основные открытые интерфейсы по средствам которых осуществляется конфигурирование аппаратных средств.	
Знать	− основные информационные технологии, используемые в автоматизированных системах; - основные программные и технические средства для безопасной работы с базой данных (БД); - новые образцы программных, технических средств для БД; - системы управления базами данных; - способы и алгоритм внедрения и продуктивного использования новых программных, технических средств для БД;	**Теоретические вопросы к зачету:** 1. Определение БД и БнД. Состав и структура БнД. 2. Назначение основных компонентов БнД. 3. Основные признаки классификации БнД. 4. Понятие и назначение лингвистических средств БнД. 5. Основные категории пользователей БД. Основные функции администратора БД. 6. Взаимосвязь этапов создания БД и используемых моделей предметной области. 7. Структурированные и слабоструктурированные данные. Особенности представления. 8. Классификационная схема моделей БД. 9. Понятие «физического» и «логического» представления. 10. Понятие физической и логической записи. 11. Примерная схема организации файлового ввода-вывода. 12. Сходство и отличие процессов обработки данных средствами файловой системы и СУБД. 13. Основные этапы эволюции систем обработки данных. Основные отличия в концепциях обработки данных разных этапов. 14. Схема управления данными в СУБД.	Б1.В.02 Информационные технологии. Базы данных
Уметь	- работать в некоторых интегрированных средах систем управления базой данных (СУБД); - построить схему БД в программных средствах создания БД; - быстро приспособиться к работе в новых интегрированных средах СУБД;	***Задача:*** По описанию предметной области и функций управления, которые необходимо реализовать, спроектировать структуру предметной области, выделить типы объектов и существенные отношения между ними. ***Вариант1.*** Создать базу данных «Персональные мероприятия сотрудников». База данных должна содержать следующую информацию: информацию обо всех возможных мероприятиях, проводимых в организации, о местах проведения мероприятий,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информацию о сотрудниках, поместить информацию о проведенном мероприятии (дата, описание, кто является ответственным, отзыв (хороший, удовлетворительный, неудовлетворительный)). ***Вариант 2.*** Создать базу данных для сотовой телефонной компании. БД хранит сведения о подключениях, клиентах, работниках, заключенных договорах. Каждый клиент может заключать несколько договоров на различные услуги. Каждый работник заключает много договоров. ***Вариант 3.*** Создать базу данных «Автосервис». База данных должна содержать следующую информацию: информацию об оказываемых услугах (наименование услуги, цена), информацию об автослесарях центра (табельный номер, паспортные данные, категория). В БД поместить информацию об оплате каждой услуги (дата оказания услуги, табельный номер мастера, какая услуга оказана, номер ремонтируемой машины).	
Владеть	- навыками работы на языке манипулирования БД; - методами оценки правильности проектирования БД;	***Задание:*** Определить логическую структуру базы данных для предметной области. ***Вариант 1.*** Создать базу данных «Библиотека». Книги сортируются по нескольким разделам, каждый раздел находится в определенном месте (этаж, сектор). БД хранит сведения о книгах, о читателях, о сотрудниках библиотеки. Сохранять сведения о выданных книгах, когда выдана книга, какая и кому. ***Вариант 2.*** Создать базу данных «Автошкола». Указать данные об учащихся, информацию об инструкторах, информацию об имеющихся учебных машинах, информацию об экзаменах (кто сдает, какому инструктору на какой машине, датах сдачи экзаменов и оценках). ***Вариант 3.*** Создать базу данных «Музей». База данных должна содержать следующую: информацию об имеющихся в наличии экспонатах (наименование, автор, источник происхождения, количество экземпляров, принадлежность к тематическому разделу, история происхождения, состояние), о музейных хранилищах, о выставочных залах. Каждое хранилище предназначено для хранения экспонатов определенного тематического направления. Содержимое выставочных залов меняется с течением времени.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Вариант 4. Создать базу данных «Банк активов предприятия». БД должна содержать информацию об активах предприятия, уязвимостей активов, угроз и атак, а так же зависимости между ними.	
Знать	─ принципы построения и функционирования, примеры реализаций современных операционных систем; ─ принципы работы элементов и функциональных узлов электронной аппаратуры; ─ типовые схемотехнические решения основных узлов и блоков электронной аппаратуры - Принципы адресации в вычислительных сетях; - Принципы организации межсетевого взаимодействия и межсетевой передачи информации	***индивидуальное задание на производственную практику:*** *Список индивидуальных тем* 1. Современные средства защиты информации 2. Современные системы компьютерной безопасности 3. Современные криптографические системы 4. Криптоанализ, современное состояние 5. Правовые основы защиты информации 6. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними 7. Технические аспекты обеспечения защиты информации. 8. Атаки на систему безопасности и современные методы защиты 9. Современные пути решения проблемы информационной безопасности РФ 10. Организация центра мониторинга событий на основе современных систем анализа информационной безопасности 11. Информационная безопасность в условиях цифровой экономики Российской Федерации 12. Безопасность сетей беспроводной передачи данных 13. Использование хэш-функций в современном мире и их криптостойкость 14. Проблемы применения средств защиты информации в операционной системе Windows 15. Алгоритмы тестирования генераторов псевдослучайных чисел 16. Система накопления и анализа данных для контроля за инцидентами в сфере информационной безопасности с учетом поведенческого подхода 17. Анализ законодательства в области размещения и использования ИТСНК на территории Российской Федерации 18. Анализ угроз безопасности информации. Возможные	Б2.Б.01(У) Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	─ применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); ─ работать с современной элементной базой электронной аппаратуры - Выбирать требуемое сетевое и телекоммуникационное оборудование, необходимое для организации вычислительной сети с требуемыми характеристиками		
Владеть	─ навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; ─ Профессиональным языком и терминологией предметной области ─ Современным сетевым оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		организационные меры, применяемые для нейтрализации ряда угроз безопасности информации 19. Актуальность обеспечения информационной безопасности на промышленных предприятиях 20. Безопасность в мире «Интернета вещей» 21. Безопасность распознавания личности по отпечаткам пальцев 22. Применение искусственных нейронных сетей для выявления инцидентов информационной безопасности 23. Угрозы информационной безопасности при «оплате в одно касание». 24. Анализ нормативной документации, регламентирующей ответственность за утечку сведений, составляющих государственную тайну 25. Математические модели в информационной безопасности 26. Обзор нормативно-правовой базы в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации 27. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований Cookie: принципы работы и безопасность использования	
Знать	-Классификацию современных программных и программноаппаратных СЗИ. -Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ. -Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-Осуществлять сбор, обработку, анализ и систематизацию научно- технической информации в области программных и программно-аппаратных средств ЗИ и систем с применением современных информационных технологий. -Основные принципы работы всех подсистем		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	системы ИБ АС.	информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на	
Владеть	- Навыками работы с подсистемами системы информационной безопасности автоматизированной системы. - Навыками администрирования системы ИБ АС.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПРОФЕССИОНАЛЬНО-СПЕЦИАЛИЗИРОВАННЫЕ КОМПЕТЕНЦИИ			
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах			
Знать	– Нормативные правовые акты в области защиты информации – Национальные, межгосударственные и международные стандарты в области защиты информации – Руководящие и методические документы	Перечень вопросов к экзамену 1. Назовите логические уровни АСУТП, предложенные в 31-ом приказе ФСТЭК России 2. Назовите группы технических средств, присущие каждому уровню 3. Базовая модель угроз безопасности персональных данных	Б1.В.02 Моделирование угроз информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	уполномоченных федеральных органов исполнительной власти по защите информации	при их обработке в информационных системах персональных данных.	
Уметь	– Оценивать информационные риски в автоматизированных системах – Классифицировать и оценивать угрозы безопасности информации – Определять подлежащие защите информационные ресурсы автоматизированных систем – Анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	Задание: ● Построить частную модель угроз ИБ для объекта защиты. ● Составьте типизированный состав компонентов распределенной информационной системы ● Определите источники угроз для АС ● Сформировать список уязвимостей объекта защиты, которые могут быть использованы для реализации угроз. ● Определить типы и возможности нарушителей в распределенной информационной системе	
Владеть	– методами выявления угроз безопасности информации в автоматизированных системах – методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе	Задание: ● Построить дерево угроз ОИ имеющего выход в глобальную сеть; ● Составить перечень актуальных угроз распределенной информационной системы. ● Составить частную модель угроз для выбранного объекта информатизации	
Знать	- нормативные правовые акты, стандарты и руководящие документы в области защиты информации; - порядок разработки модели угроз - виды нарушителей информационной безопасности	Перечень вопросов: 1. Процесс определения угроз безопасности информации в информационной системе 2. Типы и виды нарушителей 3. Возможные цели и потенциал нарушителе 4. Оценка возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя) 5. Определение актуальных угроз безопасности информации в информационной системе 6. Показатель актуальности угрозы безопасности информации 7. Оценка вероятности (возможности) реализации угрозы безопасности информации 8. Показатели, характеризующие проектную защищенность	Б1.В.06 Защита информационно-технологических ресурсов автоматизированных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационной системы 9. Определение уровня проектной защищенности информационной системы 10. Ооценка степени возможного ущерба от реализации угрозы безопасности информации 11. Результат реализации угрозы безопасности информации 12. Основные виды ущерба и возможные негативные последствия 13. Формирование экспертной группы 14. Проведение экспертной оценки 15. Определение показателя «техническая компетентность нарушителя» 16. определение показателя «возможности нарушителя по доступу к информационной системе»	
Уметь	- определять подлежащие защите информационно-технологические ресурсы автоматизированных систем; - классифицировать и оценивать угрозы безопасности информации; - оценивать потенциал нарушителя информационной безопасности	По представленным исходных данным об автоматизированной системе определить: 1. Подлежащие защите информационно-технологические ресурсы 2. Разработать модель угроз 3. Определить нарушителя, его потенциал. 4. Составить модель нарушителя	
Владеть	- методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.	По представленным исходных данным об автоматизированной системе определить: 1. Границы обследуемой автоматизированной информационной системы 2. Проектный уровень защищенности АС 3. Вероятность определяемых угроз 4. Актуальность угроз 5. Степень ущерба и последствия от реализации актуальных угроз	
Знать	пути разработки и определении приоритетов решения задач с учётом требований информационной безопасности -приемы выбора численных методов решения	Теоретические вопросы 1. Что такое линии уровня целевой функции? 2. Нахождение глобального и локального экстремума функций многих переменных.	Б1.В.ДВ.02.01 Основы теории оптимизации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	оптимизационных задач;	3. Итерационные методы решения задач оптимизации. Общая схема итерационных методов. Сходимость по градиенту. 4. Методы решения нелинейных оптимизационных задач. Градиентный метод. 5. Генетический алгоритм оптимизации	
Уметь	Самостоятельно расширять математические знания и проводить анализ прикладных задач за счет получения дополнительной информации в условиях недостающей информации; – Реализовать основные алгоритмы оптимизации средствами программного обеспечения и вычислительной техники; – Разрабатывать алгоритмы численного решения задач оптимизации	1. Написать приложение для решения задачи одномерной оптимизации с заданной точностью методом золотого сечения. 2. На основе рюкзачного алгоритма написать приложение на языке высокого уровня для реализации системы шифрования с открытым ключом	
Владеть	навыками разработки математических моделей предметных областей в постановке задач условной оптимизации – Методами оптимизации средствами вычислительной техники; – Навыками реализации задач оптимизации посредством программного обеспечения общего назначения и методо- ориентированного	Написать приложение для решения задачи многомерной оптимизации методом сопряженных градиентов. 2. Написать приложение для решения задачи многомерной оптимизации с использованием генетического алгоритма	
Знать	– Основные принципы и схемы автоматического управления; – Основные требования нормативно-правовой базы в области защиты информации; – Основные уязвимости защищенных компьютерных систем; – Модели безопасности компьютерных систем; – Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов; – Математические методы для анализа общих свойств распределенных систем.	1. Моделирование собственных частот и форм (мод) колебаний подвижной системы консольного акселерометра. 2. Моделирование электростатического поля (скалярного поля потенциала и векторного поля напряженности), создаваемого системой точечных или линейных зарядов. 3. Моделирование топологии магнитного поля системы линейных токов, например, линий электропередачи. 4. Задачи анализа и оптимизации экономических систем, которые удобно решать на моделях, представленных случайными графами и сетями. 5. Сети Петри. 6. Построение сети Петри для простейшей модели управления запасами на складе готовой продукции.	Б1.В.ДВ.02.02 Математическое моделирование распределенных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		7. Графы событий (ГС). 8. Построение и анализ графа событий для модели малого производственного предприятия. 9. Случайные графы. 10. Генерация случайных графов из заданного класса, соответствующего одной из моделей деятельности производственного предприятия	
Уметь	– Проводить теоретические исследования уровня защищенности и/или оценочного уровня доверия компьютерной системы; – Применять нормативно-правовые документы в области защиты информации; – Проводить теоретические и экспериментальные исследования уровня защищенности и/или оценочного уровня доверия компьютерной системы; – Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; – Применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами на базе современной вычислительной техники и средств автоматизации исследований; – Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	1. Произвести исследование с помощью модели переходных процессов и частотных характеристик системы. Выполнить анализ устойчивости. 2. Произвести моделирование доски Гальтона (аппроксимации биномиального закона нормальным законом распределения вероятностей), броуновского движения частицы в плоскости и пространстве. 3. Произвести моделирование стационарного телеграфного сигнала с заданной интенсивностью числа смен знака, вычисление корреляционной функции, спектральной плотности мощности и статистической погрешности оценки этих функций. 4. Произвести моделирование корреляционной функции белого шума на выходе фильтра низких частот первого порядка, полосового фильтра второго порядка, идеального полосового фильтра. 5. Выполнить генерацию дискретных случайных величин. Сделать выборку с возвращением и выборку без возвращения. 6. Выполнить генерацию случайных процессов. Выполнить генерацию Гауссовских процессов. 7. Выполнить генерацию случайных графов с заданными свойствами. Использовать метод допустимого выбора. 8. Выполнить генерацию деревьев, связных графов, ациклических графов. 9. Выполнить генерацию графов событий (ГС). 10. Произвести нахождение минимального набора переменных состояния, необходимых для однозначного воспроизведения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		поведения модели. 11. Произвести нахождение пар событий, для которых возможна необходимость установления приоритета.	
Владеть	– Навыками выявления, исследования функциональных свойств и состояния программного обеспечения; – Навыками применения математических методов для анализа общих свойств линейных распределенных систем; – Приемами разработки математических моделей систем с распределенными параметрами; – Навыками анализа и оценки угрозы информационной безопасности объекта; – Навыками исследования алгоритма программного продукта, типов поддерживаемых аппаратных платформ; – Приемами разработки математических моделей систем с распределенными параметрами.	1. Выполнить моделирование собственных частот и форм (мод) колебаний подвижной системы консольного акселерометра. 2. Выполнить моделирование электростатического поля (скалярного поля потенциала и векторного поля напряженности), создаваемого системой точечных или линейных зарядов. 3. Выполнить моделирование топологии магнитного поля системы линейных токов, например, линий электропередачи. 4. Произвести моделирование и оптимизацию потоков в случайных сетях. 5. Произвести решение задачи анализа и оптимизации экономических систем, которые удобно решать на моделях, представленных случайными графами и сетями. 6. Выполнить построение сети Петри для простейшей модели управления запасами на складе готовой продукции. 7. Выполнить построение и анализ графа событий для модели малого производственного предприятия. 8. Произвести генерация случайных графов из заданного класса, соответствующего одной из моделей деятельности производственного предприятия	
Знать	Основные положения методики моделирования угроз безопасности информации Основные положения базовой модели угроз безопасности ПДн при их обработке в ИС ПДн	1. Классификация угроз по используемым уязвимостям 2. Классификация угроз по объекту воздействия 3. Элементы описания угроз НСД 4. Общая характеристика источников угроз НСД в ИС ПДн 5. Уязвимости отдельных протоколов стека протоколов TCP/IP	Б1.Б.36 Информационная безопасность распределенных информационных систем
Уметь	Применять методику моделирования угроз безопасности информации для разработки частных моделей угроз и нарушителя	1. Составить карту уязвимостей прикладного программного обеспечения Google Chrome 2. Составить карту атак для реализации угроз стека	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	Применять базовую модель угроз безопасности ПДн для разработки частных моделей угроз и нарушителя ИС ПДн	протоколов TCP/IP	
Владеть	Навыками классификации угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных Навыками разработки частых моделей угроз безопасности информации	1. Классифицировать нарушителей выбранной ИС ПДн 2. Разработать частную модель угроз выбранной ИС	
Знать	- нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. - порядок разработки модели угроз − цели и задачи моделирования систем и процессов защиты информации; - способы обеспечения информационной безопасности информационных систем; - основные принципы построения моделей систем защиты информации - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	*перечень вопросов на защите отчета НИР:* 1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР? Какие охранные документы были получены в ходе выполнения НИР?	Б2.Б.02(Н) Научно-исследовательская работа
Уметь	- обосновать выбор подходящего метода и привести алгоритм решения задачи; - формировать множество альтернативных решений, ставить цель и выбирать оценочный критерий оптимальности способа решения - применять новые технологии проектирования и анализа систем - проводить мониторинг угроз безопасности		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационных систем		
Владеть	- навыками решения моделирования процессов защиты информации - навыками проектирования информационных структур - навыками семантического моделирования данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; − навыками анализа основных узлов и устройств современных автоматизированных систем		
Знать	- нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. - порядок разработки модели угроз - виды нарушителей информационной безопасности	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных систем; - анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации - оценивать потенциал нарушителя		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной безопасности - применять базовую модель угроз ПДн	*Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются	
Владеть	- методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе. - навыками применения базовой модели угроз ПДн		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы)	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. 44) Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. - порядок разработки модели угроз - виды нарушителей информационной безопасности	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	систем; - анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации - оценивать потенциал нарушителя информационной безопасности - применять базовую модель угроз ПДн	информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации?	
Владеть	методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе. - навыками применения базовой модели угроз ПДн		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах			
Знать	- Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;	1. Методика оценки рисков информационной безопасности компании. 2. Управление рисками. Перечислить основные понятия. 3. Метод оценки рисков на основе модели угроз и уязвимостей. 4. Расчет рисков по угрозе информационной безопасности. 5. Метод оценки рисков на основе модели информационных потоков. 6. Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики	Б1.В.05 Анализ рисков информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		управления рисками. Метод CRAMM. 7. Разработка корпоративной методики анализа рисков. 8. Современные методы и средства анализа и управление рисками информационных систем компаний. 9. Обоснование необходимости инвестиций в информационную безопасность компании.	
Уметь	- Разрабатывать политики безопасности; - использовать методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах; - анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.	– Провести расчеты оценки рисков информационной безопасности компании на основе модели информационных потоков.	
Владеть	методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем.	Задание Для заданного предприятия разработать – карту информационных активов фирмы – карту уязвимостей и угроз – отчет о результатах оценки рисков – частные политики безопасности	
Знать:	- архитектуру безопасности Интернета вещей; - угрозы безопасности IoT-систем; - уязвимости информационных систем, содержащих IoT-устройства 1.	1. Уязвимости уровня прикладных программ. 2. Типовые примеры атак на компоненты систем IoT. 3. Классификация и описание возможных угроз, применительно к области IoT. 4. Риски при использовании устройств IoT. 5. Отраслевые сетевые стандарты и модели для IoT под требования безопасности.	Б1.В.07 Безопасность Интернета вещей

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		6. Канал связи. Проводные и беспроводные сетевые протоколы и их уязвимости. –	
Уметь	разрабатывать, руководить разработкой политики безопасности информационных систем, содержащих IoT-устройства;	– Разработать политики безопасности для системы мониторинга климатических показателей на базе IoT-устройств	
Владеть	- навыками проектирования защищенных IoT-систем.	Построить модель рисков выбранной IoT-системы. Предусмотреть меры по снижению рисков на стадии проектирования системы –	
Знать	Ключевые процессы менеджмента ИБ Требования нормативно-правовых документов, регламентирующих систему менеджмента информационной безопасности (СМИБ)	1. Основные принципы создания СУИБ. 2. Процедура внедрения СУИБ. 3. Разработка политик ИБ. 4. Разработка профилей защиты и заданий по безопасности. 5. Организация режима секретности. 6. Технические политики ИБ на предприятии. 7. Идентификация рисков 8. Процессный подход для управления ИБ.	Б1.Б.34 Управление информационной безопасностью
Уметь	Проводить оценку состояния ИБ с учетом угроз и уязвимостей, связанных с информационными активами организации Определять цели применения мер и средств контроля и управления для обработки рисков	Подготовить отчет по проведенному анализу защищенности выбранного объекта: 1. Идентификацию рисков 2. Идентификацию активов и определение их владельцев 3. Идентификация угроз в отношении активов 4. Идентификация уязвимостей 5. Результаты анализа защищенности внутренней ИТ-инфраструктуры	
Владеть	Навыками выбора необходимых мер и средств контроля и управления ИБ Навыками определения способов	По проведенному анализу защищенности подготовить: 1. Рекомендации по устранению уязвимостей внутренней	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	измерения результативности выбранных мер управления ИБ	ИТ-инфраструктуры. 2. Рекомендации по устранению обнаруженных недостатков и повышению уровня защищенности	
Знать:	- Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь:	- оценивать информационные риски в автоматизированных системах; - выполнять анализ рисков информационной безопасности в распределенных информационных системах; - анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах. - определить перечень необходимых политик безопасности		
Владеть:	- методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. 44) Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- оценивать информационные риски в автоматизированных системах; - выполнять анализ рисков информационной безопасности в распределенных информационных системах; - анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах. - определить перечень необходимых политик безопасности		
Владеть	- методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПСК-7.3 способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем			
Знать	─ Методы обнаружения вторжений; ─ Современные системы обнаружения вторжений (СОВ) ─ Методы обнаружения аномалий;	Теоретические вопросы: 1. Методики распознавание атак 2. База сигнатур атак 3. Структура современных систем обнаружения вторжения 4. Подсистема сбора информации 5. Подсистема анализа (обнаружения) 6. Подсистема представления данных	Б1.В.04 Методы выявления нарушений информационной безопасности
Уметь	─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; ─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; ─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.	1. Написать алгоритм настройки выбранной системы выявления нарушений информационной безопасности в виде майнд-карты с учетом требований безопасности информации.	
Владеть	─ Методами выявления угроз ИБ; ─ Методами выявления нарушений ИБ.	1. Провести анализ угроз для выбранной корпоративной инфраструктуры и оформить его в виде майнд-карты	
Знать	─ Источники и классификацию угроз информационной безопасности; ─ Основные принципы построения систем защиты информации; ─ Основные средства и способы обеспечения	1. Объем испытаний на соответствие требованиям по ЗИ от НСД. 2. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. 3. Условия и порядок проведения аттестационных испытаний ВП.	Б1.В.08Аттестация АИС

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной безопасности, принципы построения систем защиты информации.	4. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 5. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 6. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.	
Уметь	– Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; – Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; – Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.	1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации 2. Произвести анализ информационных потоков 3. Определить состав использованных для обработки защищаемой информации средств ВТ. 4. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Определить условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.	
Владеть	– Методами выявления угроз информационной безопасности автоматизированных систем; – Методами аудита уровня защищенности АИС.	2. Произвести проверку ОИ на соответствие организационно-техническим требованиям по защите информации. 3. Определить условия и порядок проведения аттестационных испытаний ВП. 4. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 5. Определить объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 6. Произвести проверку выполнения требований по защите	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информации от утечки по акустическому и виброакустическому каналам для ОИ. 7. Составить модель угроз НСД в ИСПДн. 8. Проанализировать реализованные меры защиты информации на ОИ в соответствии с моделью угроз и особенностей конфигурации ИС.	
Знать	- способы получения информации о внутренней структуре исследуемой распределенной системе; -наиболее распространённые точки для несанкционированного входа в распределенную систему;	1. Получение информации о базе данных. 2. Применение функции include для проведения аудита защищённости. 3. Защита от SQL-инъекций. 4. Области применения XSS. 5. Слепая SQL-инъекция. 6. Получение доступа к таблице user SQL базы данных.	Б1.В.ДВ.05.01 Методы мониторинга информационной безопасности АС
Уметь	- проводить анализ уязвимостей распределённой системы; -получать несанкционированный доступ к ресурсам распределенной системы;	При помощи утилиты Nmap провести тест заданного узла. Определить операционную систему сервера. Используемые протоколы и порты. Используя данные DNS определить связанные ресурсы. Провести их тест.	
Владеть	- навыками противодействия внешним атакам на распределенную информационную сеть;	На Web сервере сконфигурировать авторизацию таким образом, чтобы сделать применение утилиты Hydra неэффективной. Разработать скрипт выполняющий проверку входной переменной для SQL – запроса. Если содержание переменной не корректно вывести соответствующее предупреждение.	
Знать	Принципы организации распределенных корпоративных ИС. Основные этапы аудита информационной безопасности. Основные мероприятия при проведении аудита защищенности ИС	1. Аудита безопасности с точки зрения злоумышленника 2. Определение направления потенциальных угроз 3. Схема реализации угрозы "Анализ сетевого трафика" 4. Схема реализации угрозы "Подмена доверенного объекта сети" 5. Схемы реализации атаки "Навязывание ложного маршрута" 6. Схема реализации угрозы "Внедрение ложного ARP-сервера"	Б1.Б.36 Информационная безопасность распределенных информационных систем
Уметь	Определять порядок организации информационного обмена между структурными подразделениями Обследовать системы на предмет наличия уязвимостей	1. Составить список уязвимостей прикладного программного обеспечения используемого на выбранном ОИ	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	Методами оценки соблюдения требований стандартов и законов, на соответствие которым проводится аудит Навыками проведения инструментального анализа защищенности (оценка достаточности имеющихся и используемых на предприятии программных и технических СЗИ и полноты их использования)	1. Реализовать атаку перехвата трафика на спроектированной по выбранному варианту виртуальной ИС 2. Реализовать атаку на DHCP Server на спроектированной по выбранному варианту виртуальной ИС	
Знать	─ Источники и классификацию угроз информационной безопасности; ─ Основные принципы построения систем защиты информации; ─ Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. ─ Методы и порядок проведения аудита защищенности информационно- технологических ресурсов	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; ─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; ─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем; ─ Проводить аудит защищенности информационно- технологических ресурсов		
Владеть	─ Методами выявления угроз информационной безопасности автоматизированных систем; ─ Методами аудита уровня защищенности АИС.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 9. Род деятельности предприятия, на котором проходила практика. 10. Какие способы защиты информации используются на предприятии? 11. Какие программные средства используются для обеспечения информационной безопасности на предприятии? 12. Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 13. Какая топология используется в локальных сетях на предприятии? 14. Как обеспечивается безопасность беспроводных сетей? 15. Как обеспечивается безопасность по виброакустическим каналам передачи информации? 16. Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 17. Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 18. Опишите способы контроля трафика по локальным сетям предприятия. 19. При помощи, каких программно-аппаратных средств	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		ограничивается доступ персонала предприятия в глобальную сеть. 20. Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 21. При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 22. Какие операционные системы используются на ПК персонала предприятия? 23. Какие операционные системы используются на серверах предприятия? 24. Понятие и виды защищаемой информации по законодательству РФ. 25. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 26. Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 27. Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 28. Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 29. Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 30. Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 31. Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 32. Основное содержание разработки Политики безопасности предприятия (организации). 33. Принципы, основные задачи и функции обеспечения информационной безопасности. 34. Раскрыть содержание правовых основ защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информации. Законодательные источники права на доступ к информации. 35. Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 36. Ответственность за нарушение законодательства в информационной сфере. 37. Основные мероприятия по защите информации при проведении совещаний и переговоров. 38. Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 39. Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 40. Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 41. Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 42. Сформулировать основные правила безопасной работы в компьютерной системе. 43. Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 44. Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 45. Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 46. Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 47. Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		48. Рассмотреть особенности разграничения доступа и аудита в СЗИ 49. Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 50. Раскрыть особенности образования электромагнитных каналов утечки информации. 51. Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	Источники и классификацию угроз информационной безопасности; – Основные принципы построения систем защиты информации; – Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. – Методы и порядок проведения аудита защищенности информационно- технологических ресурсов	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	– Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; – Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; – Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем; – Проводить аудит защищенности информационно- технологических ресурсов		
Владеть	– Методами выявления угроз информационной безопасности автоматизированных систем; – Методами аудита уровня защищенности АИС.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах			
Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных;	**Теоретические вопросы к зачету:** 1. Основные требования к распределенной обработке данных. Классификация режимов работы с БД. 2. Технологии обработки данных. Функции «типового» приложения обработки данных. 3. Архитектуры распределенной обработки данных. Достоинства и недостатки. 4. Архитектуры обслуживания клиентских запросов. Достоинства и недостатки. 5. Доступ к базам данных в двухзвенных моделях клиент-сервер. 6. Целостность БД. Понятие транзакции. Модели транзакций. 7. Виды конфликтов при параллельном выполнении транзакций. 8. Сериализация транзакций. Захват и освобождение объекта. 9. Различие визуального и невизуального способов доступа к данным 10. Основные операции доступа к данным, которые реализует объект – набор данных (TDataSet). 11. Способы поиска и фильтрации записей, предоставляемые объектом – набор данных (TDataSet). 12. Способ формирования параметризованных запросов на	Б1.В.01 Информационные технологии. Базы данных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		этапе реализации программы. 13. Способ формирования параметризованных запросов на этапе выполнения программы. 14. Визуальные компоненты доступа к данным.	
Уметь	- разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; - выделять сущности и связи предметной области; - выполнять запросы к базе данных; - нормализовывать отношения при проектировании реляционной базы данных; - создавать объекты базы данных;	***Задача:*** Разработать клиентское приложение на C# для БД обрабатываемой СУБД MS SQL Server. Приложение должно быть разделено на две части: для администратора, и для пользователей. Каждая часть должна обладать различным функционалом для одной БД. Вариант БД выбрать из перечня вариантов заданий.	
Владеть	- методиками безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.	1. Спроектировать БД «Учет и регистрация электронных ключей предприятия» с использованием любого метода проектирования из перечня вариантов. Определить количество, структуру и взаимосвязи между таблицами. Минимальное количество таблиц в БД 8 штук. Процесс проектирования подробно и поэтапно изложить в отчете. 2. Создать таблицы, определив для каждого поля таблицы свойства. Обеспечить согласованность данных (требование внешнего ключа), создав поля с подстановкой. 3. Установить связи между таблицами. 4. Разработать графический интерфейс для работы с БД (формы для пользователя и администратора) и реализовать его в клиент-серверном исполнении с использованием SQL-сервер. Примечание: БД может быть реализована 2 способами: 1. клиент-серверном на SQL-сервер - max Оценка отлично 2. локальном на MS Access - max Оценка хорошо 5. Создать следующие SQL-запросы: 1) Три запроса на выборку со сложными критериями отбора; 2) Три запроса, использующие групповые операции и статистические функции; 3) Параметрический запрос;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4) Перекрестный запрос; 5) Запрос с вычислением; 6) Запрос с использованием логической функции IIf; 7) Запрос с подзапросами; 8) Выполнить те запросы, которые указаны в самом задании. 6. Создать подчиненные формы для введения данных. 7. Создать отчеты по нескольким запросам с подведением общего итога в отчете. 8. Вывести отчетную информацию в числовом и графическом виде (диаграммы). **Требования к БД** БД «Учет и регистрация электронных ключей предприятия». В базе должна храниться информация: 1. Перечень и характеристики всех носителей информации (флэш-память, токен, смарт-карта и прочие носители) на которых может храниться электронный ключ для работников предприятия. 2. Перечень всех сотрудников предприятия с иерархией по отделам. 3. Перечень сотрудников имеющих доступ ко всей ключевой информации (администраторы БД) 4. Перечень сотрудников подавших заявку на регистрацию персонального ключа и на отмену регистрации. 5. Перечень выданных ключей. Оформить вывод отчетной документации: 1) Оформить форму на списание ключей с учетом их срока службы, указанного изготовителем. Проверка годности ключей должна быть ежедневной с выводом перечня ключей для списания на следующий день от текущей даты. 2) Оформить перечень носителей информации требующих заказа с учетом поданных заявок. 3) Рассчитать расходы предприятия на закупку ключей и расходы на уже закупленные ключи.	
Знать	- основы администрирования в операционных	Перечень вопросов:	Б1.Б.23

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	системах семейств UNIX и Windows; - средства и службы удаленного управления и администрирования ОС; - модели разделения администрирования операционных систем семейств UNIX и Windows;	1. Модель разделения администрирования Active Directory 2. Назначение и управление доменом 3. Средства удаленного администрирования сервера для ролей 4. Средства удаленного администрирования сервера для компонентов 5. Средства администрирования служб терминалов 6. Управление Свойствами пользователя для работы со службами терминалов 7. Работа служб терминалов в режиме сервера приложений	Безопасность операционных систем
Уметь	-выполнять настройку служб терминала; -создавать и выполнять настройку доменов, групп и учетный записей пользователей; -выполнять настройку и удаленное администрирование файлового сервера для ОС семейств UNIX и Windows;	Выполнить настройку служб удаленного администрирование. Создать домен, группы и пользователей в соответствии с представленным заданием преподавателя. Выполнить анализ событий в группе администрирования: 1. Безопасности. 2. Служб каталогов 3. Приложений	
Владеть	- Навыками удаленного администрирования ОС семейств UNIX и Windows; -Навыками настройки и управления службами терминала; -Навыками использования командной строки для настройки и проведения удаленного администрирования ОС семейств UNIX и Windows	Выполнить настройку служб удаленного администрирование. Создать домен, группы и пользователей в соответствии с представленным заданием преподавателя. Используя командную строку: 1. Получить список активных процессов пользователя, произвести удаление процесса. 2. Получить информации об установленном ПО с помощью реестра 3. Получить информацию об установленных драйверах и свободном пространстве удаленного ПК	
Знать	- Последовательность и содержание этапов построения виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в	Перечень вопросов: 1. Межсетевая операционная система Cisco IOS 2. Командные режимы CLI Cisco IOS 2. Система аутентификации, авторизации и учета событий,	Б1.В.ДВ.04.01 Виртуальные сети

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	облачных сетевых структурах. -Основы удаленного администрирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.	встроенная в операционную систему Cisco IOS 3. Настройка и использование Cisco AnyConnect VPN. 4. Предоставление удаленного доступа с использованием протокола SSH 5. Линии виртуальных терминалов VTY для удаленного административного доступа 6. Настройка hostname и доменное имя для удаленного доступа SSH 7. Генерирование ключей и создание учетных записей пользователей SSH 8. Разграничение ролей с помощью уровня привилегий 9. Присваивание команд к уровням привилегий 10. Система доступа на уровне ролей 11. Резервное копирование и восстановление конфигурации Cisco IOS 12. Средства удаленного мониторинга виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. 13. Аутентификация с помощью сервера RADIUS 14.Учет выполняемых действий учетной записи виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.	
Уметь	- Создавать и администрировать виртуальные локальные сети и виртуальные частные сети, а также специализированные виртуальные сети в облачных сетевых структурах. - Реализовывать политику безопасности виртуальной локальной сети и виртуальной частной сети, а также специализированной виртуальной сети в облачных сетевых структурах. - Пользоваться сетевыми средствами виртуальных сетей для обмена данными, в том числе с использованием глобальной информационной сети Интернет.	1. Выполнить проектирование виртуальной локальной сети и виртуальной частной сети в соответствии с политикой безопасности. 2. Разработать политику безопасности для удаленного администрирования виртуальной локальной сети и виртуальной частной сети, а также специализированной виртуальной сети в облачных сетевых структурах. 3. Используя сетевые средства виртуальных сетей для обмена данными, произвести резервное копирование конфигурации 4. Выполнить учет выполняемых действий учетной записи виртуальных локальных сетей и виртуальных частных сетей, а также	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	- Навыками обеспечения безопасности информации с помощью стандартных сетевых средств обмена информацией в виртуальных локальных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах. - Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, авторизации, аутентификации и аудита), виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению информационной безопасности;	1. Выполнить разграничение ролей с помощью уровня привилегий и присвоить команды к уровням привилегий 2. Настроить виртуальный терминал VTY для удаленного административного доступа 3. Произвести настройку удаленного доступа с применением SSH 4. Произвести настройку аудита действий пользователя с помощью стандартных средств обмена в виртуальных локальных сетях	
Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных;	1. Какие механизмы защиты являются общими для ОС и БД (СУБД)? 2. Перечислите характерные для технологии БД требования по безопасности данных. 3. Чем отличается управление доступом от управления целостностью БД? 4. В чем заключается сходство и различие механизмов управления доступом к БД, использующих таблицы (матрицы) доступа и внешнюю схему БД? 5. Предложите способы выявления косвенного предоставления права доступа для систем с динамическим управлением доступом (на примере СУБД DB). 6. Перечислите нарушения целостности БД, связанные с параллельным выполнением транзакций. 7. Назовите достаточное условие сериализуемости расписания выполнения транзакций. 8. Перечислите способы, позволяющие избежать тупиковых ситуаций. Перечислите способы выхода из состояния клинча транзакций. 9. Перечислите уровни восстановления БД. В чем заключается	Б1.В.ДВ.04.02 Защита программного обеспечения

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		сущность каждого уровня? 10. Защита программного обеспечения с помощью аппаратных ключей серии Guardant 11. Технологии аутентификации и шифрования. Реализация безопасной сетевой инфраструктуры для web-сервера. 12. Классификация firewall'ов и определение политики firewall'а. 13. Обеспечение безопасности web-серверов. Безопасность web-содержимого. Электронные цифровые сертификаты; SSL/TLS.	
Уметь	- разрабатывать и администрировать базы данных в соответствии с требования информационной безопасности; -настраивать защиту программного обеспечения с применением дистанционного администрирования	1. Провести администрирование реализуемой БД 2. Разработать защищенную авторизацию в БД 3. Разработать запросы к БД в защищенном исполнение 4. Реализовать защиту БД от SQL инъекций 5. Настроить защиту программного обеспечения с применением дистанционного администрирования	
Владеть	- методами настройки безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.	1. Разграничить права работы пользователей реализуемой БД и программного обеспечения 2. Выделить привилегии пользователей БД 3. Реализовать распределение меток безопасности и принудительного контроля доступа к программному обеспечению 4. Произвести настройку домена безопасности БД	
Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных; - основные средства и методы удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	- разрабатывать и администрировать базы данных в соответствии с требования информационной безопасности; -настраивать защиту программного обеспечения с применением дистанционного администрирования -настраивать удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии?	
Владеть	- методами настройки безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД. -средствами удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах -навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении			
Знать	- Классификацию уязвимостей. - Принципы систематизации уязвимостей.	1.Укажите основные категории уязвимостей 2. Приведите пример локальной уязвимости. 3. Приведите приме эксплуатационной уязвимости.	Б1.В.ДВ.03.01 Анализ безопасности информационных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4. Перечислите основные стандарты систематизации уязвимостей.	технологий
Уметь	- выполнять сканирование автоматизирование системы с цель выявления уязвимостей безопасности ИТ	1. Перечислить инструменты для выполнения сканирования уязвимостей доступные в виртуальной машине Kali Linux 2. При помощи ПО Nessus 7 выполнить сканирование уязвимостей целевой автоматизированной системе.	
Владеть	- навыками исследования уязвимостей автоматизированной системы	1. При помощи средств виртуальной машины Kali Linux исследовать заданную уязвимость, сформировать отчет. 2. При помощи MSFConsole выполнить автоматизированное исследование тестового информационно-технологического ресурса автоматизированной системы	
Знать	- основные понятия организации обеспечения информационной безопасности -основные методы организации обеспечения информационной безопасности; - принципы организации обеспечения информационной безопасности	1. ГОСТ Р МЭК 62443-3-3-2016 «Требования к системной безопасности и уровни безопасности» 2. Международные стандарты информационной безопасности 3. Международный стандарт электротехнической комиссии ANSI/ISA-62443. 4. Стандарт ISO 17799: Code of Practice for Information Security Management 5. Стандарт ISO 15408: Common Criteria for Information 6. Technology Security Evaluation 7. 6.1.3 Стандарт SysTrust 8. Стандарт BSI\IT Baseline Protection Manual 9. Правовой режим участия в международном информационном обмене.	Б1.В.ДВ.03.02 Информационная безопасность систем организационного управления
Уметь	-анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития; -организовывать и обеспечивать сохранение режима государственной тайны при выполнении функциональных обязанностей; - организовывать и обеспечивать сохранение режима конфиденциальности при	1. Регламентировать права доступа сотрудников к информации для выбранного объекта информатизации, указать цели этого доступа, требования по регламенту использования доступной информации. 2. Составить инструкции персонала основных подразделений для работы с информационными ресурсами в режиме совместного доступа с учетом требований информационной безопасности. 3. Разработать регламент реагирования на инциденты. Для	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	выполнении функциональных обязанностей;	выбранного объекта указать: основные источники информации об инцидентах, виды инцидентов, цели разбора инцидента, этапы, порядок проведения разбора инцидента, инструкции по оценке ущерба.	
Владеть	-методами формирования требований по защите объекта; -методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;	Провести анализ целесообразности реализации мероприятий по обеспечению информационной безопасности в заданных условиях.	
Знать	- – принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечению информационной безопасности	1. Правовые вопросы организации защиты информации 2. Организация работы с персоналом предприятия 3. Подбор и подготовка сотрудников отдела информационной безопасности 4. Организационно-правовые меры защиты информации на предприятии 5. Программные средства анализа рисков информационной безопасности. 6. Международные стандарты информационной безопасности 7. Стандарт ISO 17799: Code of Practice for Information Security Management 8. Стандарт ISO 15408: Common Criteria for Information 9. 6.1.3 Стандарт SysTrust 10. Стандарт BSI\IT Baseline Protection Manual 11. Стандарт COBIT 3 12. Анализ объекта защиты. Порядок и основные составляющие.	Б1.В.ДВ.05.02 Защита электронного документооборота
Уметь	-выявлять особенности и формировать требования к системе организации коллективной работы с информационными ресурсами СЭД -формировать комплекс мер по защите информации с учетом соответствия нормативным документам, технической реализуемости и экономической целесообразности;	1. В консоли администратора dlp- системы задать правила мониторинга активности рабочего стола: снятие скриншотов, анализ использования приложений, контроль буфера обмена, контроль нажатия клавиш на клавиатуре. Настроить блокировку запуска определенных приложений по атрибутам. 1. Для групп пользователей настроить правила контроля накопителей устройств:	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		• разрешить/запретить сохранять на эти устройства информацию; • создание теневых копий; • ограничить доступ полностью; • запретить запись, но разрешить чтение.	
Владеть	-навыками администрирования систем электронного документооборота -навыками настройки систем предотвращения утечек информации	Для решения задачи блокирования распространения конфиденциальной информации через каналы связи настроить правила безопасности для групп пользователей по протоколам SMTP, MAPI, HTTP . Создать сложные составные условия для контроля передачи данных, по ключевым фразам, определенным узлам. Создать имитацию инцидента. Проверить работу настроек правил.	
Знать	Этапы построения и использования СМИБ Семейство стандартов ISO/IEC 27000	1. Способы контроля и оценки эффективности имеющихся средств управления и процедур ИБ 2. Интегральный показатель эффективности СМИБ	Б1.Б.34 Управление информационной безопасностью
Уметь	Оценивать уровень знаний сотрудников в области ИБ Разрабатывать программы по обучению и повышению квалификации сотрудников в области ИБ Выявлять возможности улучшения СМИБ	Подготовить отчет по проведенному анализу защищенности: 1. Результаты анализа организационных уязвимостей 2. Распределение между ответственными лицами задач систем безопасности 3. Разработать методику оценки знаний сотрудников в области ИБ 4. Разработать инструкции для сотрудников по обеспечению организации защиты информации по требованиям ИБ	
Владеть	Навыками разработки плана обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ	По проведенному анализу защищенности подготовить: 1. Рекомендации по устранению организационных уязвимостей. 2. Разработать указания и требования Политики ИБ с учетом внедрения программно-аппаратных комплексов и введения различных инструкций	
	-основные методы организации обеспечения информационной безопасности;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта**	Б2.Б.03(П) Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- принципы организации обеспечения информационной безопасности - организационные меры защиты информации	**профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;	практика по получению профессиональных умений и опыта профессиональной деятельности
	-анализировать эффективность систем защиты информации и разрабатывать направления ее развития; -организовывать и обеспечивать сохранение режима государственной тайны; - организовывать и обеспечивать сохранение режима конфиденциальности; -формировать требования к защите информации, содержащейся в информационной системе -определить цели и задач защиты информации в информационной системе, основные этапы создания системы защиты информации		
	-методами формирования требований по защите объекта; -навыками разработки организационно-распорядительных документов		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Вопросы, подлежащие изучению: 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		периметровой охраны особо важных объектов	
Знать	-основные методы организации обеспечения информационной безопасности; - принципы организации обеспечения информационной безопасности - организационные меры защиты информации	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	-анализировать эффективность систем защиты информации и разрабатывать направления ее развития; -организовывать и обеспечивать сохранение режима государственной тайны; - организовывать и обеспечивать сохранение режима конфиденциальности; -формировать требования к защите информации, содержащейся в информационной системе -определить цели и задач защиты информации в информационной системе, основные этапы создания системы защиты информации		
Владеть	-методами формирования требований по защите объекта; -навыками разработки организационно-распорядительных документов		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ			
ПК-1 способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке			
Знать	основные приемы и методы, связанные с поиском, изучением, обобщением и систематизацией научно-технической информации	Исправьте грамматические ошибки по теме «Порядок слов в простом предложении» 1) We get usually up at 7 o'clock. 2 When you do your home assignment? 3) Where you were yesterday? Исправьте грамматические ошибки по теме «Числительное» 1) My birthday is on the twenty-one of September. 2) I am thirty (13) years old. 3) It is 5th of December. Исправьте грамматические ошибки по теме «Местоимение» 1)Peter is ill. Can you visit her? 2) The text is difficult. Do you understand all? 3) I haven't called somebody. Исправьте грамматические ошибки по теме «Существительное» 1) What are the news? 2) Three man came into the room and sat in the armchairs. 3) In evening we usually watch TV. Исправьте грамматические ошибки по теме «Прилагательное и наречие»	Б1.Б.02Иностранный язык

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		1) Everest ist the most tallest mountain in the world. 2) The results of the experiment turned out to be much best. 3) I think this song is worst than the previous one. Выберите правильный ответ на вопросы лингвострановедческого характера «Высшее образование в стране изучаемого языка» 1. What's the main difference between a college and a university in the USA? a) Colleges are smaller b) Colleges offer only undergraduate degrees c) Colleges are smaller and they offer only undergraduate degrees 2. What's the difference between a state (public university) and a private university? a) State universities are funded by the government b) State universities are usually larger and admit a wider range of students c) State universities are funded by the government and admit a wider range of students 3. Who funds private institutions of higher education in the USA? a) US government b) They are funded from tuition fees, research grants and gifts. Выберите правильный ответ на вопросы по страноведению «Геополитические особенности страны изучаемого языка» 1) How many countries does the United Kingdom consist of? a) 2 b) 3 c) 4 2) What is the state system of the United Kingdom? a) a constitutional monarchy	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		b) a parliamentary republic 3) What is the symbol of the United Kingdom? a) a rose b) a bald eagle c) Britannia Выберите правильный ответ на вопросы лингвострановедческого характера «Культура и традиции страны изучаемого языка» What is the Scottish national costume for men? a) the kilt b) the tuxedo c) the bearskin What is the most famous sport event in Scotland? a) the Highland games b) the Ccommonwealth Games c) the Wimbledon Championship What country is called a land of castles and princes? a) England b) Northern Ireland c) Wales Выберите правильный ответ на вопросы лингвострановедческого характера «Крупные города страны изучаемого языка» What are the best English resorts? a) Bristol and Southampton b) Brighton and Bath c) Leeds and Bradford What is the capital of Scotland? a) Manchester b) Edinburg	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		c) Liverpool What is the most important airport in England? a) Gatwick b) Heathrow c) Stansted	
Уметь	использовать основные приемы и методы для поиска, изучения, обобщения и систематизации научно-технической информации	Прочитайте текст и определите, является высказывание истинным или ложным. My Plans for the Future I am a first-year student now and I have chosen metallurgy as an area of specialization. I am sure it is a very demanding job. That is why I am looking now for opportunities for further development of my abilities and knowledge in the chosen field. For me, choosing a career is not only a matter of future prestige and wealth. In my opinion, a job should be interesting and socially important. To my mind, people should find satisfaction in their job. Money is naturally very important too. I am rather ambitious. I like to win competitions and be the best. I'd like to become a good spe-cialist. I am sure the most important qualities of a good specialist are to be hard-working, to speak foreign languages, to be scientifically-minded, to be energetic, to study for extra qualifica-tions in free time, to be sociable. I think I am good at mathematics and physics. It were my favourite subjects at school and I am sure it is one of the most important subjects at the University. I would like to be a monitor (the leader of the student Government at the Department). To my mind it is a good opportunity to develop my organizational and interpersonal skills and get a sol-id background. I am willing to be actively engaged in research and scientific discussions covering the problems of steel making technology improvement. I would like to take part in the student scientific con-ferences. My dream is to be a postgraduate student. My goal is to achieve a high degree of profi-ciency. I hope I'll get my Bachelor's degree in five years, and then I am planning to complete my master's degree. And I'd like to begin my PhD program. Postgraduate study at the university offers us the opportunity to study the subject of our first degree at an advanced level, or develop	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		new skills and knowledge. The University offers us the opportunity to enhance our career prospects by developing knowledge and skills relevant to our chosen career 1) The carrier choice is not socially important, but depends on your abilities. 2) The most important qualities of a good specialist are to be industrious, to speak several foreign languages, etc. 3) To develop the organizational and interpersonal skills and get a solid background one can become a monitor.	
Владеть	основными приемами и методами для поиска, изучения, обобщения и систематизации научно-технической информации	Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «О себе» to be a first-year student, to consist of, to live, my hobby is, I prefer, my favourite subjects, to spend time, at the university I, when I have free time, usually I Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Мои планы на будущее» My future specialty, department, carrier plans, to make a carrier, to do courses, to pick up a foreign language, a very demanding job, opportunities for further development of my abilities and knowledge, to take part in the student scientific conferences Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Значение иностранного языка в карьере будущего специалиста» to improve your career prospects, many benefits, give a competitive edge over other applicants, have the option to work abroad, miscommunication, feel more at ease when speaking with fellow employees, management, or clients. Составьте сообщение по предлагаемым темам, опираясь на основные лексические выражения: «Студенческая жизнь» the first step to independence, to achieve your study goals, to plan a timetable, to do a course work, to take time out from study, tutorials and labs, to hang out with friends, to attend lectures and classes	
Знать	основные приемы и методы, связанные с поиском, изучением, обобщением и	Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Географическое положение и	Б1.Б.44Иностранный язык в профессиональной

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	систематизацией научно-технической информации	политическая система страны изучаемого языка» Constitutional monarchy Корона County ВВП Island Конституционна монархия Gross national product Остров Crown Графство Соотнесите английские слова и выражения с их русскими эквивалентами по теме «Культура и традиции страны изучаемого языка» Originate Происходить Annual celebration Ежегодное празднование Religious significance Религиозное значение Official days off Фейерверк Fireworks Официальные выходные Исправьте грамматические ошибки по теме «Числительное» 1) My birthday is on the twenty-one of September. 2) I am thirty (13) years old. 3) It is 5th of December. Исправьте грамматические ошибки по теме «Местоимение» 1)Peter is ill. Can you visit her? 2) The text is difficult. Do you understand all? 3) I haven’t called somebody. Исправьте грамматические ошибки по теме «Существительное» 1) What are the news? 2) Three man came into the room and sat in the armchairs. 3) In evening we usually watch TV. Исправьте грамматические ошибки по теме «Прилагательное и наречие»	деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		1) Everest ist the most tallest mountain in the world. 2) The results of the experiment turned out to be much best. 3) I think this song is worst than the previous one. Выберите правильный ответ на вопросы лингвострановедческого характера «Высшее образование в стране изучаемого языка» 1. What's the main difference between a college and a university in the USA? a) Colleges are smaller b) Colleges offer only undergraduate degrees c) Colleges are smaller and they offer only undergraduate degrees 2. What's the difference between a state (public university) and a private university? a) State universities are funded by the government b) State universities are usually larger and admit a wider range of students c) State universities are funded by the government and admit a wider range of students 3. Who funds private institutions of higher education in the USA? a) US government b) They are funded from tuition fees, research grants and gifts. Выберите правильный ответ на вопросы по страноведению «Геополитические особенности страны изучаемого языка» 1) How many countries does the United Kingdom consist of? a) 2 b) 3 c) 4 2) What is the state system of the United Kingdom? a) a constitutional monarchy	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		b) a parliamentary republic 3) What is the symbol of the United Kingdom? a) a rose b) a bald eagle c) Britannia	
Уметь	использовать основные приемы и методы для поиска, изучения, обобщения и систематизации научно-технической информации	Прочитайте текст и определите, является высказывание истинным или ложным. Colleges, universities, and institutes: the distinctions Degree-granting institutions in the United States can be called colleges, institutes or universities. As a general rule, colleges tend to be smaller and usually offer only undergraduate degrees, while a university also offers graduate degrees. The words “school”, “college”, and “university” are often used interchangeably. An institute usually specializes in degree programs in a group of closely related subject areas, so you will also come across degree programs offered at institutes of technology, institutes of fashion, institutes of art and design, and so on. Within each college or university you will find schools, such as the school of arts and sciences or the school of business. Each school is responsible for the degree programs offered by the college or university in that area of study. Technical and vocational colleges. These institutions specialize in preparing students for entry into, or promotion within, the world of work. They offer certificate and other short-term programs that train students in the theory behind a specific vocation or technology, as well as how to work with the technology. Programs usually last two years or less. There are several thousand technical and vocational colleges across the United States, and they may be private or public institutions. State universities are founded and subsidized by U.S. state governments (for example, California, Michigan or Texas) to provide low-cost education to residents of that state. They may also be called public universities to distinguish them from private institutions. Some include the words “state university” in their title or include a regional element such as “eastern” or “northern”. State universities tend to be very large, within enrollments of 20, 000 or more students, and generally admit a wider range of students than private universities. State	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		university tuition costs are generally lower than those of private universities. Also, in-state residents (those who live and pay taxes in that particular state) pay much lower tuition than out-of-state residents. International students, as well as those from other states, are considered out-of-state residents and therefore do not benefit from reduced tuition at state institutions. In addition, international students may have to fulfill higher admission requirements than in-state residents. Private universities are funded by a combination of endowments, tuition fees, research grants, and gifts from their alumni. Tuition fees tend to be higher at private universities than at state universities, but there is no destinction made between state and non-state residents. Colleges with a religious affiliation and single-sex colleges are private. In general, private universities have enrollments of fewer than 20,000 students, and private colleges may have 2,000 or fewer students on their campuses. 1) State university tuition costs are generally lower than those of private universities. 2) Within each college or university you will find schools. 3) Technical and vocational colleges offer certificate and other short-term programs that train students in the theory behind a specific vocation or technology, as well as in how to work with the technology. Дополните диалог, используя предложенные ниже реплики Jane: Hello, Maria! You look great today! Maria: _____It's very warm today, isn't it? So I have decided to put on my new dress. Jane: Yes, the weather is lovely, as well as your new dress. But have you heard about the rain this afternoon? Maria: _____But that is okey. I have an umbrella. Jane: Oh, you are lucky, but I have no umbrella. I need to go back home to take it. Maria: Yes, be quick. Look, the sky is already full of clouds. Jane: I run. Bye, _____ Maria: Bye! Yes, I've heard about that. Hi,! Thank you! see you later.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	основными приемами и методами для поиска, изучения, обобщения и систематизации научно-технической информации	Терминологический словарь по направлению подготовки. 1. Укажите, в каких значениях употребляются следующие слова и термины, и переведите их. 1. shaft; 2. pin; 3. turn (sing, pl); 4. relay; 5. capacity; 6. handling; 7. error; 8. developing; 9. average; 10. plate; 11. female; 12. bed; 13. flight; 14. grid; 15. course; 16. hammering; 17. hand; 18. kick; 19. kill; 20. maintenance; 21. trouble; 22. trolley; 23. smash. 2. Переведите следующие термины на русский язык. 1. flywheel; 2. trip coil; 3. clock-word; 4. circuit; 5. safety; 6. switch; 7. brake gear; 8. ionic rectifier; 9. capacitor; 10. back coupling; 11. Flat rate; 12. stress; 13. electric charge; 14. winding; 15. ring; 16. friction coupler; 17. gear; 18. variable capacitor; 19. microphone; 20. electronic instrument; 21. coil. 3. Переведите следующие терминологические словосочетания на русский язык. 1. associated mode of operations; 2. data signal quality detection; 3. connection through an exchange; 4. effectively transmitted signals in sound-program transmission; 5. error-detecting system; 6. optional user facility; 7. public data transmission service; 8. two-way – alternate interaction; 9. pair of complementary channels; 10. time consistent busy hour; 11. ratio of compression; 12. indirect manual demand operation; 13. External loss time; 14. setting-up times of an international call; 15. digital line pass; 16. mean time between interruptions; 17. automatic booked call service; 18. centralized multi-end-point-connection; 19. level of maintenance; 20. emergency call service; 21. probability of successful service completion; 22. error correction by detection and repetition. 4. Переведите термины-словосочетания. 1. oil dashpots; 2. under-voltage; 3. arcing contact; 4. exhaust velocity;5. combustion zone; 6. locomotive servicing; 7. long distance call;8. play load weight; 9. out-going terminus; 10. connected clamp; 11. Good combustion; 12. over-current; 13. oil retainer; 14. excitation circuit; 15. By pass valve; 16. trip-coil; 17. Super heater header; 18. bus-bar terminals;19. tuning condenser; 20. wet battery; 21. alarm device; 22. Instrument transformer; 23. voltage transformer; 24. Pole tip; 25. boiling point;26. yield point; 27. fixed point; 28. fixed seat; 29. feed	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		mechanism;30. ceiling voltage; 31. power station; 32. power train; 33. train handling;34. train communication; 35. horse power; 36. fixing device; 37. Fixing lug; 38. flash coating; 39. flash light; 40. flash period; 41. flash suppressor. 5. Переведите много компонентные термины-словосочетания: a) a single-phase direct current locomotive, the bilateral axle box guides, a motor driven oil pump, auxiliary equipment, load and spud condition, three phase asynchronous motors, a given attractive effort characteristic, a new series of electric locomotives, high voltage d.c. motors; b) small-size universal electronic computers, the 1990 figures, a high level peace meeting, a 40-foot-long rocket powered plane, a ten per cent wage increase, the average sized motor car, the newly built locomotive repairing shop, the Fifth World Trade Union Congress. 6. Дайте варианты перевода выделенных терминов и терминологических словосочетаний на русский язык в следующих предложениях. 1. There are two basic ways to obtain plastic flow: the first by direct bearing on normal loading of the seal surfaces. 2. The incoming cross-country crude oil pipeline will be cathodically protected with an impressed current cathodic protection system designed and installed by others. The local piping will be electrically isolated from the transmission line, and underground portions will be protected plastic models of turbine casings, in-service strain and ultrasonic measurements on operational super headers, and in-pile biaxial tests and measurements on zirconium tubes were some of the practical problems discussed. 4. Concentration of the same amount of ionization in a thin-down, however, may become biologically significant in organs such as the hypothalamus, or ocular lens where loss of a few cells is crucial. 5. A core competence is something that a company does well relative to other internal activities. 6. A distinctive competence is something a company does well relative to competitors. 7. Diesel engine exhaust and some other constituents are known to the State of California to cause cancer, birth defects, and other	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		reproductive harm. 8. The transmitting stations shall conform to the maximum permitted spurious emission power levels. 9. The coast stations shall not occupy the idle radio telephone channels by emitting the identification signals, such as those generated by the call ships or tapes. 10. The signals for testing and adjustment shall be chosen in such a manner that no confusion will arise with a signal, abbreviation, etc, having a special meaning defined by the International Code of Signals.	
Знать	• Основы построения систем обработки и передачи информации, их современное состояние развития. • Основные задачи обеспечения безопасности информации в компьютерных и автоматизированных системах. • Особенности обработки информации с использованием компьютерных систем	1. Дайте определение понятию «информация». Дайте определение понятию «информационные технологии». 2. Дайте определение понятию «информационная система». 3. Дайте определение понятию «информационно-телекоммуникационная сеть». Дайте определение понятию «обладатель информации». Назовите его права и обязанности 4. Определите понятия «доступ к информации» и «конфиденциальность информации». 5. Определите понятия «предоставление информации» и «распространение информации». 6. Определите понятия «электронное сообщение», «документированная информация» и «электронный документ». 7. Дайте определение понятию «оператор информационной системы» 8. Определите классификацию информационных войн. 9. Какие объекты воздействия у информационных войн?. Какие существуют технические каналы утечки информации? 10. Как существуют средства защиты от утечки по техническим каналам? 11. Дайте определение стеганографии и криптографии. В чем их отличие?	Б1.Б.39Введение в специальность
Уметь	• Осуществлять поиск и систематизировать современную научно- техническую информацию	Провести анализ современной научно-технической информации на следующие темы:	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	по рассматриваемым вопросам в рамках дисциплины. • Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.	1. Правовая охрана программ и данных. Защита информации. 2. Методы защиты информации 3. Системы защиты информации 4. Защита баз данных 5. Защита информации от несанкционированного доступа методом криптопреобразования 6. Защита цифровой информации методами стеганографии 7. Компьютерные вирусы, типы вирусов, методы борьбы с вирусами. 8. Информационный потенциал общества. 9. Человек в информационном обществе. 10. Коллективное использование разнородных информационных ресурсов	
Владеть	• Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. • Навыками осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	1. Провести сравнительный анализ доктрины информационной безопасности от 2000г и 2016г 2. Осуществить поиск и составить список основных федеральных законов в области информационной безопасности РФ	
Знать	особенности обработки информации в сфере Big Data	1. Основные функции библиотеки Pandas для объединения Big Data из различных источников. 2. Укажите используемую инфраструктуру для хранения, обработки и передачи Big Data. 3. Технологии поиска Big Data: обычный поиск, полнотекстовый и интеграция данных. 4. Возможности систематизации Big Data с использованием технологии MapReduce. 5. Поиск в структурированных, полуструктурированных и неструктурированных Big Data. 6. Технологии облачного хранения Big Data. 7. Хранилища данных (Data Warehouse). Типы хранилищ. ЦОДы	Б1.Б.43 Основы Data инжиниринга

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	обобщать, систематизировать, обеспечивать надежную инфраструктуру полученной научно-технической информации в сфере data инжиниринг.	**Задача**. Представьте витрину данных, которая будет описывать источники данных, используемые учреждением или организацией. Составьте реестр исходных данных с описанием обменных форматов. **Задача**. Опишите метаданные и структуру данных в указанной предметной области. Опишите жизненный цикл метаданных. Проведите анализ контента и оценку требований. Запишите спецификацию системных требований.	
Владеть	методами сбора и обобщения научно-технической информации по теоретическим сведениям, проблемам и задачам, решаемым в курсе "Data Инжиниринг", в т.ч. с использованием литературы на иностранном языке.	**Задача.** С помощью информационно-поисковых систем осуществите поиск из внешних источников научно-технической информации в области информационной безопасности на иностранном языке в структуре Hadoop. **Задание.** Определите, какое количество 10 Тб HDD необходимо для хранения набора данных, содержащего координаты, скорости и метаинформацию (тип объекта и время измерения по указанной характеристике) для всех объектов на территории аэропорта.	
Знать	- Основы построения систем обработки и передачи информации, их современное состояние развития. -Современные поисковые системы и базы данных в сфере профессиональной деятельности. Язык запросов и организацию поиска научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности - Особенности обработки информации с использованием компьютерных систем	***индивидуальное задание на производственную практику:*** *Список индивидуальных тем* 1. Современные средства защиты информации 2. Современные системы компьютерной безопасности 3. Современные криптографические системы 4. Криптоанализ, современное состояние 5. Правовые основы защиты информации 6. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними 7. Технические аспекты обеспечения защиты информации. 8. Атаки на систему безопасности и современные методы защиты 9. Современные пути решения проблемы информационной безопасности РФ 10. Организация центра мониторинга событий на основе современных систем анализа информационной безопасности 11. Информационная безопасность в условиях цифровой экономики Российской Федерации 12. Безопасность сетей беспроводной передачи данных	Б2.Б.01(У) Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	- Проводить поиск, обобщение и систематизацию современной научно -технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам. - Анализировать современную научно-техническую информацию по рассматриваемым в рамках учебной-практики проблемам и задачам.		
Владеть	- Навыками сбора современной научно-технической информации по рассматриваемым в		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	рамках учебной-практики проблемам и задачам. - Навыками проведения исследовательских работ по рассматриваемым в рамках учебной-практики проблемам и задачам	13. Использование хэш-функций в современном мире и их криптостойкость 14. Проблемы применения средств защиты информации в операционной системе Windows 15. Алгоритмы тестирования генераторов псевдослучайных чисел 16. Система накопления и анализа данных для контроля за инцидентами в сфере информационной безопасности с учетом поведенческого подхода 17. Анализ законодательства в области размещения и использования ИТСНК на территории Российской Федерации 18. Анализ угроз безопасности информации. Возможные организационные меры, применяемые для нейтрализации ряда угроз безопасности информации 19. Актуальность обеспечения информационной безопасности на промышленных предприятиях 20. Безопасность в мире «Интернета вещей» 21. Безопасность распознавания личности по отпечаткам пальцев 22. Применение искусственных нейронных сетей для выявления инцидентов информационной безопасности 23. Угрозы информационной безопасности при «оплате в одно касание». 24. Анализ нормативной документации, регламентирующей ответственность за утечку сведений, составляющих государственную тайну 25. Математические модели в информационной безопасности 26. Обзор нормативно-правовой базы в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации 27. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований Cookie: принципы работы и безопасность использования	
Знать	Основы построения систем обработки и	*перечень вопросов на защите отчета НИР:*	Б2.Б.02(Н) Научно-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	передачи информации, их современное состояние развития. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах. Особенности обработки информации с использованием компьютерных систем	1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР? Какие охранные документы были получены в ходе выполнения НИР?	исследовательская работа
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно- технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.		
Владеть	Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Навыками участия в проведении исследовательских работ по рассматриваемым в рамках дисциплины проблемам и задачам. Основными методами научного познания в области защиты информации автоматизированных систем, а так же их применения к решению прикладных задач.		
Знать	- Основы построения систем обработки и передачи информации, их современное состояние развития. -Современные поисковые системы и базы данных в сфере профессиональной деятельности. Язык запросов и организацию поиска научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых	Б2.Б.04(Пд) Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- Особенности обработки информации с использованием компьютерных систем	практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на	
Уметь	- Проводить поиск, обобщение и систематизацию современной научно -технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам. - Анализировать современную научно-техническую информацию по рассматриваемым в рамках учебной-практики проблемам и задачам.		
Владеть	- Навыками сбора современной научно-технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам. - Навыками проведения исследовательских работ по рассматриваемым в рамках учебной-практики проблемам и задачам		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-2	**способностью создавать и исследовать модели автоматизированных систем**		
Знать	- структуру и состав автоматизированных систем управления - информационные и технологические ресурсы автоматизированных систем	Перечень вопросов: 1. Функциональная часть автоматизированной информационной системы 2. Виды автоматизированных информационных систем	Б1.В.06 Защита информационно-технологических ресурсов автоматизированных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- способы определения и представления информационных потоков автоматизированных систем	3. Программное и техническое обеспечение АИС 4. Методология структурного анализа и проектирования, интегрирующая процесс моделирования (SADT) 5. Методология и стандарт функционального моделирования(IDEF0) 6. Методология моделирования и стандарт документирования процессов, происходящих в систем(IDEF3) 7. Диаграммы потоков данных(DFD)	систем
Уметь:	- проводить исследование модели автоматизированной системы - определять и классифицировать информационно-технологические ресурсы АС	Разработать диаграмму потоков данных для следующих АИС: 1. Охранная частная организация 2. Медицинское учреждение 3. Образовательное учреждение Определить и классифицировать информационно-технологические ресурсы	
Владеть	- навыками анализа информационной инфраструктуры автоматизированной системы; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.	Разработать модели потоков данных и процессов, происходящих в системе, для следующих АИС: 1. Охранная частная организация 2. Медицинское учреждение 3. Образовательное учреждение Провести анализ информационной инфраструктуры. Определить и категорировать информационные ресурсы организации подлежащие защите.	
Знать	Основные информационные технологии, используемые в автоматизированных системах;─ Классификацию современных автоматизированных систем;─ Основные методы и технологии проектирования, моделирования, исследования автоматизированных систем.Теоретические вопросы 1.Выпуклое	метод. Метод искуственногобазиса. Анализ устойчивости решения, анализ чувствительности оптимальных решений к изменениям параметров управления. Решение двойственных задач линейного программирования. Интерпретация двойственных переменных.4.Транспортная задача. Необходимое и достаточное условия ее разрешимости.5.Способы решения задач о назначении. Венгерский метод решения. Задачи распределительного	Б1.В.ДВ.02.01 Основы теории оптимизации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	программирование. Локальный и глобальный минимум. 2.8. Линейное программирование. Постановка задачи. Двойственные задачи. Примеры задач ЛП.3.Симплекс	типа.Уметь─ Демонстрировать способность и готовность к решению задач оптимизации применительно к различным предметным областям;─ Определять возможность применения основных положений и методов теории оптимизации для организации мер по защите информации в автоматизированных системах;─ Находить оптимальные стратегиивыбора средств защиты информации.1.•Написать приложение для решения задачи одномерной оптимизации методом покоординатного спуска. Оценить реализованный метод : скорость сходимости, вычислительная и аналитическая сложность.2.Найти минимум целевой функции методом покоординатного спуска: U=x1^2+x2^2+1.5*x1*x2. Начальная точкаM0=(3;3).Считать, что минимум найден с заданной точностью, если расстояние между точками Miи Mi	
Уметь	Основные информационные технологии, используемые в автоматизированных системах;─ Классификацию современных автоматизированных систем;─ Основные методы и технологии проектирования, моделирования, исследования автоматизированных систем.Теоретические вопросы 1.Выпуклое программирование. Локальный и глобальный минимум. 2.8. Линейное программирование. Постановка задачи. Двойственные задачи. Примеры задач ЛП.3.Симплекс	метод. Метод искуственногобазиса. Анализ устойчивости решения, анализ чувствительности оптимальных решений к изменениям параметров управления. Решение двойственных задач линейного программирования. Интерпретация двойственных переменных.4.Транспортная задача. Необходимое и достаточное условия ее разрешимости.5.Способы решения задач о назначении. Венгерский метод решения. Задачи распределительного типа.Уметь─ Демонстрировать способность и готовность к решению задач оптимизации применительно к различным предметным областям;─ Определять возможность применения основных положений и методов теории оптимизации для организации мер по защите информации в автоматизированных системах;─ Находить оптимальные стратегиивыбора средств защиты информации.1.•Написать приложение для решения задачи одномерной оптимизации методом покоординатного спуска. Оценить реализованный метод : скорость сходимости, вычислительная и аналитическая сложность.2.Найти минимум целевой функции методом покоординатного спуска: U=x1^2+x2^2+1.5*x1*x2. Начальная точкаM0=(3;3).Считать, что минимум найден с заданной точностью, если расстояние между точками Miи Mi	
Владеть	Навыками использования стандартных	Навыками использования стандартных методов и моделей	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	методов и моделей математического анализа, теории оптимизации, а так же их применения к решению прикладных задач.─ 1.Реализовать алгоритмрешения задачи об укладке рюкзака.2.Написать приложение для решения задачи многомерной оптимизации методом Ньютона. Геометрическая интерпретация метода	математического анализа, теории оптимизации, а так же их применения к решению прикладных задач.─ 1.Реализовать алгоритмрешения задачи об укладке рюкзака.2.Написать приложение для решения задачи многомерной оптимизации методом Ньютона. Геометрическая интерпретация метода	
Знать	– Принципы и методы проектирования программно-аппаратного обеспечения; – Принципы и методы проектирования программно-аппаратного обеспечения; – Методы планирования и организации работ по защите информации.	1. Моделирование стационарного телеграфного сигнала с заданной интенсивностью числа смен знака, вычисление корреляционной функции, спектральной плотности мощности и статистической погрешности оценки этих функций. 2. Моделирование корреляционной функции белого шума на выходе фильтра низких частот первого порядка, полосового фильтра второго порядка, идеального полосового фильтра. 3. Сеточная модель акустического канала. Исследование зависимости амплитулно-частотных и фазо-частотных характеристики канала от согласования с нагрузкой. 4. Сеточная модель длинной линии связи. Исследование зависимости амплитудно -частотных и фазо-частотных характеристики линии связи от числа узлов сетки и от согласования с нагрузкой.	Б1.В.ДВ.02.02 Математическое моделирование распределенных систем
Уметь	– Разрабатывать и использовать профили защиты и задания по безопасности; – Готовить проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов; – Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы.	5. Произвести исследование с помощью модели переходных процессов и частотных характеристик системы. Выполнить анализ устойчивости. 6. Произвести моделирование стационарного телеграфного сигнала с заданной интенсивностью числа смен знака, вычисление корреляционной функции, спектральной плотности мощности и статистической погрешности оценки этих функций. 7. Произвести моделирование корреляционной функции белого шума на выходе фильтра низких частот первого порядка, полосового фильтра второго порядка, идеального полосового фильтра. 8. Генерация случайных графов с заданными свойствами. Метод допустимого выбора.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		9. Генерация деревьев, связных графов, ациклических графов. 10. Графы событий (ГС). Определение ГС. 11. Нахождение минимального набора переменных состояния, необходимых для однозначного воспроизведения поведения модели. 12. Нахождение пар событий, для которых возможна необходимость установления приоритета. 13. Редукция ГС. 14. Задачи анализа и оптимизации распределенных систем, которые удобно решать на моделях, представленных ГС. 15. Случайные графы. 16. Использование случайных графов в моделировании распределенных систем. 17. Моделирование и оптимизация потоков в случайных сетях.	
Владеть	– Навыками разработки технических заданий, рабочих проектов, планов и графиков проведения работ по защите информации; – Навыками выполнения требований нормативно-технической документации по соблюдению установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации; – Навыками проектирования программных и аппаратные средств защиты информации в соответствии с техническим заданием.	1. Выполнить моделирование собственных частот и форм (мод) колебаний подвижной системы консольного акселерометра. 2. Выполнить моделирование электростатического поля (скалярного поля потенциала и векторного поля напряженности), создаваемого системой точечных или линейных зарядов. 3. Выполнить моделирование топологии магнитного поля системы линейных токов, например, линий электропередачи. 4. Произвести моделирование и оптимизацию потоков в случайных сетях. 5. Произвести решение задачи анализа и оптимизации экономических систем, которые удобно решать на моделях, представленных случайными графами и сетями. 6. Выполнить построение сети Петри для простейшей модели управления запасами на складе готовой продукции. 7. Выполнить построение и анализ графа событий для модели малого производственного предприятия. 8. Произвести генерация случайных графов из заданного класса, соответствующего одной из моделей деятельности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		производственного предприятия	
Знать	-основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -методы оценки качества моделей, методы и средства моделирования и оптимизации бизнес-процессов -основные угрозы безопасности информации и модели нарушителя в автоматизированных системах -способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах	*перечень вопросов на защите отчета НИР:* 1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР? Какие охранные документы были получены в ходе выполнения НИР?	Б2.Б.02(Н) Научно-исследовательская работа
Уметь	-строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач -применять различные методы моделирования, исследования и верификации моделей -разрабатывать постановку задачи моделирования и выбирать методы и средства моделирования систем защиты информации − анализировать и оценивать угрозы информационной безопасности объекта; − разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем		
Владеть	навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач -навыками формализации задач и постановки задач моделирования -навыками выбора и обоснования критериев эффективности функционирования моделей		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	-навыками разработки, документирования информационных систем с учетом требований по обеспечению информационной безопасности; -навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите -методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем		
Знать	- основные принципы моделирования и виды моделей, требования, предъявляемые к моделям; - методы оценки качества моделей, методы и средства моделирования; - методы исследования моделей автоматизированных систем; - структуру и состав автоматизированных систем управления	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- применять различные методы моделирования автоматизированных систем; - выбирать методы и средства моделирования подсистем защиты информации; - анализировать и оценивать угрозы информационной безопасности объекта.		
Владеть	- навыками анализа информационной инфраструктуры автоматизированной системы; - методами моделирования автоматизированных систем; - основами построения моделей автоматизированных систем; - навыками формализации задач и постановки задач моделирования; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-3	**способностью проводить анализ защищенности автоматизированных систем**		
Знать	Основы методологии научных исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Классификацию современных компьютерных систем. Современные способы использования компьютерных технологий для проведения исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.	1. Понятие информационной безопасности государства. 2. Источники угроз информационной безопасности для объекта информатизации. 3. Классификация угроз информационной безопасности для объекта информатизации. 4. Требования защиты информации.	Б1.Б.26Основы информационной безопасности
Уметь	Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. Анализировать основные узлы и устройства современных автоматизированных систем. Пользоваться сетевыми информационными ресурсами для подбора необходимых современных	1. Определить угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду. 2. Определить угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	компьютерных систем и правил работы в этих системах. Эффективно использовать современные компьютерные технологии для изучения предмета исследования.		
Владеть	Представлением о возможности использования информационных технологий для решения профессиональных задач. Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности. Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности. Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.	1. Составить перечень программного обеспечения, позволяющего автоматизировать работу в области ИБ. 2. Составить перечень сертифицированных средств ЗИ от НСД. 3. Составить перечень средств СКЗИ.	
Знать	Критерии оценки эффективности и надежности средств защиты распределенных информационных систем. Принципы построения и функционирования распределенных информационных систем в защищённом исполнении. Методики анализа и контроля защищенности РИС в защищённом исполнении.	Вопросы к экзамену: 1. Определение сведений, представляющих для организации интеллектуальную собственность. 2. Примерный перечень сведений, составляющих служебную или коммерческую тайну организации. 3. Этапы работ по проектированию системы ИБ.	Б1.Б.36Информационная безопасность распределенных информационных систем
Уметь	Анализировать техническую и сопроводительную документацию по обеспечению ИБ. Анализировать программные и архитектурно-технические решения компонентов автоматизированных систем в защищённом исполнении.	1. Составьте предварительный Перечень сведений, содержащих служебную или коммерческую тайну, для структурных подразделений (отделов, служб) выбранной организации. 2. Определите возможный ущерб, в результате несанкционированного распространения сведений, включаемых в Перечень для выбранного предприятия.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	Проводить выбор технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты.	3. Определите затраты на защиту рассматриваемых сведений для выбранного предприятия. 4. Определите перечень контрмер, обеспечивающих ИБ выбранного объекта.	
Владеть	Навыками анализа основных узлов автоматизированных систем. Навыками анализа основных узлов автоматизированных систем в защищённом исполнении. Методами и технологиями проектирования, моделирования, исследования автоматизированных систем в защищённом исполнении.	1. Разработайте сценарий осуществления противоправных действий и список ранжированных угроз для выбранного предприятия. 2. Определите величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость для выбранного предприятия. 3. Создайте информационно-логическую модель для выбранного предприятия.	
Знать	- перечень инструментов для проведения анализа уязвимостей программного обеспечения; - базовый функционал инструментов для проведения анализа уязвимостей программного обеспечения;	1. В чем проблемы проведения доказательства правильности программного обеспечения с помощью формальных методов? 2. Приведите отличие техники формального доказательства правильности программного обеспечения от символьного выполнения программ? 3. Дайте определение верификации и валидации программного обеспечения. 4. В чем суть композиции верифицированных программ? 5. Расскажите о международном проекте по верификации программного обеспечения. 6. Перечислите контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения. 7. Какие бывают проблемы анализа безопасности программного обеспечения? 8. Назовите основные угрозы безопасности программного	Б1.В.09 Анализ уязвимостей программного обеспечения

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обеспечения. 9. Что такое алгоритмические и программные закладки программного обеспечения? 10. Приведите классификацию методов и средств анализа безопасности программ.	
Уметь	- применять технические средства для проведения анализа уязвимостей программного обеспечения	Определить протокол, используемый для авторизации участников сети. Выполнить атаку Pixie Dust. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности программного обеспечения.	
Владеть	- навыками работы с специализированным программным обеспечением для проведения анализа безопасности программного обеспечения	Провести комплексный тест выбранного экземпляра ПО при помощи инструментов дистрибутива Kali Linux 2.	
Знать	- Критерии оценки эффективности и надежности средств защиты распределенных информационных систем - Принципы построения и функционирования распределенных информационных систем в защищённом исполнении -Мероприятия для обеспечения защиты информации	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-Анализировать техническую и сопроводительную документацию по обеспечению ИБ. -Анализировать целесообразность выбора технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты. -Проводить контроль за событиями безопасности и действиями пользователей в информационной системе -Проводить анализ и оценку		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	функционирования системы защиты информации информационной системы	оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной	
Владеть	-Навыками выбора средств защиты информации -Навыками документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Критерии оценки эффективности и надежности средств защиты распределенных информационных систем - Принципы построения и функционирования распределенных информационных систем в защищённом исполнении -Мероприятия для обеспечения защиты информации	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	-Анализировать техническую и сопроводительную документацию по обеспечению ИБ. -Анализировать целесообразность выбора технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	-Проводить контроль за событиями безопасности и действиями пользователей в информационной системе -Проводить анализ и оценку функционирования системы защиты информации информационной системы	применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим	
Владеть	-Навыками выбора средств защиты информации -Навыками документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-4	**способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы**		
Знать	-Методы и средства разработки моделей на основе теории графов -Методы, средства для построения модели угроз и модели нарушителя информационной безопасности на основе теории графов	1. Перечислить подходы, которые могут быть применены для моделирования СЗИ 2. Графовые модели компьютерных атак 3. Риск-ориентированные модели систем защиты информации 4. Перечислите виды графов атак. Приведите примеры 5. Применение алгоритмов поиска точки сочленения, мостови блоков графа для нахождения критических узлов сетевых коммуникаций. 6. Критические вершины и ребра.	Б1.Б.19Теория графов и ее приложения

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	-Использовать технологии автоматизированного проектирования информационных систем -Применять методы теории графов для построения модели нарушителя в автоматизированных системах	1. Составить матрицу смежности и списки смежности для представления заданного ориентированного графа. Оценить размер вычислительных ресурсов для хранения и обработки созданных структур данных. 2. Написать программу (C++, Delphi, Java, C#- на выбор), реализовать представление компьютерной сети в виде графа. Найти критические компоненты	
Владеть	-Навыками применения графовых алгоритмов для определения ресурсов, необходимых для обеспечения безопасности информационной системы -Методами построения моделей для контроля эффективности мер защиты информации	На основе перечня активов предприятия составить граф уязвимостей ИС. Ребрам графа соответствуют реализации этих уязвимостей, вес ребра- вероятность реализации, Реализовать на языке программирования высокого уровня один из алгоритмов поиска кратчайших путей для заданного графа угроз ИС. Обосновать применение алгоритма к графу данного вида.	
Знать	– основные источники угроз ИБ; – классификацию угроз информационной безопасности; – Типовую модель угроз информационной безопасности – Нормативно-методические документы в области моделирования угроз, – способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах;	Перечень вопросов к экзамену 1. Угрозы мобильным устройствам. 2. Угрозы безопасности ПДн. 3. Каналы реализации угроз безопасности ПДн. 4. Угрозы за счет реализации ТКУИ. 5. Классификация угроз безопасности персональных данных по способу реализации. 6. Общая характеристика уязвимостей информационной системы персональных данных. Классификация, Причины возникновения уязвимостей. 7. Наиболее часто реализуемые угрозы. 8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 9. Ошибки, возникающие при моделировании угроз.	Б1.В.02 Моделирование угроз информационной безопасности
Уметь	– Разрабатывать частную модель угроз автоматизированной системы – Определять актуальные угрозы для автоматизированной системы; – разрабатывать модель нарушителя	Задание 1.Определить источники угроз для объекта информатизации. 2. Сформировать список уязвимостей объекта защиты, которые могут быть использованы для реализации угроз.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.	3. Определить перечень угроз безопасности на основе имеющихся отечественных каталогов угроз. 4. Определить Типы и возможности нарушителей	
Владеть	– Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; – Навыками разработки частных моделей угроз	Задание 1. Составить частную модель угроз ПДн объекта информатизации 2. Построить дерево угроз АС. 3. Составить модель нарушителя	
Знать	- нормативные и правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; - основы функционирования ГосСОПКА; - понятия объектов и субъектов КИИ;	Теоретические вопросы: 1. Федеральный закон №187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры РФ» 2. Положение о банке данных угроз безопасности информации. 3. Форма акта проверки, составляемого по итогам проведения гос. контроля в области обеспечения безопасности значимых объектов КИИ РФ. 4. Требования по обеспечению безопасности значимых объектов КИИ РФ. 5. Перечень объектов КИИ РФ подлежащих категорированию	Б1.В.11 Обеспечение информационной безопасности критической информационной инфраструктурой
Уметь	- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ; - способы реализации угроз безопасности и возможные последствия от их реализации; - определять требования по устранению возможных уязвимостей, приводящих к возникновению угроз безопасности информации;	Задания: *1.* Составить майнд-карту угроз безопасности информации (УБИ) значимого объекта КИИ. *2.* Составить майнд-карты оценки возможностей внешних и внутренних нарушителей для значимого объекта КИИ.	
Владеть	- навыками работы с нормативными и правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов	Задания: 1. Составить перечень показателей критериев значимости объектов КИИ РФ. 2. Выбрать из информационной системы «Банк данных УБИ	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	КИИ; - навыками работы с информационными базами данных, содержащими информацию по угрозам безопасности информации и уязвимостями ПО значимых объектов КИИ; - навыками выявления и анализа угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ;	ФСТЭК России» УБИ по результатам оценки возможностей внешних и внутренних нарушителей значимого объекта КИИ. 3. Выбрать из информационной системы «Банк данных УБИ ФСТЭК России» УБИ по результатам анализа уязвимостей значимого объекта КИИ.	
Знать	-Базовую модель угроз ПДн -Нормативно-методические документы в области моделирования угроз -Способы реализации угроз безопасности информации -Типы нарушителя информационной безопасности в автоматизированных системах -Методику разработки модели угроз	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-Разрабатывать частную модель угроз автоматизированной системы -Определять актуальные угрозы для автоматизированной системы; -Разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.		
Владеть	- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - Навыками разработки частных моделей угроз		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	-Базовую модель угроз ПДн -Нормативно-методические документы в области моделирования угроз -Способы реализации угроз безопасности информации -Типы нарушителя информационной безопасности в автоматизированных системах -Методику разработки модели угроз	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:*	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	-Разрабатывать частную модель угроз автоматизированной системы -Определять актуальные угрозы для автоматизированной системы; -Разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.		
Владеть	- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - Навыками разработки частных моделей угроз		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-5	**способностью проводить анализ рисков информационной безопасности автоматизированной системы**		
Знать	– методологию анализа рисков информационной безопасности – методики определения информационно-технологических ресурсов, подлежащих защите – способы применения анализа рисков в информационной безопасности при работе над междисциплинарными проектами – перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами	1. Назвать угрозы информационной безопасности в информационных системах. 2. Перечислить оценочные стандарты в информационной безопасности. 3. Описать «Оранжевую книгу» как оценочный стандарт. 4. Международный стандарт ISO/IEC 15408. Описать критерии оценки безопасности информационных систем. 5. Перечислить стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. 6. Международный стандарт ISO/IEC 27001:2005 Назвать требования к системам управления информационной безопасностью. 7. Сертификация СУИБ на соответствие ISO 27001.	Б1.В.05 Анализ рисков информационной безопасности
Уметь	– применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами	Провести расчеты оценки рисков информационной безопасности компании по методу оценки рисков на основе частной модели угроз.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	– выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите		
Владеть	– терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите – навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	***Задание:*** Для заданного предприятия определить: информационные активы компании; ценность активов; какие угрозы могут повлиять на информационные активы; с помощью каких механизмов можно защитить ключевые активы; уровень риска и предполагаемых потерь. провести оценку рисков ИБ (по выдранной методике): инвентаризацию информационных активов и их стоимости; определение методологии, необходимой для проведения оценки рисков и ее применение в конкретной компании; анализ возможных угроз и уязвимостей; определение мер, направленных на осуществление ИБ; создать матрицу рисков; осуществить количественную и качественную оценку рисков; подготовить отчет о выполненной работе по оценке рисков; подготовить плана оптимизации рисков.	
Знать	- методологию анализа рисков информационной безопасности; - методики определения информационно-технологических ресурсов, подлежащих защите;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите. -оценить риски информационной безопасности автоматизированной системы		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	- навыками анализа рисков информационной безопасности автоматизированных систем -методиками анализа рисков	требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- методологию анализа рисков информационной безопасности; - методики определения информационно-технологических ресурсов, подлежащих защите;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- выполнять анализ особенностей деятельности организации и использования в ней		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите. -оценить риски информационной безопасности автоматизированной системы	знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на	
Владеть	- навыками анализа рисков информационной безопасности автоматизированных систем -методиками анализа рисков		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности			

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Знать	Основные информационные технологии, используемые в автоматизированных системах. Сущность и понятие информационной безопасности и характеристику ее составляющих. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.	Вопросы для зачета 8. Угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду. 9. Классификация защищаемой информации по видам тайны. 10. Классификация защищаемой информации по степеням конфиденциальности. 11. Стратегия развития информационного общества в России.	Б1.Б.26Основы информационной безопасности
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности. Анализировать современную научно-техническую информацию по информационной безопасности. Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	1. Определить угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду. 2. Определить угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.	
Владеть	Основными методами научного познания в области защиты информации. Навыками участия в проведении исследовательских работ по информационной безопасности. Профессиональной терминологией в области информационной безопасности. Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах	1. На основе проведенного анализа нормативно-правовых документов в области защиты информации автоматизированных систем разработать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах на современном уровне развития общества.	
Знать	- Основные каналы обмена данными между программными компонентами распределенной системы. - способы организации программных компонент	1.Укажите порядок действий программной компоненты при инициализации канала связи по протоколу TCP/IP 2. Правила записи провайдера для подключения к SQL БД 3. Применение ODBC при подключении к БД	Б1.Б.37 Методы проектирования

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	распределенной системы разных уровней - объектно-реляционную модель взаимодействия между базами данных и программными компонентами.	4. Какое представление имеет таблица базы данных в программной компоненте при применении объектно-реляционной модели.	защищенных распределенных информационных систем
Уметь	- применять паттерн MVC при проектировании распределенных систем. - применять паттерн ORM при проектировании распределенных систем	1. По заданной структуре БД разработать программную модель БД. 2. Укажите программную компоненту, которая обрабатывает входящий HTTP запрос в паттерне MVC. 3. Посредством, какой программной компоненты паттерна MVC осуществляется связь с БД.	
Владеть	- навыками реализации паттернов проектирования в заданной среде разработки - навыками моделирования аппаратной части распределенной системы	1. Разработать программную компоненту с применением библиотеки Django задачей, которой будет получение курса валют ЦБ на указанную дату или период и последующая визуализация полученных данных. 2. Выполнить моделирование аппаратной части распределенной системы торгового предприятия в соответствии с техническим заданием.	
Знать	- методологию и этапы проектирования базы данных; - метод «сущность-связь» для проектирования БД; -методы и подходы создания инфологической модели БД;	**Теоретические вопросы к зачету:** Операции реляционной алгебры. Определение реляционных операций соединения, пересечения и деления через пять других операций. Понятие и основные свойства отношения. Назначение и особенности этапов проектирования БД. Подходы к системному анализу предметной области. Характеристика модели информационной системы Захмана. Концептуальные модели данных. Модель «сущность-связь». Сущности, атрибуты, связи. Сущности-связи и мощности связей. Принципы отображения концептуальной схемы на выбранную модель данных. . Сходство и отличие даталогической и физической модели данных. . Физические структуры данных реляционных СУБД. . Физические структуры индексов реляционных СУБД. . Понятие функциональной и многозначной зависимости. . Нормализация отношений. Первая, вторая, третья нормальные формы. Нормальная форма Бойса-Кодда. . Нормализация отношений. Процедура нормализации.	Б1.В.01 Информационные технологии. Базы данных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		. Реляционная модель данных. Получение реляционной схемы из ER-диаграммы . Язык определения данных и язык манипулирования данными. Назначение. Функциональные возможности (на примере SQL). . Основные понятия OLAP-технологии . Способы хранения многомерных данных. . Основные достоинства и недостатки способов ROLAP, MOLAP, HOLAP. . Виды запросов, использующиеся при работе с многомерными данными.	
Уметь	-разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; - применять средства обеспечения безопасности баз данных;	***Задание:*** Определить логическую структуру базы данных для предметной области. Спроектировать базу данных. Составить запросы на выборку с условиями отбора, запросы с параметром и несколько запросов с использованием статистических функций SQL. ***Вариант 1.*** Создать базу данных «Оптовая база». Оптовая база имеет в распоряжении несколько складов, каждый из которых предназначен для хранения товаров определенного типа. База данных должна содержать информацию об имеющихся на базе товарах, о размещении товаров по складам, информацию об оптовых покупателях, о накладных на продажу каждого вида товара (кто, что заказал, в каком количестве, дата заказа, дата оплаты). Вывести следующую информацию: 1) Статистика реализации товаров по месяцам, по видам товаров. 2) Определить загруженность каждого склада товарами. 3) Вывести общие стоимости заказов для каждого покупателя. ***Вариант 2.*** Создать базу данных «Деканат». БД деканата определенного факультета хранит сведения о нескольких специальностях. На каждой специальности имеется одна или несколько групп. У специальности известны: код, название, профессия выпускаемых специалистов, год открытия специальности, название выпускающей кафедры. В каждой группе числится несколько студентов. Студенты в сессию сдают несколько дисциплин. Итогам сдачи сохраняются в БД. Вывести следующую	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информацию: 1) Получить возможность просмотра полной информации об успеваемости студентов в виде перекрестной таблицы. 2) Вывести статистику успеваемости по заданному студенту, группам, специальностям, по отдельным дисциплинам, преподавателям, факультету в целом. ***Вариант 3.*** Спроектировать базу данных «ЖД вокзала». В БД должна содержаться информация о поездах, пассажирах, рейсах и о проданных билетах. Вывести следующую информацию: 1) Количество свободных мест на каждый рейс. 2) Прибыль с каждого направления. 3) Статистику по популярности направлений. ***Вариант 4.*** Спроектировать базу данных «Аэропорта». В БД должна содержаться информация о самолетах, пассажирах, рейсах и о проданных билетах. Вывести следующую информацию: 1) Количество занятых мест на каждый рейс. 2) Прибыль с каждого самолета. 3) Количество вылетов по вводимому направлению.	
Владеть	- основами проектирования БД; - навыками отображения предметной области на конкретную модель данных;	***Задание:*** Определить логическую структуру базы данных для предметной области. Спроектировать базу данных. Составить запросы на выборку с условиями отбора, запросы с параметром и несколько запросов с использованием статистических функций SQL. ***Вариант 1.*** Спроектировать базу данных «Автовокзала». В БД должна содержаться информация об автобусах, пассажирах, рейсах и о проданных билетах. Вывести следующую информацию: 1) Количество свободных мест на каждый рейс. 2) Прибыль с каждого направления. 3) Количество рейсов у каждого автобуса. ***Вариант 2.*** Спроектировать базу данных «Кинотеатра». В БД должна содержаться информация о фильмах (название, жанр, актеры, и т.д.), о залах и их размерах (ряды, кол-во мест), о сеансах и о проданных билетах. Вывести следующую информацию: 1) Количество билетов проданных на заданный сеанс. 2) Прибыль с каждого фильма. 3) Количество свободных мест на сеанс. ***Вариант 3.*** Спроектировать базу данных "Дипломное	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		проектирование". Группа студентов готовится к защите диплома. Каждый студент группы описывается личностными характеристиками, имеет тему диплома и собственного руководителя дипломного проектирования. Предоставляемых тем для проектирования гораздо больше, чем студентов в группе. Преподаватель, являющийся руководителем дипломного проектирования, может вести одного или нескольких студентов. Готовая дипломная работа подается на рецензию трем специалистам, каждый из которых выставляет свою оценку. Один и тот же рецензент может оценивать работу нескольких студентов. Вывести следующую информацию: 1) Выставить оценку студенту как среднее арифметическое между тремя оценками рецензентов и оценкой на защите. 2) Начислить стипендию студентам. 3) Сформировать приказы об отчислении.	
Знать	- область применения IoT-систем; - архитектуру IoT-систем; - принципы построения систем на базе IoT-устройств;	1. Применение облачных технологий и сервисно-орентированных архитектур в IoT 2. Обработка данных в IoT 3. Состав IoT-систем 4. Технологии IoT: 2G/3G/4G, 5G Спутниковая (VSAT) ,LPWAN (LORA,LTE-M,NB IOT,NB FI) 5. Услуги инфраструктуры(IaaS), Платформа как услуга(PaaS), услуги программного обеспечения (SaaS). Подключение сенсоров и актуаторов к микроконтроллерам	Б1.В.07 Безопасность Интернета вещей
Уметь	планировать работы по проектированию сложных IoT-систем; - проектировать структуру и архитектуру системы на базе IoT- устройств с использованием современных технологий	Разработать систему мониторинга климатических показателей серверного помещения на базе IoT-устройств	
Владеть	навыками проектирования, тестирования и отладки систем на базе IoT-устройств;	Разработать приложения: - приложение имитированного устройства Python - приложение Python для вызова прямых методов на имитированном устройстве. Осуществить управление подключенным к центру Интернета	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		вещей устройством.	
Знать	- Методы, способы, средства, последовательность и содержание этапов разработки программного обеспечения и компонентов безопасности программного обеспечения;	1.Как делается верификация моделей программ методом model checking? 2. Опишите логику дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации. 3. Опишите технологии создания алгоритмически безопасных процедур. 4. Какие бывают методы создания самотестирующихся и самокорректирующихся программ? 5. Опишите создание безопасного программного обеспечения на базе методов теории конфиденциальных вычислений. 6. Как делается защита программ и забывающее моделирование на RAM-машинах? 7. Какие вы знаете способы обеспечения надежности программ для контроля их технологической безопасности? 8. Перечислите процессы обеспечения функциональной безопасности программных продуктов в международных стандартах IEC и ISO. 9. Назовите методы идентификации программ и их характеристик.	Б1.В.09 Анализ уязвимостей программного обеспечения
Уметь	- проводить анализ уязвимостей программного обеспечения; - выполнять реверс инжиниринг программного обеспечения;	Выполнить анализ экземпляра ПО на наличие следующих уязвимостей: Уязвимость к включению файлов, возможность SQL-инъекции, Возможность переполнения буфера, подверженность состоянию гонки. При помощи встроенных утилит Linux выполнить реверс-инжиниринг предложенного экземпляра ПО	
Владеть	- навыками противодействия атакам на программное обеспечение;	Разработать модуль контроля целостности исполняемого файла ПО. Реализовать защиту от XSS	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Знать	источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;	*перечень вопросов на защите отчета НИР:* 1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР? Какие охранные документы были получены в ходе выполнения НИР?	Б2.Б.02(Н) Научно-исследовательская работа
Уметь	анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;		
Владеть	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; методами формирования требований по защите информации; навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем		
Знать	─ источники и классификацию угроз информационной безопасности; ─ основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; ─ основные угрозы безопасности	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информации и модели нарушителя в автоматизированных системах;	знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на	
Уметь	─ анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; ─ классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; ─определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения поддерживать конфигурацию информационной системы и ее системы защиты информации		
Владеть	─ навыками документирования действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации ─ методами формирования требований по защите информации; ─ навыками анализа основных узлов и устройств современных автоматизированных систем; ─ навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем ─ навыками обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	— источники и классификацию угроз информационной безопасности; — основные средства и способы	**индивидуальное задание на производственную преддипломную практику:**	Б2.Б.04(Пд) Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	обеспечения информационной безопасности, принципы построения систем защиты информации; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;	*Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:*	
Уметь	– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; –определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения поддерживать конфигурацию информационной системы и ее системы защиты информации		
Владеть	– навыками документирования действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации – методами формирования требований по защите информации; – навыками анализа основных узлов и устройств современных автоматизированных систем; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем – навыками обеспечения защиты информации при выводе из эксплуатации аттестованной		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной системы	1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		охраны особо важных объектов	
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ			
Знать	нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов	Теоретические вопросы 1. Виды информации, подлежащие защите в соответствии с законодательством Российской Федерации. 2. Государственная тайна. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. 3. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. 4. Лицензионные требования ФСТЭК России на деятельность по технической защите конфиденциальной информации. 5. Лицензионные требования ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. 6. Сертификация. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации 7. Определение понятия «угроза безопасности информации». Способы реализации угроз безопасности информации.. Определение понятий «контролируемая зона», «ОТСС», «ВТСС», «зона 2», «зона 1», «контролируемая зона (КЗ)». 8. Методы и способы анализа угроз безопасности информации. Соотношения «зоны 2» и «зоны 1» по отношению к размеру «контролируемой зона (КЗ)». при решении задач технической защиты информации. 9. Порядок проведения оценки опасности угрозы. 10. Понятие ущерба. Методы и способы оценки ущерба. 11. Структура системы защиты государственной тайны и государственной системы защиты информации. Место службы безопасности объекта	Б1.Б.31 Организационное и правовое обеспечение информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		12. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта. 13. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности. 14. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима. 15. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. 16. Требования к помещениям и хранилищам, в которых ведутся закрытые работы. 17. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей.	
Уметь	разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	1. Оценить угрозы информационным ресурсам выбранного предприятия (укажите наиболее вероятные виды киберпреступлений). 2. Указать мероприятия, проводимые при создании системы защиты информации в корпоративной инфраструктуре. 3. Составьте перечень РД ФСТЭК, учитываемых при разработке «Политики безопасности» на промышленном предприятии.	
Владеть	способностью разрабатывать научно-техническую документацию в области защиты информации	1. Указать цель обеспечения информационной безопасности предприятия. Задать величину степени защищенности создаваемой на объекте системы защиты информации и стоимость используемых активов АС. Выбрать и обосновать стратегические принципы безопасности АС. Оценить величину ущерба активам АС при реализации угроз. Рассчитать ожидаемые потери после создания системы информационной безопасности.	
Знать	нормативные правовые акты и нормативные методические документы в области	*перечень вопросов на защите отчета НИР:*	Б2.Б.02(Н) Научно-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	обеспечения информационной безопасности, структуру научно-технических отчетов	1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР? Какие охранные документы были получены в ходе выполнения НИР?	исследовательская работа
Уметь	разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности		
Владеть	способностью разрабатывать научно-техническую документацию		
Знать	-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-принимать участие в разработке проектов нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности		
Владеть	-навыками разработки научно-техническую документации, научно- технических отчетов по		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	результатом выполненных работ	информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	-принимать участие в разработке проектов нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - применять нормативные правовые акты и		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	нормативные методические документы в области обеспечения информационной безопасности	требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии?	
Владеть	-навыками разработки научно-техническую документации, научно- технических отчетов по результатом выполненных работ		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-8	**способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем**		
Знать	- основные типы угроз ИБ распределенных информационных системах. - основные механизмы защиты распределенной системы от угроз ИБ	1. Укажите основные типы угроз ИБ в распределенной системе. 2. Укажите основные механизмы защиты распределенной системы от угроз ИБ	Б1.Б.37 Методы проектирования защищенных распределенных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	- применять готовые программно-аппаратные средства по обеспечению ИБ в распределенных системах.	Подключить Auth0 к проекту Django Подключить SSL сертификат к проекту Django	информационных систем
Владеть	- навыками конфигурирования устройств, входящих в состав проектируемой распределенной системы - навыками конфигурирования основных программных средств, входящих в состав проектируемой распределенной системы	1. Выполнить настройку DMZ на маршрутизаторе L1. 2. Создать механизм тунелирования данных между сервером и клиентами. 3. Подключить механизм сессий к проекту Django	
Знать	─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ современную нормативно-правовую базу создания защищенных распределенных информационных систем; ─ инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	─ разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; ─ применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем		
Владеть	─ методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ навыками разработки комплексной инфраструктуры защищенной информационной системы; ─ навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ современную нормативно-правовую базу создания защищенных распределенных информационных систем; ─ инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:*	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	─ разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; ─ применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем		
Владеть	─ методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ навыками разработки комплексной инфраструктуры защищенной информационной системы; ─ навыками работы с ведущими программными и аппаратными комплексными		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	средствами защиты информации	– ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-9	**способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности**		
Знать	Основные элементы персонального компьютера и их функциональное назначение, базовые топологии автоматизированных систем; – Логическую, функциональную и структурную схему персонального компьютера, устройства организующие работу вычислительных систем; – Логику работы центрального процессора при выполнении вычислений и при передаче данных между ЦП и периферийными устройствами ПК.	1. Архитектура и структура вычислительной машины. Уровни детализации вычислительной машины. 2. Фон-неймановская модель ЭВМ. Основные принципы построения ЭВМ. 3. Типы структур вычислительных машин и вычислительных машин. 4. Классификация и основные характеристики ЭВМ. 5. Области применения ЭВМ различных классов. 6. Архитектура системы команд. Классификация АСК. Хронология развития АСК. Классификация АСК по составу и сложности команд. 7. Типы и форматы операндов (логические данные и строки). 8. Типы и форматы операндов (числовые данные и символьная информация). 9. Функциональная организация фон-неймановской ВМ (устройство управления, память). 10. Функциональная организация фон-неймановской ВМ	Б1.Б.28 Организация ЭВМ и вычислительных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		(арифметико-логическое устройство, модуль ввода/вывода). 11. Система команд ВМ. Аспекты, характеризующие систему команд ЭВМ. 12. Система операций ВМ. 13. Шины. Транзакции.Типы шин. 14. Режимы работы шины. 15. Иерархия шин. 16. Шина адреса, шина данных и шина управления. 17. Схемы приоритетов при арбитраже шин. Децентрализованный арбитраж. 18. Централизованный параллельный арбитраж шин. 19. Централизованный последовательный арбитраж шин. Децентрализованный арбитраж. 20. Память. Характеристики памяти. 21. Иерархическая память. Принцип локальности по обращению. 22. Основная память. 23. Синхронные и асинхронные ЗУ. Статические и динамические ОЗУ. 24. ПЗУ. 25. Кэш-память. Структура системы с основной и кэш-памятью. Характеристики кэш-памяти. 26. Способы отображения основной памяти на кэш-память. 27. Алгоритмы замещения информации в заполненной кэш-памяти. 28. Алгоритмы согласования содержимого основной памяти и кэш-памяти. 29. Виртуальная память. Страничная организация виртуальной памяти. 30. Виртуальная память. Сегментная организация виртуальной памяти. 31. Внешние запоминающие устройства. 32. Понятие системы ввода/вывода ВМ. Адресное пространство системы ввода/вывода. 33. Модули ввода/вывода. Методы управления вводом/выводом. Каналы и процессоры ввода/вывода. 34. Подсистема прерываний ВМ. Аппаратное обеспечение для поддержки прерываний. запрет и разрешение прерываний. 35. Подсистема прерываний ВМ.Обслуживание нескольких	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		устройств. Управление запросами устройств. Исключения. 36. Конвейеризация вычислений. Суперскалярные процессоры. 37. Уровни параллелизма вычислений. Классификация параллельных вычислительных систем. 38. Топология сетей. 39. Коммуникационные сети.	
Уметь	требуемый перечень компонентов ПК под конкретное техническое задание; ─ Определять основные неисправности ПК и подключенных к нем устройств; ─ Проектировать одноранговые вычислительные сети.	1.Определить комплектующие для сборки ПК на процессоре семейства AMD, выполняющего работу с текстовыми редакторами 2. Определить комплектующие для сборки ПК на процессоре семейства Intel, выполняющего работу с графическими редакторами(рендеринг). 3. Определить комплектующие для сборки ПК на процессоре семейства Intel, выполняющего фукнции сервера 1С. 4.Используя осцилограф определить неисправности интерфейса SVGA 5.Используя осцилограф определить неисправности интерфейса PS/2 6. Спроектировать однораговую вычислительную сеть с подключением трех ПК	
Владеть	Навыками сборки ПК из отдельных комплектующих; ─ Навыками работы с осциллографом; ─ Навыками настройки адаптеров сетевых подключений	1. Определить основные элементы ПК. Указать основные этапы сборки ПК отдельными комплектующими. 2. По указанной конфигурации компьютера произвести подбор блока питания с учетом потребляемой мощности элементов ПК и требуемых разъемов подключения 3. Выполнить подключение и настройку осциллографа для получения сигнала Data интерфейса PS/2 keyboard 4. Настроить одноранговую вычислительную сеть из 3 ПК, используя встроенные свойства сетевого адаптера и функции ОС	
Знать	понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем основные принципы построения защищенных распределенных компьютерных систем документы ФСТЭК России, регламентирующие	1. Понятие, виды и структура автоматизированных систем 2. Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения безопасности информации в АС. 3. Система и структура функциональных требований по защите от НСД в АС, группы и классы защищенности АС. 4. Общая структура требований безопасности к изделиям и	Б1.Б.33Разработка и эксплуатация защищенных автоматизированных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	порядок разработки моделей угроз в автоматизированных системах. • современные принципы построения архитектуры ИС.	системам ИТ, классы функциональных требований безопасности. 5. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении. 6. Анализ защищенности АС	
Уметь	осуществлять анализ несложных процессов проектирования применять государственные стандарты при проектировании автоматизированных систем в защищенном исполнении • разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	***Задание*** Составить техническое задание на создание системы защиты ПДн, обрабатываемых в распределенных информационных системах, имеющих подключение к сетям связи общего пользования.	
Владеть	приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем приемами разработки проектов нормативных документов, регламентирующих работу по защите информации • навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	***Задание.*** Разработать защиту объекта информатизации: Объект 2 категории. 3 здания, 50 помещений, наличие прилегающей территории, подлежащей контролю. Штат 100 человек. СВТ 150 ед., 5 серверов, распределенная сеть, выход в глобальные сети. Два выделенных помещения; 2 объекта вычислительной техники. Исходя из прикладного назначения ОИ следует обоснованно выбрать (рекомендовать к применению): - класс защищенности автоматизированной системы (АС), которая производит хранение и обработку конфиденциальной информации на объекте информатизации, - класс защищенности средств вычислительной техники (СВТ), составляющих аппаратно-программную поддержку автоматизированной системы, - класс межсетевых экранов (МЭ) по уровню защищенности от НСД, реализующих защиту внутренней вычислительной сети ОИ, - класс применяемых на ОИ антивирусных средств, - уровень контроля программного обеспечения средств защиты информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		В проекте защиты следует использовать сертифицированные средства и системы, прошедшие сертификацию не ниже выбранных классов.	
Знать	- варианты интерпретации бинарного потока данных; - структуру пакетов данных транспортного уровнять протокола TCP;	1. Сериализация данных 2. Big-endian и Little-Endian. 3. Связь TCP и модели ISO/OSI/ 4. Структура протокола TCP. 5. Формат пакета данных протокола TCP.	Б1.Б.38 Технология построения защищенных распределенных приложений
Уметь	- выполнять анализ данных транспортного уровнять протокола TCP при помощи специализированного программного обеспечения;	1.Записать в файл полученные от удаленного сервера пакеты данных протокола TCP. 2. В полученном файле выполнить поиск пакетов содержащие полезную информацию. 3. По известному шаблону выполнить сериализацию полученных данных.	
Владеть	-навыками сериализации данных;	На языке C# реализовать алгоритм выполняющий преобразование двоичной строки данных в заданную структуру. На языке C# реализовать алгоритм выполняющий преобразование произвольной структуры в двоичную строку.	
Знать	- Стандарты в области оценки защищенности компьютерных систем - Критерии оценки безопасности информационных технологий - Методы оценки защищенности компьютерных систем	Перечень вопросов: 1. Что такое уровень гарантированности? 2. Какие виды гарантированности бывают? 3. Что такое классы безопасности и уровни доверия? 4. Перечислите классы функциональных требований в ISO 15408. 5. Перечислите классы требований доверия в ISO 15408. 6. Перечислите оценочные уровни доверия в стандарте ISO 15408. 7. Перечислите группы элементов управления в стандарте ISO 17799. 8. Перечислите ключевые элементы управления в ISO 17799.	Б1.В.03 Методы и стандарты оценки защищенности компьютерных систем
Уметь	- Проводить анализ защищенности компьютерных систем - Выполнять оценку систем	Задание: Оценить показатели защиты информации для заданной системы	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной безопасности - Составлять диаграммы информационной безопасности	Виды систем: 1. Информационно-поисковые системы 2. Электронный документооборот и делопроизводство 3. Электронные архивы 4. Системы управления ресурсами организации 5. Системы автоматизации проектирования 6. Информационно-аналитические системы 7. Системы поддержки принятия решений 8. Системы видеоконференцсвязи и цифровой телефонии 9. Ситуационные и управляющие центры Построить причинно-следственную диаграмму Исикавы для выявления и ранжирования имеющихся причинно-следственных связей возникновения угроз	
Владеть	- Методами оценки защищенности компьютерных систем - Методами тестирования защищенности компьютерных систем	Построить причинно-следственную диаграмму Исикавы для выявления и ранжирования имеющихся причинно-следственных связей утечки данных Составить план тестирования защищенности компьютерной системы методами белого и черного ящика: 1. Информационно-поисковые системы 2. Электронный документооборот и делопроизводство 3. Электронные архивы 4. Системы управления ресурсами организации 5. Системы автоматизации проектирования 6. Информационно-аналитические системы 7. Системы поддержки принятия решений 8. Системы видеоконференцсвязи и цифровой телефонии Ситуационные и управляющие центры	
Знать	- Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем - Основные принципы построения защищенных распределенных компьютерных систем - Документы ФСТЭК России, регламентирующие порядок разработки моделей	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	угроз в автоматизированных системах. - Современные принципы построения архитектуры ИС.	знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на	
Уметь	- Осуществлять анализ несложных процессов проектирования; - Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов		
Владеть	- Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации - Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации - Определять уровни защищенности и доверия программно- аппаратных средств защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем - Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации - Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; - Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем	**индивидуальное задание на производственную преддипломную практику:**	Б2.Б.04(Пд) Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- Основные принципы построения защищенных распределенных компьютерных систем - Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. - Современные принципы построения архитектуры ИС.	*Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:*	
Уметь	- Осуществлять анализ несложных процессов проектирования; - Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов		
Владеть	- Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации - Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации - Определять уровни защищенности и доверия программно- аппаратных средств защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем - Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации - Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем;		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		охраны особо важных объектов	
ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности			
Знать	*Способы разработки сложного программного обеспечения.* *Эффективные способы реализации структур данных и конкретных алгоритмов при решении различных задач.* *Требования, предъявляемые к разработке внешних спецификаций, для разрабатываемого программного обеспечения.*	Теоретические вопросы к экзамену: 1. Базовые понятия ООП. 2. Типы управляющих структур структурного программирования. 3. Методики (стратегии) разработки программ, относящиеся к структурному программированию. 4. Программирование «сверху вниз». 5. Отличие процедур и функций. 6. Характеристики модуля. 7. Основополагающие концепции ООП. 8. Основные элементы схем алгоритма. 9. Компоненты среды программирования. 10. Понятие компилятора. 11. Классификация языков программирования. 12. Виды динамических структур данных. Особенности работы с ними. 13. Универсальная обработка особых ситуаций. 14. Технология работы с файлами в C#.	Б1.Б.20 Языки программирования
Уметь	*Планировать разработку сложного программного обеспечения.* *Проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении различных задач.* *Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения.*	1. Написать программу, которая переводит введенную сумму в выбранную валюту (доллар, евро, шекели) и выводит курс перевода. Для реализации интерфейса использовать формы. 2. Написать программу для решения задачи: Дано натуральное число N. Вычислить: — — — 3. Написать программу для решения задачи: Даны x, y. Вычислить:	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4. Для матрицы из 8 столбцов и 2 строк определить номер каждого столбца, сумма элементов которого меньше нуля, и число таких столбцов. Составить блок-схему и программу.	
Владеть	*Навыками разработки типового программного обеспечения.* *Навыками разработки внешней спецификации для разрабатываемого программного обеспечения.* *Навыками разработки сложного программного обеспечения.*	Создать Windows-приложение для моделирования движения человека. Пользователь задает входные параметры (начальная скорость, ускорение, направление движения) и на экране видит движущегося человека. В приложении должны быть реализованы следующие функции: 1. Возможность изменять входные параметры моделирования. 2. Выбор пользователем указателем мыши начальной и конечной точки движения (фигура человека перемещается в начальную точку указанную пользователем). 3. Возможность добавления в движение прыжков вверх. 4. Создание встроенного справочного материала о расчетах с учетом входных параметров. Приложение должно быть реализовано с использованием иерархии классов. В приложении должны быть следующие пункты меню: 1. Создать новую попытку – при его выборе убирается последнее движение и остается только выбор параметров движения. 2. Сохранить – сохраняются результаты вычисления для всех точек бега в файл Excel с указанием входных параметров. 3. Выход – закрытие приложения 4. Справка – краткое руководство по программе и данные автора.	
Знать	Современные технологии программирования. Области и особенности применения языков	Теоретические вопросы: 1. Функциональные возможности Python (лямбда-функции и т.д.)	Б1.Б.21 Технологии и методы программирования

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	программирования высокого уровня; Основные виды интегрированных сред разработки программного обеспечения. Способы обработки исключительных ситуаций; Современные технологии и методы программирования, предназначенные для создания прикладных программ.	2. Работа с файлам и папками в Python. Хранение структурированных данных в файлах. 3. Модули и пакеты 4. Регулярные выражения. 5. Обработка значений даты и времени 6. ООП 7. Tkinter 8. Работа с файлами xls, pdf и word. 9. Формат JSON 10. Формат CSV	
Уметь	Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; Работать с основными средами интегрированной разработки программного обеспечения; Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; Реализовывать разработанную структуру классов для задач предметной области.	1.Реализовать собственное **key-values** хранилище. Данные будут сохраняться в файле **storage.data**. 2. Добавлять новые данные в хранилище и получение текущих значений. 3. Вывод на печать, значений из хранилища. 2.Написать декоратор to_json, который можно применить к различным функциям, чтобы преобразовывать их возвращаемое значение в JSON-формат с учетом сохранения корректного имени декорируемой функции.	
Владеть	Навыками реализации алгоритмов на языках программирования высокого уровня; Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. Технологиями программирования распределенных автоматизированных систем;Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.	Написать приложение для реализации следующих задач: 1. . Информационно-поисковая система “БДУ”. 2. Система учета успеваемости студентов. 3. Автоматизированная система складского учета. 4. Программа-тренажер для исследования простейших графиков функций.	
Знать	– основы теории электрических цепей – принципы работы элементов и функциональных	– Что нужно обеспечить при подключении к линии связи, чтобы вся энергия информационного сигнала стала поступать в	Б1.Б.22 Электроника и

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	узлов электронной аппаратуры – типовые схемотехнические решения основных узлов и блоков электронной аппаратуры	подключенное устройство? – Как называются Z-, Y-, H- параметры четырехполюсника? Как определить эти параметры, используя методы короткого замыкания и холостого хода? – Как измерить АЧХ и ФЧХ четырехполюсника в лаборатории с использованием типовых измерительных приборов? – При каких условиях входное сопротивление четырехполюсника равно отношению выходного напряжения к выходному току? – Используя частотные свойства конденсатора и катушки индуктивности, объяснить работу ФНЧ Т-типа. – Какие фильтры могут использоваться в источниках питания ЭВМ, в радиоприемниках, в устройствах защиты от гармонических помех? – Где больше модуль коэффициента отражения в линии с потерями: в сечении нагрузки или на входе линии? – Как искажаются прямоугольные импульсы в ФНЧ, в ФВЧ и в ПФ? Поясните, используя спектральные представления, причину и характер искажений коротких по длительности импульсов в ФНЧ с фиксированной граничной частотой. – Объясните причину появления помех в работе переносного радиоприемника, если его близко расположить от компьютера. Как изменится уровень этих помех, если приемник переключить на более высокочастотный диапазон? – Какой из усилителей: ОЭ, ОБ или ОК, потребляет от источника сигнала минимальный ток, а какой – максимальный? – Перечислите виды внешней обратной связи в усилителях. Какая обратная связь называется положительной, а какая отрицательной? Существуют ли обратные связи, которые не оказывают влияния на коэффициент усиления усилителя? – Как можно уменьшить шум квантования при программной реализации на ЭВМ цифровой обработки сигналов?	схемотехника
Уметь	– применять на практике методы анализа электрических цепей – работать с современной элементной базой электронной аппаратуры	– Докажите, что средняя мощность, потребляемая участком цепи, содержащей резисторы, конденсаторы и катушки не может быть отрицательной. – Найдите напряжение на катушке, если ток через нее возрастает с	

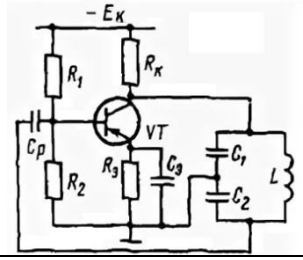
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	– использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации	течением времени по линейному закону (по экспоненциальному закону, квадратично). – На конце линии короткое замыкание. Чему равны амплитуда и начальная фаза отраженной волны в сечении нагрузки, если амплитуда падающей волны в этом сечении равна 5 В, а начальная фаза равна нулю? – Отраженная волна взаимодействует с третьей частью падающей волны в линии с малыми потерями с резистивной нагрузкой. Нарисовать распределение амплитуды напряжения смешанной волны вдоль линии. Рассчитать КСВ и КБВ. – Волновое сопротивление линии связи в компьютерной сети равно 100 Ом (витая пара). Найти максимально и минимально возможные амплитуды напряжения волны в сечении нагрузки с сопротивлением 300 Ом (на входе рабочей станции), если амплитуда напряжения на входе линии (на выходе сервера) равна 10 В. Для простоты потерями в линии пренебречь. – Во сколько раз надо увеличить сопротивление нагрузки, чтобы получить двукратное увеличение коэффициента усиления в каскадах ОЭ и ОБ? Чем ограничивается величина сопротивления нагрузки в этих усилителях? – Составьте схему шифратора с 4 входами и 2 выходами. – Постройте схему демультиплексора с двумя выходами. – Используя полусумматор и полный сумматор, нарисуйте схему трехразрядного двоичного сумматора, предполагая, что от внешних устройств сигналы переноса не поступают. –	
Владеть	– навыками работы с программными средствами схемотехнического моделирования – навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации – навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы	– Как измерить узловое напряжение? Как измерить контурный ток в сложной цепи? Всегда ли можно измерить контурный ток в цепи? – Почему для съема информации с участка цепи удобнее использовать вольтметры, а не амперметры? – Напряжение от батареи постоянного тока подается на ФНЧ, ФВЧ, ПФ и ЗФ. На выходах каких фильтров будет гореть индикаторная лампочка? – Какие фильтры могут использоваться в источниках питания ЭВМ, в радиоприемниках, в устройствах защиты от гармонических	

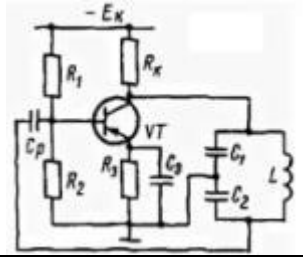
Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		помех? – В каком случае влияние распределенных параметров в длинной линии при прочих равных условиях больше: при увеличении в 2 раза частоты сигнала или при увеличении в 2 раза длины линии? – Какие требования предъявляются к полосе пропускания системы связи, использующей импульсные сигналы? Достаточно ли, например, для передачи прямоугольных импульсов с частотой следования 10 МГц иметь полосу пропускания канала связи, равную тем же 10 МГц? – Какой из двух усилителей: резистивный или резонансный, нужно использовать для усиления речевого сигнала, а какой – для усиления сигнала телевизионной станции? Что случится, если выбор усилителя будет сделан ошибочно? – Сравнивая схемы элемента ТТЛ и КМДП логического элемента, назовите причины, по которым в микропроцессорах используются элементы на полевых транзисторах. – Нарисуйте временные диаграммы установки синхронного D-триггера в нулевое и единичное состояния. – Используя элемент И-НЕ, нарисуйте схему D-триггера со статической синхронизацией.	
Знать	Виды сетевых топологий; - Принципы передачи информации по телекоммуникационным каналам; - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; - Классификацию сетевых протоколов.	Перечень вопросов: 1. Физические принципы передачи информации по различным каналам связи 2. Характеристики и технологические ограничения, присущие каналами связи при передаче информации по ним 3. Методы обеспечения надежной передачи информации при передаче ее по различным каналам связи 4. Классификация и назначение сетевых протоколов сетей ЭВМ 5. Основные технические характеристики сетевого оборудования 6. Уровни сетевого оборудования(концентратор, коммутатор, маршрутизатор) 7. Принцип функционирования коммутатора уровня 2+ 8. Активное и пассивное сетевое обрудование 9. Оптических патч-корды и пигтейлы 10. Принцип функционировании и основные рабочие характеристики оптоволоконного сетевого оборудования	Б1.Б.30Сети и системы передачи информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	Самостоятельно диагностировать неисправности сетей ЭВМ; - Контролировать безотказное функционирование сетей ЭВМ; - Осуществлять подбор инструментальных и программных средств тестирования сетей ЭВМ; - Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.	1. Выполнить диагностику неисправности или аномалии работы сети ЭВМ. 2. Сделать заключение о возможности или невозможности дальнейшей эксплуатации при данной неисправности сети. 3. Предложить комплекс мер по устранению неисправности сети ЭВМ. 4. Разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ 5. Разработать топологию вычислительной сети и выполнить подбор сетевого оборудования в соответствии с технических заданием	
Владеть	Методиками проектирования топологии вычислительных сетей; - Навыками определения и поиска неисправностей в сетях ЭВМ; - Навыками настройки сетевого оборудования.	1. Определить состав сетевого оборудования, каналов связи и программного обеспечения для построения вычислительной сети согласно техническому заданию. 2. Разработать конфигурацию сетевого оборудования в соответствии с топологией сети 3. Выполнить настройку сетевого оборудования в соответствии с топологией сети и выполнить инициализацию устройств 4. Произвести фильтрацию трафика вычислительной сети с помощью свободно распространяемых программ-анализаторов WireShark или Ethereal с определением принадлежности трафика, используемого сетевого протокола и сетевых портов. 5. Определить ошибки или аномалии передачи данных на основе анализа сетевого трафика	
Знать	Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ. Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.	Вопросы к экзамену: 1. Подсистемы СЗИ автоматизированной системы. 2. Концепция MBR и GPT. 3. Обеспечение безопасности доступа к данным и приложениям ИС на основе продуктов MicroSoft, Oracle и Aladdin. Сравнительный анализ. 4. Обеспечение целостности и доступности информации в	Б1.Б.32 Программно-аппаратные средства обеспечения информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		КС.	
Уметь	Исследовать эффективность контрольных проверок работоспособности применяемых программно-аппаратных средств защиты информации. Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей ИБ АС.	В СЗИ «Страж NT» зарегистрировать несколько внешних носителей информации, настроить права доступа к ним, отредактировать политику доступа к ним по умолчанию. Затем необходимо настроить политику использования пользователями групп устройств. Продемонстрировать различия в работе зарегистрированных внешних носителей информации.	
Владеть	Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ. Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.	В СЗИ «Страж NT» на документы, расположенные в КС, установить контроль целостности, а также настроить дополнительный аудит. Осуществить пользователями с различными правами доступа попытки доступа к документам. Продемонстрировать журнал событий, отфильтровать события и заархивировать его.	
Знать	- Современные методы и средства защиты информации в компьютерных системах; - принципы и способы использования существующих средств ЗИ в компьютерных системах; - принципы применения современных методов оценки безопасности компьютерных систем;	Перечень вопросов: 1. Средства защиты в компьютерных системах 2. Теоретико-вероятностный метод оценки защищенности в компьютерных системах 3. Экспертный метод оценки в компьютерных системах 4. Статистический метод оценки в компьютерных системах 5. Вероятностно-статистический метод оценки рисков в компьютерных системах 6. Взаимосвязь угроз, уязвимостей и рисков 7. Оценки защищенности на основе модели комплекса механизмов защиты 8. Семантические показатели защищенности компьютерных систем 9. Нечеткие оценки защищенности компьютерных систем 10. Комплексные оценки защищенности компьютерных систем 11. Типовая архитектура системы выявления атак 12. Методы тестирования системы защиты	Б1.В.03 Методы и стандарты оценки защищенности компьютерных систем
Уметь	- выявлять угрозы и определять их актуальность для современных компьютерных	Используя метод оценки защищенности на основе модели комплекса механизмов защиты определить защищенность,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	систем; - применять современные методы оценки безопасности компьютерных систем;	обеспечиваемой отдельным механизмом и СЗИ в целом. Определить эффективность применяемых методов обеспечения безопасности компьютерной системы. Виды организаций: 1. Информационно-поисковые системы 2. Электронный документооборот и делопроизводство 3. Электронные архивы 4. Системы управления ресурсами организации 5. Системы автоматизации проектирования 6. Информационно-аналитические системы 7. Системы поддержки принятия решений 8. Системы видеоконференцсвязи и цифровой телефонии 9. Ситуационные и управляющие центры	
Владеть	- практическими навыками применения методов обеспечения безопасности компьютерных систем; - навыками применения современных методов оценки безопасности компьютерных систем.	Используя онлайн-калькулятор банка данных угроз ФСТЭК определить базовые, временные и контекстные метрики угроз информационной безопасности компьютерных систем: 1. Информационно-поисковые системы 2. Электронный документооборот и делопроизводство 3. Электронные архивы 4. Системы управления ресурсами организации 5. Системы автоматизации проектирования 6. Информационно-аналитические системы 7. Системы поддержки принятия решений	
Знать	− характеристики и область применимости базовых электронных компонентов; − схемотехнику основных электронных узлов радиотехнических систем; − программное обеспечение для разработки систем передачи информации в целом и отдельных её узлов.	**Типовые вопросы к экзамену:** 1. Состав (структура), классификация и основные параметры передатчиков. 2. Выходные каскады передатчиков. 3. Состав (структура), классификация и основные параметры приемников. 4. Входные цепи приемников. 5. Принцип действия супергетеродинного приемника. 6. Детектирование высокочастотных колебаний.	Б1.В.ДВ.01.01 Основы радиотехники

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Детекторные каскады приемников. 7. Структура и принцип работы генератора с самовозбуждением (автогенереторов). 8. Структура и принцип работы генератора с внешним возбуждением (усилители мощности радиочастоты).	
Уметь	− создавать имитационные модели радиотехнических систем передачи информации с помощью специализированного программного обеспечения; − проводить анализ систем передачи информации в целом; − разрабатывать системы передачи информации в целом и отдельных её узлов; − создавать программное обеспечение для разработки системы передачи информации в целом и отдельных её узлов.	**Пример типового задания к лабораторной работе** Создайте в пакете Simulink среды Matlab модель генератора радиочастоты 200 МГц выполненного по схеме «ёмкостной трехточки» (см. рисунок). Выберите соответствующий транзистор, напряжение источника питания, рассчитайте номиналы пассивных компонентов. 	
Владеть	− навыками проектирования и создания отдельных элементов и узлов радиотехнических устройств; − методами анализа работоспособности электронных узлов радиотехнических устройств с помощью специализированного программного обеспечения; − методами разработки системы передачи информации в целом и отдельных её узлов	**Пример типового задания к лабораторной работе** Для имитационной модели генератора радиочастоты 200 МГц выполненного по схеме «ёмкостной трехточки» оцените стабильность частоты в режиме холостого хода при изменении напряжения источника в диапазоне ±10%. Оцените стабильность частоты при изменении номинальном напряжении источника и изменении сопротивления нагрузки в диапазоне от $10R_к$ до $0,5R_к$.	
Знать	− характеристики и область применимости базовых электронных компонентов; − схемотехнику основных электронных узлов систем передачи данных; − программное обеспечение для разработки систем передачи информации в целом и отдельных её узлов.	**Типовые вопросы к экзамену:** 1. Состав (структура), классификация и основные параметры передатчиков. 2. Выходные каскады передатчиков. 3. Состав (структура), классификация и основные параметры приемников. 4. Входные цепи приемников. 5. Принцип действия супергетеродинного приемника. 6. Детектирование высокочастотных колебаний.	Б1.В.ДВ.01.02 Физические основы передачи информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Детекторные каскады приемников. 7. Структура и принцип работы генератора с самовозбуждением (автогенереторов). 8. Структура и принцип работы генератора с внешним возбуждением (усилители мощности радиочастоты).	
Уметь	− создавать имитационные модели систем передачи информации с помощью специализированного программного обеспечения; − проводить анализ систем передачи информации в целом; − разрабатывать системы передачи информации в целом и отдельных её узлов; − создавать программное обеспечение для разработки системы передачи информации в целом и отдельных её узлов.	**Пример типового задания к лабораторной работе** Создайте в пакете Simulink среды Matlab модель генератора радиочастоты 200 МГц выполненного по схеме «ёмкостной трехточки» (см. рисунок). Выберите соответствующий транзистор, напряжение источника питания, рассчитайте номиналы пассивных компонентов. 	
Владеть	− навыками проектирования и создания отдельных элементов и узлов устройств передачи данных; − методами анализа работоспособности электронных узлов устройств связи с помощью специализированного программного обеспечения; − методами разработки системы передачи информации в целом и отдельных её узлов	**Пример типового задания к лабораторной работе** Для имитационной модели генератора радиочастоты 200 МГц выполненного по схеме «ёмкостной трехточки» оцените стабильность частоты в режиме холостого хода при изменении напряжения источника в диапазоне ±10%. Оцените стабильность частоты при изменении номинальном напряжении источника и изменении сопротивления нагрузки в диапазоне от $10R_к$ до $0,5R_к$.	
Знать	- Типовые структуры и принципы организации виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. - Программно-аппаратные средства обеспечения информационной безопасности в виртуальных локальных компьютерных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах	Перечень вопросов: 1. Для чего нужны VLAN сети? Характеристики и особенности таких сетей. 2. Транковое соединение выполняет какую роль и какой протокол тегирует пакеты для этого соединения? 3. Протокол VTP. Какие существуют режимы работы протокола VTP? 4. Как настроить VTP протокол на коммутаторе? Достоинства протокола VTP. 5. Какие могут быть неисправности при настройке VLAN? Как их	Б1.В.ДВ.04.01 Виртуальные сети

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		искать? 6. Назначение и принцип работы динамического протокол инициализации транка (DTP) 7. Опишите архитектуру Router-on-a-Stick 8. FlexVPN технология соединения сетей. Назначение протокола IKEv2 9. PPTP, L2TP, PPPoE соединения и их отличия. 10. Набор протоколов для обеспечения защиты данных передаваемых по сетевому протоколу в виртуальных частных сетях(IPSec) 11. Совместная работа IPSec и NAT. Основные проблемы при настройке. 12. Механизмы аутентификация для VPN 13. ESP, AH протоколы и их отличия. 14. Динамический и статический VTI. Основные настройки параметров. 15. Как работает GRE и NHRP? 16. Назовите основные этапы настройки SSL VPN для удаленного подключения. 17. Назначение и принцип работы межсетевого экрана в виртуальных частных сетях	
Уметь	- Создавать защищенные вычислительные сетей с применением виртуализации; - Применять технологии и средства защиты информации для обеспечения безопасности информации в вычислительных сетях.	1. Выполнить подбор сетевого оборудования исходя из его рабочих характеристик и наличия средств обеспечения безопасности информации в вычислительных сетях; 2. Разработать топологию вычислительной сети согласно поставленной задаче, определить факторы риска с точки зрения информационной безопасности в разработанной сети; 3. Разработать политику аутентификации пользователей специализированных виртуальных сетей в облачных сетевых структурах 4. Произвести конфигурирование SSL для виртуальных локальных сетей и виртуальных частных сетей согласно поставленной задаче	
Владеть	- Навыками разработки, внедрения и документирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в	1. Выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, сежсетевой экран) для построения разработанной топологии сети соблюдая требования по защите информации; 2.Реализовать разработанную политику сетевой безопасности при	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	облачных сетевых структурах, с учетом требований по обеспечению безопасности.	настройке и конфигурированию сетевого оборудования. 3. Разработать документация о переводе исходного состояния сети в текущее в соответствии с поставленной задачей 4. Разработать документацию о внедрении специализированных виртуальных сетей в корпоративную сеть предприятия 5. Разработать журнал настроек для заданных виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению безопасности.	
Знать	Современные технологии программирования. Области и особенности применения языков программирования высокого уровня; Основные виды интегрированных сред разработки программного обеспечения. Основные методы эффективного кодирования. Способы обработки исключительных ситуаций; Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении.	1. Перечислите меры, используемые для защиты программных продуктов от несанкционированного использования. 2. Перечислите модули системы технической защиты ПО от несанкционированного использования. Кратко охарактеризуйте функции каждого из них. 3. Приведите примеры характеристик среды, к которым можно осуществить привязку ПО для обнаружения факта несанкционированного использования. 4. В чем достоинства и недостатки встроенных и пристыковочных систем защиты ПО? 5. На какие из модулей системы защиты ПО от несанкционированного использования обычно осуществляет атаку злоумышленник? 6. Перечислите требования к блоку сравнения характеристик среды. 7. В чем особенности атак злоумышленника на блок установки характеристик среды и блок ответной реакции? 8. Перечислите и охарактеризуйте базовые методы нейтрализации систем защиты ПО от несанкционированного использования. 9. Перечислите средства статического исследования ПО. Кратко охарактеризуйте их. 10. Перечислите средства динамического исследования ПО. Кратко охарактеризуйте их. 11. Перечислите основные WinAPI функции, которые может использовать злоумышленник для локализации кода	Б1.В.ДВ.04.02 Защита программного обеспечения

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		защиты. В каких случаях злоумышленник попытается отлавливать каждую из этих функций? 12. Перечислите и охарактеризуйте базовые методы противодействия отладке программного обеспечения. 13. Перечислите и охарактеризуйте несколько триков для отладчиков реального и защищенного режимов. В чем их недостатки? 14. Перечислите и охарактеризуйте базовые методы противодействия дизассемблированию программного обеспечения. 15. Охарактеризуйте способ защиты от отладки, основанный на особенностях конвейеризации процессора. 16. Охарактеризуйте возможности противодействия отладке и дизассемблированию, основанные на использовании недокументированных инструкций и недокументированных возможностей процессора. В чем недостатки данных методов? 17. Охарактеризуйте шифрование кода программы как наиболее универсальный метод противодействия отладке и дизассемблированию ПО. 18. Дайте определение программы с потенциально опасными последствиями. Какие функции свойственны данным программам? 19. Перечислите основные классы программ с потенциально опасными последствиями. Дайте их сравнительную характеристику. 20. Что понимают под активизирующим событием? Перечислите основные виды активизирующих событий для РПВ. 21. Перечислите и охарактеризуйте основные модели взаимодействия прикладной программы и РПВ. 22. Опишите основные группы деструктивных функций, свойственных программным закладкам.	
Уметь	Реализовывать на языке высокого уровня	1. Разработать алгоритм от несанкционированного доступа. Доступ к файлу данных по паролю.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	алгоритмы решения профессиональных задач; Работать с основными средами интегрированной разработки программного обеспечения; Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; Реализовывать разработанную структуру классов для задач предметной области.	2. Разработать алгоритм и реализовать программу для защиты программ с помощью контрольного суммирования. 3. Разработать алгоритм и реализовать программу защиты сопровождения: регистрация обращений**.** 4. Разработать алгоритм и реализовать программу защиты программного обеспечения от несанкционированного доступа путем привязки ПО к ПК.	
Владеть	Навыками реализации алгоритмов на языках программирования высокого уровня; Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.	1. Используя брандмауэр Windows настроить доступ приложения к локальной сети и интернет 2. Используя встроенные средства Windows настроить доступ пользователя к программному обеспечению 3. Настроить защиту от программ-шантажистов и провести оценку журнала событий Windows 4. Используя встроенные средства Windows настроить доступ к программному обеспечению через доступ к папке	
Знать	- Современные технологии программирования. - Основные виды интегрированных сред разработки программного обеспечения. - Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении. - Принципы работы элементов и функциональных узлов электронной аппаратуры; -Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; - Работать с основными средами интегрированной разработки программного обеспечения;		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; - Реализовывать разработанную структуру классов для задач предметной области. -Работать с современной элементной базой электронной аппаратуры; -Использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации - Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.	применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим	
Владеть	- Навыками реализации алгоритмов на языках программирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем. -Навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации; - Методиками проектирования топологии вычислительных сетей; - Навыками настройки сетевого оборудования.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Современные технологии программирования. - Основные виды интегрированных сред разработки программного обеспечения. - Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении. - Принципы работы элементов и функциональных узлов электронной аппаратуры; -Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты	Б2.Б.04(Пд) Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; - Работать с основными средами интегрированной разработки программного обеспечения; - Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; - Реализовывать разработанную структуру классов для задач предметной области. -Работать с современной элементной базой электронной аппаратуры; -Использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации - Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.	информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на	
Владеть	Навыками реализации алгоритмов на языках программирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем. -Навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации; - Методиками проектирования топологии вычислительных сетей; - Навыками настройки сетевого оборудования		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-11	**способностью разрабатывать политику информационной безопасности автоматизированной системы**		
Знать	- задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и	**Теоретические вопросы** **1.** Что относится к административному уровню обеспечения информационной безопасности? **2.** Что относится к среднему уровню обеспечения информационной безопасности? **3.** Что относится к нижнему уровню обеспечения информационной безопасности?	Б1.Б.34Управление информационной безопасностью

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - основные угрозы безопасности информации и модели нарушителя объекта информатизации; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики ИБ организации;	**4.** Организация режима секретности. **5.** Принципы формирования политики информационной безопасности организации.	
Уметь	- разрабатывать модели угроз и модели нарушителя ОИ; - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; - разрабатывать предложения по совершенствованию системы управления ИБ АС.	1. Разработать частную модель угроз для заданного ОИ. Составить предложения по совершенствованию системы управления информационной безопасностью.	
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	**1.** На основе частной модели угроз разработать заданную политику безопасности.	
Знать	- систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - уровни политик информационной безопасности назначение политик верхнего, среднего и нижнего уровня	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; -разрабатывать политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала	специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для	
Владеть	- владеть навыками разработки политик безопасности различных уровней. -владеть навыками формирования комплекта организационной документации, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:*	Б2.Б.04(Пд) Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	ограниченного доступа; - уровни политик информационной безопасности назначение политик верхнего, среднего и нижнего уровня	– закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика.	
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; -разрабатывать политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала		
Владеть	- владеть навыками разработки политик безопасности различных уровней. -владеть навыками формирования комплекта организационной документации, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. 44) Сформулировать основные особенности построения периметровой охраны особо важных объектов	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
ПК-12	**способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы**		
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз.	**Теоретические вопросы** **1.** Основные принципы организации СУИБ. 2. Что понимают под профилем защиты. 3. Содержание профиля зашиты. 4. Что включает в себя методика определения защищенности ИС. 5. Что включает в себя активное и пассивное тестирование системы защиты. **6.** Методики определения рисков.	Б1.Б.34Управление информационной безопасностью
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.	Провести анализ защищенности заданного ОИ.	
Владеть	- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	Подготовить отчет по проведенному анализу защищенности: 1. Общие описание объекта обследования 2. Структура и состав комплекса программно-технических средств 3. Результаты анализа организационных уязвимостей 4. Результаты анализа защищенности внешнего периметра сети 5. Результаты анализа защищенности внутренней ИТ-инфраструктуры **6.** Рекомендации по устранению обнаруженных недостатков и повышению уровня защищенности	
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:**	Б2.Б.03(П) Производственная-практика по получению

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз	*Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:*	профессиональных умений и опыта профессиональной деятельности
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.		
Владеть	- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		охраны особо важных объектов	
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.		
Владеть	- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. 44) Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-13	**способностью участвовать в проектировании средств защиты информации автоматизированной системы**		
Знать	- способы организации обмена данными при помощи технологии RPC; - способы организации обмена данными при помощи технологии RMC; - способы организации обмена данными при помощи очередей; - функционал платформы .Net в части организации обмена данными; - функционал Run-Time Engine; - криптографические протоколы обмена информацией;	1.Модели промежуточного уровня. 2. Модель клиент-сервер. 3. Распределение приложений по уровням. 4. Удаленный вызов процедур. 5. Передача параметров по значению. 6. Передача параметров по ссылке. 7. Синхронный и асинхронный вызов RPC. 8. Удалённый вызов методов. 9. Сохранные и нерезедентные объекты. 10. Реализация ссылок на объекты. 11. Статическое и динамическое удаленное обращение к методам. 12. Модель распределенных объектов Java. 13. Сохранность и синхронность во взаимодействиях.	Б1.Б.38 Технология построения защищенных распределенных приложений
Уметь	- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи на языке C#; - разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи в среде разработки LabVIEW;	На языке C# реализовать алгоритм обработки ошибок возникающих при обмене данных по технологии Socket по протоколу TCP. На языке C# реализовать алгоритм обработки ошибок возникающих при обмене данных по технологии Socket по протоколу UDP. На языке C# реализовать алгоритм переподключения к серверу. В среде LabVIEW разработать блок-диаграмму обработки ошибок возникающих при обмене данных по технологии Socket по протоколу TCP. В среде LabVIEW разработать блок-диаграмму обработки ошибок возникающих при обмене данных по технологии Socket по протоколу UDP. В среде LabVIEW разработать блок-диаграмму переподключения к серверу.	
Владеть	- навыками оформления программной	Оформить часть кода на языке C# по ЕСПД.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	документации по ЕСПД; - навыками сериализации данных.	Оформить часть блок-диаграммы LabVIEW по ЕСПД. На языке C# разработать алгоритм чтения заголовка файла в формате BMP. В среде LabVIEW разработать блок-диаграмму чтения заголовка файла в формате JPEG.	
Знать	- способы организации обмена данными при помощи технологий RPC,RMC и очередей; - криптографические протоколы обмена информацией; - общий порядок действий по выбору мер защиты информации для их реализации в информационной системе - методы проектирования средств защиты информации;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи; - разрабатывать и исследовать модели информационно- технологических ресурсов, проектировать средства защиты информации АС - выбрать меры защиты информации для их реализации в информационной системе в рамках ее системы защиты информации		
Владеть	- навыками оформления программной документации по ЕСПД; - методами исследования информационно-технологических ресурсов -навыками определения необходимого набора мер защиты информации (базового, адаптированного, уточненного)		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- способы организации обмена данными при помощи технологий RPC,RMC и очередей; - криптографические протоколы обмена информацией; - общий порядок действий по выбору мер защиты информации для их реализации в информационной системе - методы проектирования средств защиты информации;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи; - разрабатывать и исследовать модели информационно- технологических ресурсов, проектировать средства защиты информации АС - выбрать меры защиты информации для их реализации в информационной системе в рамках ее системы защиты информации		
Владеть	- навыками оформления программной документации по ЕСПД; - методами исследования информационно-технологических ресурсов -навыками определения необходимого набора мер защиты информации (базового, адаптированного, уточненного)		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 44) Род деятельности предприятия, на котором проходила практика. 45) Какие способы защиты информации используются на предприятии? 46) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 47) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 48) Какая топология используется в локальных сетях на предприятии? 49) Как обеспечивается безопасность беспроводных сетей? 50) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 51) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 52) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 53) Опишите способы контроля трафика по локальным сетям предприятия.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		54) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 55) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 56) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 57) Какие операционные системы используются на ПК персонала предприятия? 58) Какие операционные системы используются на серверах предприятия? 59) Понятие и виды защищаемой информации по законодательству РФ. 60) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 61) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 62) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 63) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 64) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 65) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 66) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 67) Основное содержание разработки Политики безопасности предприятия (организации). 68) Принципы, основные задачи и функции обеспечения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационной безопасности. 69) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 70) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 71) Ответственность за нарушение законодательства в информационной сфере. 72) Основные мероприятия по защите информации при проведении совещаний и переговоров. 73) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 74) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 75) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 76) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 77) Сформулировать основные правила безопасной работы в компьютерной системе. 78) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 79) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 80) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 81) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 82) Классифицировать программно-аппаратные средства	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		защиты информации. Сформулировать основные их характеристики. 83) Рассмотреть особенности разграничения доступа и аудита в СЗИ 84) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 85) Раскрыть особенности образования электромагнитных каналов утечки информации. 86) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации ПК			
Знать	методы и подходы к экспериментальному исследованию и моделированию, применяемые в физике и распространяющиеся на другие области знаний	**Примерный перечень вопросов и заданий по лабораторным работам (1 семестр)** ***№ 1 «Применение законов сохранения для определения скорости полета пули»*** 1. Приведите примеры сил, дающих разные виды потенциальной энергии. Какие из них присутствуют в данной работе? Изобразите схему экспериментальной установки и укажите на ней силы, действующие на все тела, входящие в систему, в каждый момент времени. 2. Какие величины имели кинетическая и потенциальная энергия системы «пуля+маятник» в различные моменты опыта? Представьте схему изменения кинетической и потенциальной энергии системы. 3. Для каких моментов времени в данном эксперименте можно применять закон сохранения механической энергии, а для каких нельзя и почему? Схема. 4. Для каких моментов времени в данном эксперименте можно применять закон сохранения импульса, а для каких нельзя и почему? Схема 5. Используя законы сохранения получите формулу для расчета	Б1.Б.09Физика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		скорости полета пули в данной работе. 6. Как производится обработка экспериментальных данных в данной работе. Как определяется доверительный интервал скорости и средняя квадратическая погрешность отклонения маятника? ***№ 3 «Определение моментов инерции тел с помощью крутильного маятника. Проверка теоремы Штейнера»*** 1. Что такое момент инерции тела? В чем состоит смысл этой физической характеристики? 2. Как вычисляется момент инерции тела относительно точки и относительно оси? 3. Сформулируйте теорему Штейнера. В каком случае ее применяют? Как применить теорему Штейнера в данной работе? 4. Каков характер зависимости момента инерции от расстояния, на котором находится тело от оси вращения? 5. Как экспериментально определяется момент инерции тела в данной лабораторной работе? 6. Какие законы сохранения применяются для вывода расчетных формул? ***№ 4 «Исследование вращательного движения твердого тела вокруг неподвижной оси»*** 1. Каков характер зависимости момента инерции от расстояния, на котором находится тело от оси вращения? В данной работе. Постройте график этой зависимости. 2. Как экспериментально определяется момент инерции тела в данной лабораторной работе? 3. Какие законы сохранения применяются для вывода расчетных формул? Получите формулу для расчета момента инерции маятника. 4. Какова зависимость углового ускорения тела от момента приложенных к нему сил и момента инерции тела? Постройте график данной зависимости 5. Как на маятнике Обербека могут быть определены угловое	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		ускорение, момент действующих сил и момент инерции? 6. Как в данной работе рассчитывается погрешность определения момента инерции тела относительно произвольной оси вращения? 7. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных. ***№ 5 «Определение характеристик затухающих колебаний физического маятника»*** 1. Почему колебания маятника в данной работе будут затухающими, даже при выключенном электромагните? 2. Запишите уравнения затухающих и незатухающих колебаний, сравните их. 3. Как амплитуда затухающих колебаний зависит от времени и от числа колебаний? 4. Каков физический смысл величин применительно к данной работе: *начальная амплитуда колебаний, начальная фаза колебаний, круговая частота колебаний, период колебаний, коэффициент затухания, время релаксации, логарифмический декремент затухания, добротность.* Как они меняются с ростом U? 5. Как меняются характеристики затухающих колебаний *начальная амплитуда колебаний, начальная фаза колебаний, круговая частота колебаний, период колебаний, коэффициент затухания, время релаксации, логарифмический декремент затухания, добротность* если один из параметров данного физического маятника: I , m , L , k увеличится (либо уменьшится) при фиксированных значениях оставшихся? 6. Для чего, в данной работе, графики строят в логарифмическоммасштабе? 7. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных. ***№7 «Определение скорости звука методом стоячей волны»***	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		1. Что такое механическая волна? Каков механизм образования волны в данной работе? 2. Что представляет собой звуковая волна? 3. Как и от чего зависит скорость звука? 4. Как образуется стоячая волна? Выведите уравнение стоячей волны. 5. От чего и как зависит амплитуда стоячей волны? 6. Какие устройства создают бегущую и стоячую волны в данной работе? ***№ 11 «Изучение статистических закономерностей»*** 1. Каково распределение дроби по ячейкам на доске Гальтона? Какое распределение аналогично данному в МКТ? 2. Каково распределение электронов по модулю скорости в данной работе? Что происходит при изменении напряжения накала? 3. Какие статистические методы применяются в данной работе? 4. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных. ***№ 14 «Определение показателя адиабаты методом Клемана и Дезорма»*** 1. Объясните ход эксперимента и результаты расчета. 2. Назовите процессы, происходящие с газом, в ходе эксперимента и изобразите их графически. 3. Запишите уравнения для вывода формулы показателя адиабаты. 4. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных. 5. Как в данной работе минимизируется погрешность экспериментальных данных? ***№ 15 «Проверка закона возрастания энтропии»*** 1. Какая модель использовалась в данной работе для проверки	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		закона возрастания энтропии в замкнутой системе? 2. Что такое «микросостояние» и «макросостояние» термодинамической системе. Как их можно задать для данной модели (в первой и второй части работы)? 3. Что такое термодинамическая вероятность? Какие числовые значения она может принимать? Как она рассчитывалась в данной работе? Как она связана с энтропией? 4. Что такое флуктуации? Наблюдались ли они в данной работе? 5. Дайте определение второго начала термодинамики. Определите условия, при которых закон выполняется. Выполнялся ли он в данной работе?	
Уметь	− пользоваться современной аппаратурой для проведения физического эксперимента; − использовать физические модели для описания реальных процессов, с помощью приборов измерять физические величины, производить обработку экспериментальных данных и анализировать полученные результаты	**Примерный перечень вопросов и заданий по лабораторным работам (2 семестр)** ***№ 21 «Исследование электростатического поля с помощью зонда»*** 1. Что такое напряженность электрического поля? Как графически представить распределение напряженности в разных точках электрического поля в данной работе? 2. Что такое потенциал электростатического поля? Как графически представить распределение потенциала в разных точках электрического поля в данной работе? 3. Чему равна работа по перемещению заряда вдоль эквипотенциальной поверхности и по замкнутому контуру, ограниченному участками силовых и эквипотенциальных линий? Вычислите работу по перемещению заряда по заданной траектории. 4. Как изменится картина силовых и эквипотенциальных линий при увеличении (уменьшении) напряженности между электродами? ***№ 24 «Расширение предела измерения амперметра постоянного тока»*** 1. Каков принцип действия электроизмерительных приборов магнитоэлектрического и электромагнитного типа,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		применяемы в данной работе? 2. Что называют током полного отклонения и напряжением полного отклонения электроизмерительного прибора? 3. Каким образом включают амперметр и вольтметр в электрическую цепь для измерения тока и напряжения? Продемонстрируйте навыки включения этих приборов в электрическую цепь. 4. Что такое шунт? Для чего и как он используется? Продемонстрируйте использование шунта. 5. Что такое добавочное сопротивление? Для чего и как оно используется? Продемонстрируйте использование добавочного сопротивления. 6. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных. 7. Как в данной работе минимизируется погрешность экспериментальных данных? ***№ 26 «Измерение ёмкости конденсаторов мостовым методом»*** 1. Что такое конденсатор и его электроемкость? 2. Как определяется электроемкость при параллельном и последовательном соединении конденсаторов? 3. Как в данной работе проверяется закон последовательного и параллельного соединения конденсаторов? 4. Какая измерительная схема применялась в данной работе? 5. Что такое сопротивление конденсатора? 6. Приведите вывод формулы для определения неизвестной ёмкости в исследуемой схеме. ***№ 27 «Изучение резонанса напряжений»*** 1. Что такое колебательный контур? Какой вид колебаний наблюдался в данной работе? 2. Выведите уравнение колебательного контура 3. Схематически представьте векторную диаграмму	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		напряжений, для используемого в работе, колебательного контура. 4. Что такое резонанс напряжений? Обоснуйте, полученные в работе, графики. 5. Что такое добротность? Как она определялась в данной работе? ***№ 28 «Определение индуктивности катушки и магнитной проницаемости ферромагнитного тела»*** 1. Какие приборы применялись в данной работе для определия параметров постоянного и переменного тока? 2. Получите формулу для расчета полного сопротивления цепи переменного тока, используемой в данной работе (или представленной преподавателем). 3. Как определялась индуктивность катушки в данной работе? Каким еще способом можно определить индуктивность? 4. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных. ***№ 32 «Определение радиуса кривизны линзы и полосы пропускания светофильтра с помощью колец Ньютона»*** 1. Как объясняется появление колец Ньютона? 2. Получите формулы для расчета радиусов темных и светлых колец Ньютона. 3. Получите формулу для определения радиуса кривизны линзы. 4. Как в данной работе минимизируется погрешность экспериментальных данных? ***№ 34 «Определение длины световой волны и характеристик дифракционной решетки»*** 1. Каковы параметры и характеристики дифракционной решетки, применяемой в эксперименте? 2. Получите формулу для определения длины световой волны	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		при дифракции на дифракционной решетке. 3. Каково практическое применение дифракционных решеток? 4. Как в данной работе минимизируется погрешность экспериментальных данных? ***№ 35 «Определение концентрации растворов сахара и постоянной вращения»*** 1. На основе какого явления определяется концентрация раствора сахара в данном эксперименте? 2. Поясните устройство и принцип действия призмы Николя 3. Поясните устройство и принцип действия полутеневого сахариметра 4. Как в данной работе минимизируется погрешность экспериментальных данных?	
Владеть	− навыками работы с измерительными приборами и оборудованием; − методами проведения физических измерений, расчета величин и анализа полученных данных	**Примерный перечень вопросов и заданий по лабораторным работам (3 семестр)** ***№ 36 «Снятие вольтамперных характеристик фотоэлемента и определение его чувствительности»*** 1. Проанализируйте полученные в лабораторной работе ВАХ 2. Как определяется постоянная Планка в данном эксперименте? 3. Как в данной работе минимизируется погрешность экспериментальных данных? 4. Как в данной работе рассчитывается погрешность определения постоянной Планка? 5. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных. ***№ 37 «Исследование излучения абсолютно черного тела»*** 1. Проанализируйте полученные в лабораторной работе зависимости. 2. Как определяется постоянная Стефана-Больцмана и постоянная Вина в данном эксперименте?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		3. Как в данной работе минимизируется погрешность экспериментальных данных? 4. Как в данной работе рассчитывается погрешность определения постоянной Стефана-Больцмана и постоянной Вина? 5. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных ***№ 41 «Исследование возбуждения атомов газа»*** 1. Объясните принцип определения возбужденных состояний атомов газа в эксперименте? 2. Поясните принцип работы электронной лампы 3. В каком диапазоне электромагнитных волн лежит излучение возбужденных атомов паров ртути и почему? 4. Как в данном эксперименте определяется область локализации электрона и как полученные данные согласуются с теоретическими предпосылками? ***№ 42 «Определение главных квантовых чисел возбужденных состояний атома водорода»*** 1. Поясните устройство и принцип работы спектроскопа, используемого в данной работе 2. Получите формулу для определиния главных квантовых чисел возбужденных состояний атома водорода и других водородоподобных атомов 3. Что называется градуировочным графиком? 4. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных ***№ 51 «Изучение закономерностей α-распада»*** 1. Что такое активность радиоактивного элемента, ее вычисление и единицы измерения. 2. В чем состоит закон Гейгера - Неттола?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		3. Как оценить энергию α - частицы? 4. Устройство и принцип работы счетчика Гейгера-Мюллера. 5. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных ***№ 53 «Определение максимальной энергии β-частиц и идентификация радиоактивных препаратов»*** 1. Какие известны разновидности бета-распада? Какая из них исследуется в данном эксперименте? 2. В каких диапазонах находятся периоды полураспада и энергии бета- распада природных радионуклидов? 3. Каковы основные особенности взаимодействия бета-частиц с веществом? 4. Продемонстрируйте возможность применения среды Microsoft Excel (или другой среды) для обработки экспериментальных данных	
Знать	• Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации. • методы шифрования, использующие классические симметричные алгоритмы, • методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации, • методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. • общие принципы действия шифровальной машины Энигма • общие принципы шифрования, используемые в	**Вопросы для зачета** 1. Основные понятия криптографии. 2. Модели шифров. 3. Открытые сообщения и их характеристики. 4. Виды информации, подлежащие закрытию, их модели и свойства. 5. Блочные и поточные шифры. 6. Понятие криптосистемы. 7. Ручные и машинные шифры. 8. Основные требования к шифрам. 9. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок 10. Поточные шифры. Шифры замены. Одноалфавитные и многоалфавитные замены. 11. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа.	Б1.Б.27 Криптографические методы защиты информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	алгоритме симметричного шифрования AES • принципы шифрования информации с помощью биграммного шифра Плейфера • Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.	12. Вопросы криптоанализа простейших шифров замены. 13. Стандартные алгоритмы криптографической защиты данных. **Перечень вопросов для экзамена** 1. Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. 2. Методы получения случайных и псевдослучайных последовательностей. 3. Методы усложнения последовательностей псевдослучайных чисел. 4. Методы криптоанализа. 5. Понятие криптоатаки. 6. Классификация криптоатак. 7. Классификация методов анализа криптографических алгоритмов 8. Шифры с открытыми ключами 9. Криптосистемы RSA и Эль-Гамаля. 10. Преимущества асимметричных систем шифрования. 11. Криптографические хэш-функции. 12. Характеристики и алгоритмы выработки хэш-функций. 13. Модели криптографических протоколов 14. Понятие криптографического протокола. 15. Основные примеры, классификация криптографических протоколов. понятие электронной цифровой подписи. 16. Стандарты ЭЦП. 17. Протоколы установления подлинности. 18. Протоколы управления ключами. 19. Взаимосвязь между протоколами аутентификации и цифровой подписи. 20. Протоколы сертификации ключей. 21. Протоколы распределения ключей. 22. Аппаратные возможности АПМДЗ «Криптон-Замок»	
Уметь	• исследовать различные методы защиты текстовой информации и их стойкости на	Провести оценку шифрования по критериям: • Надежность шифров.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	основе подбора ключей • Участвовать в настройке криптографических средств обеспечения информационной безопасности. • Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ. • Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.	• Имитостойкость шифров. • Помехоустойчивость шифров. • Криптографическая стойкость шифров. • Имитация и подмена сообщения. Характеристика имитостойкости шифров. • Коды аутентификации. • Характеристики помехоустойчивости.	
Владеть	• Техникой настройки криптографических средств обеспечения информационной безопасности. • Навыками использования криптографических средств обеспечения информационной безопасности автоматизированных систем. • Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	1. Оценить криптостойкость метода шифрования с помощью биграммного шифра Плейфера и возможности применения метода в современных криптосистемах. 2. Разграничить доступа к аппаратным ресурсам ПЭВМ с АПМДЗ «Криптон-Замок». Создать несколько пользователей с различными правами доступа. Обеспечить контроль целостности установленной программной среды. Настроить блокировку компьютера при НСД. Проверить журнал событий. 3. Спроектировать конфигурацию СКЗИ для многофункционального АРМ.	
Знать	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по технической защите информации. Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.	Вопросы к экзамену 1. Характеристики способов и средств наблюдения в оптическом диапазоне. 2. Характеристики зрительной системы человека. 3. Виды и характеристики объективов. 4. Визуально-оптические приборы (бинокли, трубы. Телескопы) 5. Приборы ночного видения и тепловизоры. 6. Способы и средства наблюдения в радиодиапазоне. 7. Задачи, решаемые при перехвате сигналов и	Б1.Б.29 Техническая защита информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		структура типового комплекса для перехвата. 8. Виды и характеристики антенн. 9. Радиоприёмники и их характеристики. 10. Способы и средства прослушивания, слуховая система человека. 11. Стетоскопы и телефонные закладки. 12. Метод ВЧ-навязывания и его применение для добывания информации. 13. Характеристики закладных устройств, затрудняющие их обнаружение. 14. Средства и методы (не меньше двух) обнаружения закладных устройств.	
Уметь	Участвовать в настройке технических средств обеспечения информационной безопасности. Самостоятельно настраивать технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации. Применять технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств обеспечения информационной безопасности.	Задания: 1. Замаскировать речевые сигналов акустическими шумами в аудитории с использованием системы виброакустической и акустической защиты Соната-АВ (модель 3М). 2. Обеспечить защиту речевой информации от съема по вибрационному каналу в аудитории с использованием системы виброакустической и акустической защиты Соната-АВ (модель 3М). 3. Вычислить мощность радиосигнала в канале CDMA с использованием анализатора спектра «АКС-1301». 4. Настроить СЗИ Соната-АВ. 5. Провести исследование систем активного зашумления и расчет показателей их эффективности с использованием комплекса «Сигурд». 6. Рассчитать отношения «сигнал/шум» в отходящих линиях с использованием комплекса «Сигурд».	
Владеть	Техникой настройки технических средств обеспечения информационной безопасности. Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления	1. С использованием комплекса «Кассандра» определить количество пиковых сигналов в заданном диапазоне частот. Провести полный анализ каждого пикового сигнала. Установить пояснительные метки на все пиковые сигналы. Вывести спектрограмму заданного диапазона частот, графики накопленных максимумов. Найти сигнал максимальной мощности и пометить его. 2. С использованием комплекса «Кассандра» в заданном	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	потенциальных уязвимостей информационной безопасности автоматизированных систем.	диапазоне частот регистрировать и заносить в список слабые шумоподобные сигналы. Регистрировать факт наличия излучения на заданной частоте. Провести анализ определения линии порога с использованием критерия «идеального наблюдателя» и критерия Неймана-Пирсона. Обосновать способ создания линии порога. 3. Найти радиозакладку с помощью комплекса радиомониторинга «Кассандра». 4. С использованием комплекса «Кассандра» создать базу данных легальных сигналов и создать на ее основе эталонную панораму частот. Найти разность эталонной и текущей панорам.	
Знать	Виды программных и программно-аппаратных средств защиты информации. Принципы администрирования системы ИБ АС. Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ.	Вопросы к экзамену: 1. Обеспечение разграничения и контроля доступа пользователей к техническим средствам вычислительной сети на примере АПМДЗ «КРИПТОН-ЗАМОК». 2. Предмет и задачи программно-аппаратной защиты информации. 3. Идентификация и аутентификация пользователя. 4. Типовые схемы идентификации и аутентификации пользователя. 5. Управление доступом к информации в КС. 6. Основные механизмы систем защиты информации в ИС на примере СЗИ «Страж NT».	Б1.Б.32 Программно-аппаратные средства обеспечения информационной безопасности
Уметь	Самостоятельно настраивать программные и программно-аппаратные средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных СЗИ. Применять программные и программно-аппаратные средства обеспечения ИБ.	В СЗИ «Страж NT» настроить приложение для работы с грифованными ресурсами, исходя из записей аудита в журнале событий. Продемонстрировать различия работы с ресурсами, имеющими различные грифы. Создать шаблон настройки приложения для использования грифованных носителей и применить его для всех пользователей.	
Владеть	Техникой настройки программных и программно-аппаратных средств обеспечения ИБ. Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС. Навыками анализа архитектурно-технических и схемотехнических решений компонентов АС с	Провести тестирование СЗИ «Страж NT». Осуществить переидентификацию пользователей без перезагрузки операционной системы. Произвести маркировку документов и продемонстрировать различия печати нескольких документов с разными грифами. Продемонстрировать блокировку и разблокировку системы. Произвести аварийное снятие системы защиты. Затем	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	целью выявления потенциальных уязвимостей ИБ АС.	восстановить подсистему идентификации и работоспособность основных служб СЗИ «Страж NT».	
Знать	- Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. - Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации. - Способы контрольных проверок работоспособности и эффективности применяемых программных и программно- аппаратных СЗИ.	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- Участвовать в настройке технических средств обеспечения информационной безопасности. - Самостоятельно настраивать технические средства обеспечения информационной безопасности. - Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации. - Применять технические средства обеспечения информационной безопасности. - Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно- аппаратных СЗИ. - Применять программные и программно-аппаратные средства обеспечения ИБ.		
Владеть	- Техникой настройки технических средств обеспечения информационной безопасности - Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. - Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной безопасности автоматизированных систем. - Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС.	– изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. - Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации. - Способы контрольных проверок работоспособности и эффективности применяемых программных и программно- аппаратных СЗИ.	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- Участвовать в настройке технических средств обеспечения информационной безопасности. - Самостоятельно настраивать технические средства обеспечения информационной безопасности. - Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации. - Применять технические средства обеспечения информационной безопасности. - Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно- аппаратных СЗИ. - Применять программные и программно-аппаратные средства обеспечения ИБ.		
Владеть	- Техникой настройки технических средств обеспечения информационной безопасности - Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем. - Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС.	– изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем			
Знать	– уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; – требования к разработке и производству, проведению испытаний, поддержке безопасности СЗИ для определения уровня доверия; – положение о системе сертификации средств защиты информации; – продукцию, которую необходимо сертифицировать; – состав участников системы сертификации и их основные функции; – этапы сертификации; – требования к защищенность информации в автоматизированных системах; – требования к проведению испытаний СЗИ; порядок проведения сертификационных испытаний.	1. Что понимают под сертификацией? 2. Основные отличия сертификации от лицензирования и аттестации. 3. Сколько участников входит в процесс сертификации ФСТЭК России? 4. Перечислите основные этапы сертификации. 5. Виды сертификационных испытаний. 6. Назовите основные отличия инспекционного контроля от сертификационных испытаний. 7. Перечислите основные руководящие документы в области сертификации СЗИ. 8. Какие существуют этапы при отборе образца продукции при проведении сертификационных испытаний? 9. Основные положения руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». 10. Основные положения руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». 11. Основные положения руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от	Б1.Б.33 Разработка и эксплуатация защищенных автоматизированных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		несанкционированного доступа к информации». 12. Основные положения руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». 13. Общий порядок проведения сертификации СЗИ. 14. Виды сертификационных испытаний. ●	
Уметь	– составлять техническое задание на выполнение работ по проведению сертификационных испытаний; – составлять акт отбора образца; – подать заявку на сертификацию; оформить экспертное заключение и проект сертификата соответствия по результатам сертификации.	**Задание** Составить заявку на сертификацию в федеральный орган по сертификации, которая должна включать: • наименование заявителя; • наименования продукции, которую Заявитель просит сертифицировать; • перечень нормативных и методических документов, на соответствие требованиям, которых Заявителю необходимо сертифицировать продукцию; • предложения Заявителя по выбору испытательной лаборатории, которая будет проводить сертификационные испытания; ● • дополнительные условия или сведения	
Владеть	навыками проведения испытаний средств защиты информации, а также обеспечения безопасности средств защиты информации в ходе их применения	**Задание** 1. Выбрать любое свободное ПО. Найти всю возможную информацию о продукте (техническую и функциональную) необходимую для его дальнейшей сертификации. 2. Составить соглашение о неразглашении (NDA) между испытательной лабораторией и заявителем. 3. Определить используемую общественную лицензию, под которой распространяется выбранное ПО, и обозначить основные отличия от других существующих лицензий. ● Определить достаточность найденных материалов для проведения сертификации. Описать какие входные данные дополнительно необходимы для проведения сертификационных работ.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Знать	- способы организации автоматизированных систем; - подходы к проведению сертификации средств защиты информационной безопасности;	1. Децентрализованные автоматизированные системы. 2. Гомогенные и гетерогенные автоматизированные системы. 3. Система сертификации ФСТЭК России. 4. Порядок проведения сертификации средства защиты информации 5. Сертификационные испытания средства защиты информации	Б1.В.ДВ.05.01 Методы мониторинга информационной безопасности АС
Уметь	- составлять регламент испытаний средств защиты информации автоматизированных систем	По заявленным характеристикам определить является ли средство подлежащим сертификации и определить перечень требуемых испытаний.	
Владеть	- навыками применения специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем;	При помощи утилиты aircrack-ng выполнить анализ радиочастот в диапазоне 2.4 гГц. Определить количество беспроводных сетей и количество участников этих сетей. При помощи Metasploit провести аудит безопасности страница авторизации роутера.	
Знать	уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; - положение о системе сертификации средств защиты информации; -продукцию, которую необходимо сертифицировать; -состав участников системы сертификации и их основные функции; -этапы сертификации; - требования к проведению испытаний СЗИ; -порядок проведения сертификационных испытаний	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	─ составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия; ─ проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия ─ проводить анализ сертификата соответствия.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	─ нормативно-правовой базой в области сертификации средств защиты информации ─навыками проведения испытаний средств защиты информации,	*Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы)	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; - положение о системе сертификации средств защиты информации; -продукцию, которую необходимо сертифицировать; -состав участников системы сертификации и их основные функции; -этапы сертификации; - требования к проведению испытаний СЗИ; -порядок проведения сертификационных испытаний	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	─ составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия; ─ проводить анализ решения о проведении сертификации средства защиты информации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	/сертификационных испытаний для продления срока действия сертификата соответствия – проводить анализ сертификата соответствия.	– изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 44) Род деятельности предприятия, на котором проходила практика. 45) Какие способы защиты информации используются на предприятии? 46) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 47) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 48) Какая топология используется в локальных сетях на предприятии? 49) Как обеспечивается безопасность беспроводных сетей? 50) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 51) Охарактеризуйте должностные обязанности лиц	
Владеть	– нормативно-правовой базой в области сертификации средств защиты информации –навыками проведения испытаний средств защиты информации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		ответственных за обеспечение информационной безопасности на предприятии. 52) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 53) Опишите способы контроля трафика по локальным сетям предприятия. 54) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 55) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 56) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 57) Какие операционные системы используются на ПК персонала предприятия? 58) Какие операционные системы используются на серверах предприятия? 59) Понятие и виды защищаемой информации по законодательству РФ. 60) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 61) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 62) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 63) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 64) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		65) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 66) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 67) Основное содержание разработки Политики безопасности предприятия (организации). 68) Принципы, основные задачи и функции обеспечения информационной безопасности. 69) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 70) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 71) Ответственность за нарушение законодательства в информационной сфере. 72) Основные мероприятия по защите информации при проведении совещаний и переговоров. 73) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 74) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 75) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 76) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 77) Сформулировать основные правила безопасной работы в компьютерной системе. 78) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 79) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		80) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 81) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 82) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 83) Рассмотреть особенности разграничения доступа и аудита в СЗИ 84) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 85) Раскрыть особенности образования электромагнитных каналов утечки информации. 86) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	– правила оформления научно-технической документации; – принципы работы и параметры используемого оборудования для проведения экспериментально-исследовательских работ; – типовые схемы экспериментального исследования основных электронных приборов и устройств	Определение сертификации средств защиты информации Правила и участники сертификации средств защиты информации Законодательно-правовые основы сертификации Традиционные руководящие документы Гостехкомиссии России Классы защищенности средств вычислительной техники Классы защищенности межсетевых экранов Классы защищенности автоматизированных систем Функциональные требования безопасности Требования доверия к безопасности . Требования к системам обнаружения вторжений . Требования к средствам антивирусной защиты	ФТД.01 Тестирование систем защиты информации автоматизированных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	– составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия; – проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия – проводить анализ сертификата соответствия.	Провести тестирование механизмов фильтрации данных и трансляции адресов Провести тестирование механизмов идентификации и аутентификации администраторов Провести тестирование механизмов контроля целостности Провести тестирование антивирусной защиты	
Владеть	– терминологий в области экспериментально–исследовательских работ, а также способностью вести аргументированную дискуссию по результатам экспери-ментально-исследовательских работ; – нормативно-правовой базой в области сертификации средств защиты информации	Составить план и пояснить этапы методики сертификационных испытаний Составить план и пояснить этапы тестирования дискреционного принципа контроля доступа Составить план и пояснить этапы тестирования мандатного принципа контроля доступа Составить план и пояснить этапы тестирования механизмов очистки памяти Составить план и пояснить этапы тестирования механизмов изоляции модулей Составить план и пояснить этапы тестирования механизмов идентификации и аутентификации субъектов доступа Составить план и пояснить этапы тестирования механизмов контроля целостности Составить план и пояснить этапы тестирования испытаний межсетевых экранов	
ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации			
Знать	– Средства выявления нарушений информационной безопасности; – Подходы и методы выявления нарушений информационной безопасности;	Теоретические вопросы: 1. Обнаружение аномалий в защищаемой системе. 2. Обнаружение злоупотреблений в защищаемой системе. 3. Накопление наиболее характерной статистической информации для каждого параметра оценки. 4. Обучение нейронных сетей значениями параметров оценки. 5. Статистика Байеса.	Б1.В.04 Методы выявления нарушений информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	– Принимать участие в анализе результатов систем обнаружения вторжений (СОВ); – Проводить анализ существующих методов выявления нарушений и определять узкие места;	Задания: 1. Составить майнд-карту действий сотрудника компании выбранной должности для организации канала утечки конфиденциальных данных компании; 2. Провести анализ методов выявления нарушений одной из выбранной СОВ для устранения канала утечки с майнд-карты из 1 задания.	
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками исследования методов и алгоритмов, используемых в работе систем мониторинга ИБ;	1. Провести сравнительный анализ (методов и алгоритмов, используемых в работе систем) 2х систем обнаружения и предотвращения вторжений (IPS/IDS), имеющихся на сегодняшний день на рынке.	
Знать	– Средства анализа информационной безопасности; – Классификацию систем защиты информации; – Средства организации аттестации по требованиям безопасности информации.	1. Методики проведения аттестации ИС по требованиям защиты ПДн. 2. Цели и задачи аттестационных испытаний. 3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.	Б1.В.08 Аттестация АИС
Уметь	– Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; – Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.	3. Произвести измерения ПЭМИН от технических средств и составить протокол аттестационных испытаний 4. Произвести анализ информационных потоков, 5. Произвести проверку механизма обеспечения целостности. 6. Произвести проверку механизма регистрации и учета.	
Владеть	– Навыками использования средств анализа информационной безопасности;	2. Определить объем испытаний на соответствие требованиям по	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	– Навыками проведения аттестации в соответствии с существующими нормативами.	ЗИ от НСД. 3. Произвести аттестационные испытания и составить протокол для объекта информатизации (ОИ) на соответствие требованиям безопасности информации по направлению «Защита информации от НСД». 4. Разработать методику проведения аттестационных испытаний ОИ в соответствии с моделью угроз. 5. Составить заключение по результатам аттестационных испытаний.	
Знать	Средства анализа информационной безопасности; Классификацию систем защиты информации; Средства организации аттестации ВП по требованиям безопасности информации.	*перечень вопросов на защите отчета НИР:* 1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР? Какие охранные документы были получены в ходе выполнения НИР?	Б2.Б.02(Н) Научно-исследовательская работа
Уметь	Принимать участие в исследованиях аттестации системы защиты информации; Принимать участие в исследованиях и анализе аттестации системы защиты информации; Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.		
Владеть	Навыками использования средств анализа информационной безопасности; Навыками участия в проведении экспериментально- исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.		
Знать	– Средства анализа информационной безопасности;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта**	Б2.Б.03(П) Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	─ Классификацию систем защиты информации; ─ Средства организации аттестации по требованиям безопасности информации	**профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;	практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; ─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.		
Владеть	─ Навыками использования средств анализа информационной безопасности; ─ Навыками проведения аттестации в соответствии с существующими нормативами.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Вопросы, подлежащие изучению: 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		охраны особо важных объектов	
Знать	─ Средства анализа информационной безопасности; ─ Классификацию систем защиты информации; ─ Средства организации аттестации по требованиям безопасности информации	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; ─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.		
Владеть	─ Навыками использования средств анализа информационной безопасности; ─ Навыками проведения аттестации в соответствии с существующими нормативами.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	Средства анализа информационной безопасности; Классификацию систем защиты информации; – Средства организации аттестации ВП по требованиям безопасности информации.	Методики проведения аттестации ИС по требованиям защиты ПДн. Цели и задачи аттестационных испытаний. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. Условия и порядок проведения аттестационных испытаний объекта ВТ. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ. Объем испытаний на соответствие требованиям по ЗИ от НСД. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. Условия и порядок проведения аттестационных испытаний ВП. . Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. . Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. . Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.	ФТД.01 Тестирование систем защиты информации автоматизированных систем
Уметь	Принимать участие в исследованиях аттестации системы защиты информации; Принимать участие в исследованиях и анализе аттестации системы защиты информации; Проводить научно-исследовательские работы при	7. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации с целью дальнейшего тестирования. 8. Произвести тестирование информационных потоков 9. Определить состав использованных для обработки	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.	защищаемой информации средств ВТ и составить план тестирования. 10. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 11. Определить условия и порядок проведения тестирования для аттестации объекта ВТ. 12. Произвести тестирование защиты информации от утечки за счет ПЭМИ СВТ.	
Владеть	Навыками использования средств анализа информационной безопасности; Навыками проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.	52. Определить объем тестирования на соответствие требованиям по ЗИ от НСД. 53. Произвести проверку ВП на соответствие организационно-техническим требованиям по защите информации. 54. Определить условия и порядок тестирования ВП для последующей аттестации. 55. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 56. Определить объем тестирования ВП на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 57. Произвести тестирование требований по защите информации от утечки по акустическому и виброакустическому каналам для ВП.	
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации			
Знать	Классификацию технических средств перехвата информации Возможности технических средств перехвата информации Организацию защиты информации от утечки по	Вопросы к экзамену 15. Способы подключения и защита телефонной линии. 16. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него. 17. Беззаходовые методы прослушивания помещений по	Б1.Б.29 Техническая защита информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	техническим каналам на объектах информатизации.	ТЛ. 18. Мобильные системы связи и их использование в информационных атаках. 19. Защита информации от атак с помощью сотовых телефонов и диктофонов. 20. Оптические каналы утечки информации (атака и защита). 21. Радиоэлектронные каналы утечки информации. 22. Пассивные и активные методы защиты информации в радиоэлектронном канале. 23. Способы и принципы инженерно технической защиты информации. 24. Способы и средства инженерной защиты и технической охраны объектов. 25. Утечка информации по ПЭМИН и применяемые меры защиты. 26. Зоны электромагнитного поля и возможности утечки информации. 27. Контролируемая зона и критерий защищённости СВТ.	
Уметь	Классифицировать технические средства перехвата информации. Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации Выявлять каналы утечки информации Проводить контроль эффективности мер по защите информации техническими средствами	Задания: 1. Изучить устройство и принципы работы комплекса радиомониторинга и цифрового анализа сигналов «Кассандра». 2. Обнаружить устройства и проанализировать сети Wi-Fi с использованием комплекса радиомониторинга и цифрового анализа сигналов «Кассандра». 3. Обеспечить маскировку информативных ПЭМИН устройств вычислительной техники, размещённой в аудитории МГТУ с использованием генератора радиошума ГШ-1000М. 4. Обеспечить подавление нормальной работы телефонных закладок любых типов подключения во время переговоров с использованием устройства защиты Прокруст 2000 в аудитории МГТУ.	
Владеть	Средствами технической защиты информации. Методами технической защиты	1. Провести исследование ТС на наличие информативных сигналов ПЭМИН с использованием комплекса «Сигурд». 2. Произвести расчет показателей защищенности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информации. Навыками проведения проверки защищенности информации и эффективности мер по защите информации	технических средств от утечки информации по каналу ПЭМИН в соответствии с действующими нормативными документами с использованием комплекса «Сигурд».	
Знать	- перечень инструментов для проведения мониторинга защищенности информации;	1. Режимы сканирования сетей. 2. Способы определения операционной системы на исследуемом узле. 3. Инструменты для проведения MITM атаки 4. Инструменты для проведения bruteforce.	Б1.В.ДВ.05.01 Методы мониторинга информационной безопасности АС
Уметь	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;	Определить протокол, используемый для авторизации участников сети. Выполнить атаку Pixie Dust. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности устройства. Выполнить атаку на роутер с авторизацией по протоколу WPA2. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности устройства.	
Владеть	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;	Провести комплексный тест выбранного узла при помощи инструментов дистрибутива Kali Linux 2.	
Знать	- перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;		
Владеть	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;	– изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности			
Знать	– основы принятия управленческих решений	Сущность и содержание управленческого решения. Классификация и целевая ориентация управленческих решений. Требования к управленческому решению. Обобщенная схема процесса разработки управленческих решений. Формы разработки и реализации управленческих решений. Факторы, влияющие на управленческое решение.	Б1.Б.10Основы управленческой деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Влияние внешней среды на реализацию альтернативных решений. Взаимодействие моделей и методов при разработке управленческих решений. Аналитические, статистические и математические методы. Экспертные и эвристические методы. Метод сценариев. Метод дерева решений. Типы моделей. Понятие о системах. Выбор критерия эффективности. Проблемы в межличностных контактах. Характеристики коммуникационных сетей. Понятие управления человеческими ресурсами. Основные этапы управления человеческими ресурсами. Руководство и лидерство.	
Уметь	– организовывать работу малых коллективов исполнителей	Практическое задание 1 "Эволюция управленческой мысли и школы научного управления», примерный перечень тем: 1. Теория и практика управления в рабовладельческом обществе: управление в странах Древнего Востока (Египет, Вавилон, Индия, Китай) 2. Управленческие концепции мыслителей античных государств (Греция, Рим) 3. Трансформация управленческих идей в период расцвета и упадка феодального общества, развития рыночного уклада 4. Управленческие концепции в XVI–XVIII вв.: трактовка власти и управления Н. Макиавелли; «утопические проекты» организации экономики и управления 5. Теоретические основы возникновения управленческой науки: теория разделения и специализации труда Ч. Бэббиджа, философия производства Э. Юра, идеи Р. Оуэна 6. Школа научного управления. Влияние Ф. У. Тейлора на развитие теории и практики управления 7. Развитие идей Ф. У. Тейлора: в трудах Г. Гантта; теория рационализации управления Ф. и Л. Гилбрет 8. Школа научного управления. Принципы эффективности управления Г. Эмерсона; принципы организации производства Г. Форда 9. Административная школа менеджмента. Административная теория А. Файоля	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		10. Развитие административной теории: теория организации Л. Гулика; управленческие принципы Дж. Муни и А. Рейли; синтетическая теория Л. Урвика 11. Теория бюрократической организации М. Вебера 12. Развитие бюрократической теории в работах Р. Мертона; трактовка бюрократии А. Гоулднером 13. Теория жизненного цикла бюрократических структур Э. Доунса; модернизация теории бюрократии М. Крозье 14. Школа человеческих отношений. Промышленная психология Г. Мюнстерберга; философия управления М. П. Фоллетт. Теория организации Ч. Барнарда 15. Сущность хоторнских экспериментов. Управленческие идеи Э. Мэйо 16. Теория организационного поведения Ф. Ротлисбергера 17. Бихевиористская школа менеджмента Предпосылки формирования и особенности 18. Теория мотивации и управления А. Маслоу; теория стилей руководства Д. Макгрегора; теория мотивации и обогащения труда Ф. Герцберга 19. Количественный подход. Развитие математических методов исследования в системе управления 20. Системный подход в менеджменте. История возникновения и особенности системного подхода 21. Управленческие идеи П. Друкера. Модель «Маккинси – 7С» 22. Ситуационный подход в менеджменте. Возникновение и основы ситуационного подхода к управлению. Ситуационные теории управления 23. Специфика российского менеджмента в первой половине XX в.: теория и практика управления в дореволюционный период. Развитие менеджмента в 1920-е гг. 24. Особенности развития теории и практики управления в период формирования командно-административной системы в СССР 25. Тенденции отечественного менеджмента во второй	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		половине XX в. Аудиторное тестирование. Примерное тестовое задание «Эволюция теории и практики управления» Главный исполнитель воли фараона и управляющий всеми делами государства в Древнем Египте номархи писцы наместники фараона везиры Важнейший вклад вавилонян в развитие управленческой мысли предписания о служебных обязанностях верховного сановника свод законов Хаммурапи поучения Птаххотепа Представители высшей касты в Древней Индии кшатрии шудры брахманы вайшьи Основы управления государством в мирное и военное время в Древней Индии изложены в книге Аюрведы книге правителя области Шан законах Ману трактате Артхашараста Источник концепции полицейского управления даосизм дегизм конфуцианство моизм Автор политического учения о функциях верховного правителя Никколо Макиавелли Адам Смит	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Томас Мор Илон Маск Согласно трактату "Государь" хороший правитель должен вводить льготы для граждан в управлении опираться на средние слои способствовать развитию рынка иметь абсолютный авторитет у народа Томас Тор был казнен как автор произведения "Утопия" отказа подчиняться Папе Римскому и признавать католицизм главной верой как автор манифеста "В защиту семи таинств" в результате отказа присягнуть Генриху VIII и сохранения верности католицизму В "Утопии" Томаса Мора идеальное общество подчиняется законам демократии и коллективизма националистично контролируется и регулируется законом является анархичным Большой вклад в развитие учетной, аналитической и контрольной функции управления в период зарождения рыночного уклада внес Лука Пачоли Марсилий Падуанский Григорий III Никколо Макиавелли Практическое задание 4 «Методы стратегического планирования. SWOT-анализ» Составить список сильных и слабых сторон организации, а также угроз и возможностей внешней среды и этап установить связи между ними Практическое задание 7 «Управление поведением человека в организации» Охарактеризовать стили неэффективного лидерства, разработанных И. Адизесом: «Герой-одиночка», «Бюрократ», «Поджигатель», «Горячий сторонник», «Мертвый пень», которые описывают менеджеров, способных выполнять только одну функцию из четырех необходимых или вообще не выполнять ни одной, заполнив таблицу	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	– навыками управления поведением человека в организации	Практическое задание 5 «Методы принятия управленческих решений» Подготовка проекта решения ЛПР (на ком лежит ответственность за принятое решение) и группой экспертов с использованием вероятностного метода. Определить проблему и условия риска - возможность потерь в условиях неопределенности: по пессимистическому и оптимистическому сценарию. Определить упущенную выгоду. Построить дерево решений Практическое задание 6 «Руководство и лидерство. Стили лидерства» Используя «решетку лидерства» *Роберта Блейка и Джейн Моутон* (1985), основанную на предположении о том, что лидеры организаций действуют в двух направлениях, которые обозначаются как «внимание на производство» и «внимание на людей», смоделировать ситуации использования базовых типов лидерского поведения (одного или нескольких) на примере конкретной организации	
Знать	Основные меры по защите информации в автоматизированных системах. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Принципы организации работы малых коллективов исполнителей.	Вопросы для зачета 4. Требования защиты информации. 5. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду. 6. Угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду. 7. Угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.	Б1.Б.26Основы информационной безопасности
Уметь	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.	1. Классифицировать защищаемую информацию по видам тайны. 2. Классифицировать защищаемую информацию по степеням конфиденциальности. 3. Составить перечень средств ЗИ для обеспечения защиты от утечки по акустическому каналу.	
Владеть	Профессиональной терминологией в области информационной безопасности. Навыками участия в проведении	1. Составить глоссарий по терминологии в области информационной безопасности. 2. Исследовать угрозы национальной безопасности страны в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	исследовательских работ по информационной безопасности. Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.	военной сфере. 3. Исследовать стратегия развития информационного общества в России.	
Знать	организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	Теоретические вопросы 18. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта. 19. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности. 20. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима. 21. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. 22. Требования к помещениям и хранилищам, в которых ведутся закрытые работы. 23. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. 24. Защита информации в экстремальных ситуациях.	Б1.Б.31 Организационное и правовое обеспечение информационной безопасности
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности -анализировать и обобщения информации на стадии принятия и реализации управленческого решения, -пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров	1. Описать выбранный объект обеспечения физической безопасности: сооружения, предметы, люди. Описать для него организацию охраны, пропускного и внутриобъектового режима.	
Владеть	-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований,	1. Разработать требования к организации работы режимного помещения предприятия. 2. Написать регламент организации защиты информации при приеме посетителей, командированных лиц и иностранных представителей.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	-методами организации и управления деятельностью служб защиты информации на предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов,	3. Написать инструкцию по защита информации в экстремальных ситуациях.	
Знать	организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации -организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности -анализировать и обобщения информации на стадии принятия и реализации управленческого решения, -пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров		
Владеть	-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований, -методами организации и управления деятельностью служб защиты информации на		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов	– изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации -организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:*	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности -анализировать и обобщения информации на стадии принятия и реализации управленческого решения, -пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров		
Владеть	-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	Федерации, муниципальных образований, -методами организации и управления деятельностью служб защиты информации на предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов	– ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы			
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные угрозы безопасности информации и модели нарушителя в ИС; - стратегии обеспечения ИБ, способы их организации и оптимизации.	**Теоретические вопросы** 1. Назовите основные угрозы безопасности информации 2. Дайте описание внешнего нарушителя 3. Кто относится к внутренним нарушителям 4. Цели тестирования системы защиты	Б1.Б.34Управление информационной безопасностью
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.	1. Провести анализ защищенности внешнего периметра корпоративной сети. 2. Провести анализ защищенности внутренней ИТ-инфраструктуры.	
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о	По проведенному анализу защищенности подготовить: 1. Рекомендации по устранению организационных	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	применимости механизмов контроля в контексте управления рисками ИБ.	уязвимостей. 2. Рекомендации по устранению уязвимостей внешнего периметра сети. 3. Рекомендации по устранению уязвимостей внутренней ИТ-инфраструктуры.	
Знать	- нормативные методические документы ФСТЭК России в области ИБ АС; - основные угрозы безопасности информации и модели нарушителя в АС; - способы оптимизации систем управления информационной безопасности (СУИБ).	Теоретические вопросы: 1. Модель угроз информационной безопасности STRIDE 2. Модель оценки рисков DREAD 3. Нормативные и правовые акты, методические документы и национальные стандарты РФ в области обеспечения безопасности, относящиеся к управлению информационной безопасностью.	Б1.В.10 Системы управления информационной безопасностью
Уметь	- анализировать применяемые инструменты в области проектирования и управления ИБ с учетом стоимости и категорирования защищаемых объектов; - обосновывать целесообразность применяемых мер по обеспечению ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.	Задания: 1. Выбрать решение для защиты выбранной корпоративной инфраструктуры. 2. Обосновать целесообразность выбранного решения для защиты выбранной корпоративной инфраструктуры.	
Владеть	- навыками расследования инцидентов ИБ; - навыками сбора и анализа исходных данных, проведение обследования бизнес-процессов компании, входящих в область действия СУИБ; - навыками оценки активов (первичных и вторичных) компании, входящих в область действия СУИБ; - навыками определения владельцев и ценности активов;	Задания: 1. Определить основные векторы атак и попытаться смоделировать их на выбранной корпоративной инфраструктуре. 2. Провести анализ GPO средствами SCM. 3. Протестировать на проникновение инструментом OWASP ZAP выбранное веб-приложение.	
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные принципы создания системы управления информационной безопасностью.	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:**	Б2.Б.03(П) Производственная-практика по получению профессиональных умений

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- методы реализации системы управления безопасностью	*Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:*	и опыта профессиональной деятельности
Уметь	- проводить оценку информационных рисков, - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.		
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ. - навыками подготовки документации СУИБ		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		охраны особо важных объектов	
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные принципы создания системы управления информационной безопасностью. - методы реализации системы управления безопасностью	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- проводить оценку информационных рисков, - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.		
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ. - навыками подготовки документации СУИБ		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности			
Знать	Основы организационного и правового обеспечения ИБ. Основные нормативные и правовые акты в области обеспечения ИБ. Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. Методики проектирования АС в защищенном исполнении.	Вопросы к экзамену: 1. Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них. 2. Этапы формирования Перечня сведений, содержащих служебную или коммерческую тайну, для структурных подразделений (отделов, служб) организации. 3.Подсистемы интегрированной архитектуры систем ИБ.	Б1.Б.36Информационная безопасность распределенных информационных систем
Уметь	Реализовывать разработанную автоматизированную систему с учетом требований ИБ. Организовывать реализацию разработанной АС с учетом требований информационной безопасности. Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.	1. Разработайте ТЗ на создание системы информационной безопасности для выбранного ОИ. 2. Разработайте ТЗ на создание системы информационной безопасности для выбранной АИС. 3. Разработайте архитектуру системы ИБ.	
Владеть	Навыками разработки автоматизированных систему с учетом требований ИБ. Навыками контроля разработки АС с учетом требований ИБ.	1. Разработайте модель системы управления ИБ (на основе процессно-ролевой модели) для выбранного ОИ. 2. Разработайте модель системы управления ИБ (на основе процессно-ролевой модели) выбранной АИС.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	Навыками контроля эффективности применения разработанной АС в защищенном исполнении. Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении.	3. Разработайте технически-рабочий проект создания системы ИБ.	
Знать	- Основы организационного и правового обеспечения ИБ. - Основные нормативные и правовые акты в области обеспечения ИБ. - Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. - классификацию информационных систем по требованиям защиты информации.	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- Определять класс защищенности информационной системы - Принимать участие в реализации разработанной АС с учетом требований информационной безопасности. - Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. - Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении. - выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы - определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации		
Владеть	- Навыками разработки автоматизированных систему с учетом требований ИБ. - Навыками контроля разработки АС с учетом требований ИБ. - Навыками выбора средств защиты информации,		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	сертифицированных на соответствие требованиям по безопасности информации - Навыками разработки сопроводительной документации к разработанной подсистеме защиты информации АС	– изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Основы организационного и правового обеспечения ИБ. - Основные нормативные и правовые акты в области обеспечения ИБ. - Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. - классификацию информационных систем по требованиям защиты информации.	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- Определять класс защищенности информационной системы - Принимать участие в реализации разработанной АС с учетом требований информационной безопасности. - Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. - Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении. - выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы - определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	- Навыками разработки автоматизированных систему с учетом требований ИБ. - Навыками контроля разработки АС с учетом требований ИБ. - Навыками выбора средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации - Навыками разработки сопроводительной документации к разработанной подсистеме защиты информации АС	– изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем			
Знать	основные меры по защите информации в автоматизированных системах (организационные, правовые); автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Теоретические вопросы 1. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. 2. Лицензируемые виды деятельности в области защиты информации. 3. Порядок получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации. Существующие лицензионные требования. 4. Порядок получения лицензии ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. 5. Существующие лицензионные требования. 6. Сертификация. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации	Б1.Б.31 Организационное и правовое обеспечение информационной безопасности
Уметь	разрабатывать проекты нормативных и организационно- распорядительных документов,	1. Разработать проект документа «Допуск должностных лиц к информации ограниченного доступа, не отнесенной к	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия разрабатывать предложения по совершенствованию системы управления ИБ	государственной тайне».	
Владеть	методами организации и управления деятельностью служб защиты информации на предприятии	1. Разработать проект документа «Оценка соответствия помещения требованиям к помещениям и хранилищам, в которых ведутся закрытые работы.	
Знать	- требования к содержанию документов, разрабатываемых при проектировании распределенной информационной системы - виды и комплектность документов	Перечислить виды документов разрабатываемых при проектировании защищенной распределенной системы? Какой ГОСТ регулирует состав комплекта документов разрабатываемых при проектировании защищенной распределенной системы?	Б1.Б.37Методы проектирования защищенных распределенных информационных систем
Уметь	- разрабатывать структурную схему комплекса средств по обеспечению ИБ - разрабатывать общее описание системы защиты распределенной системы	Перечислить перечень основных структурных элементов применяемых при проектировании комплекса средств по обеспечению ИБ распределённой системы	
Владеть	- навыками описания программного обеспечения участвующего в обеспечении ИБ распределенной системы	Разработать программный документ по ГОСТ 19.101 на систему контроля сессией проекта Django	
Знать	─ нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; ─ организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	─ применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; ─ разрабатывать, реализовывать, оценивать и		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	корректировать процессы менеджмента информационной безопасности; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии?	
Владеть	– навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; – нормативными требованиями по защите информации; – навыками организации и обеспечения режима секретности – навыками разработки организационно-распорядительных документов		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. 44) Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	─ нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; ─ организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с	Б2.Б.04(Пд) Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	защиты информации;	требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии?	
Уметь	─ применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; ─ разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; ─ разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем		
Владеть	─ навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; ─ нормативными требованиями по защите информации; ─ навыками организации и обеспечения режима секретности ─ навыками разработки организационно-распорядительных документов		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; – нормативные правовые акты в области защиты информации; – основные методы управления проектами в	1. Перечислить национальные стандарты, рекомендуемые к применению при создании автоматизированных систем в защищенном исполнении 2. Рассказать порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении 3. Перечислить документы, относящиеся к эксплуатационной	ФТД.02 Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	области информационной безопасности.	документации на систему защиты автоматизированной системы 4. Перечислить виды испытаний автоматизированных систем 5. Перечислить виды программных документов 6. Перечислить требования к управлению документами проекта 7. Рассказать об основных понятиях проектного менеджмента и установить их взаимосвязь 8. Дать определение эксплуатационной документации на автоматизированную систему	
Уметь	– разрабатывать эксплуатационную документацию на систему защиты автоматизированных систем; – анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; – проводить технико-экономическое обоснование и исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности.	5. Составить перечень необходимой документации стадии «Рабочая документация», относящейся к эксплуатационной 6. Составить технологическую инструкцию для системы защиты автоматизированной системы 7. Составить руководство по эксплуатации системы защиты автоматизированной системы 8. Составить программу опытной эксплуатации для системы защиты автоматизированной системы 9. Составить схему организационной структуры управления проектами и определить взаимосвязи основных понятий проектного менеджмента	
Владеть	– методами анализа технической документации информационной инфраструктуры автоматизированной системы; – навыком документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.	9. Составить руководство по эксплуатации комплекса технических средств системы защиты автоматизированной системы 10. На основании технического задания определить требования к составу и содержанию работ по подготовке системы защиты к вводу в действие; 11. Составить инструкцию для администратора безопасности информации автоматизированной системы; 12. Разработать инструкцию по формированию и ведению базы данных (набора данных)	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации			
Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики информационной безопасности организации.	1. Комплект типовых документов по информационной безопасности. 2. Типовые документы для внедрения СУИБ организации. 3. Комплект типовых документов для операторов ПДн: a. Проектная документация; b. Положения и политики; c. Планы; d. Инструкции и регламенты; e. Приказы; f. Акты; g. Журналы; h. Перечни; i. Обязательства и уведомления; j. Согласия субъекта. 4. Комплект типовых документов для управления рисками информационной безопасности. 5. Методика анализа защищенности ИС. 6. Последовательность мероприятий по анализу защищенности. 7. Структура отчета по результатам анализа защищенности. 8. Тестирование системы защиты по методу «черного» и «белого» ящика. 9. Анализ защищенности внешнего периметра корпоративной сети. 10. Анализ защищенности внутренней ИТ-инфраструктуры. 11. Методы предотвращения сетевых атак на периметр сети.	Б1.Б.34Управление информационной безопасностью

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		12. Инструментальные средства анализа защищенности. 13. Основные принципы создания СУИБ. 14. Процедура внедрения СУИБ. 15. Разработка политик ИБ. 16. Разработка профилей защиты и заданий по безопасности. 17. Расследование инцидентов ИБ. 18. Организация режима секретности. 19. Технические политики ИБ на предприятии. 20. Процессный подход для управления ИБ.	
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.	1. Разработать заданную частную политику информационной безопасности. 2. Составить описание информационной инфраструктуры организации. **3.** Выбрать и обосновать меры защиты информационных ресурсов.	
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	Разработать Технические политики (Technical Policy) информационной безопасности на заданном предприятии.	
Знать	- принципы разработки политики информационной безопасности компании/организации; - области действия СУИБ;	Теоретические вопросы: 1. Основные принципы создания СУИБ 2. Эффективное управление политиками безопасности	Б1.В.10 Системы управления информационной безопасностью
Уметь	- разрабатывать частные Политики ИБ; - определять цели и механизмы контроля обработки рисков ИБ и оценки их применимости для конкретного решения;	Задания: 1. Подобрать оптимальную для выбранной корпоративной инфраструктуры СУИБ из имеющихся в данный момент на рынке предложений. Обосновать выбор. 2. Провести анализ конфигураций политик безопасности с целью обеспечения их согласованности для выбранной	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		корпоративной инфраструктуры.	
Владеть	- навыками обучение и повышение осведомленности персонала предприятия/организации в области обеспечения безопасности информации; - навыками документирование процессов управления ИБ (политики, процедуры, записи);	Задания: 1. Смоделировать шаблоны политик безопасности для выбранной корпоративной инфраструктуры с установленными продуктами безопасности Cisco для дальнейшего создания шаблонов политик безопасности.	
Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - принципы формирования политики информационной безопасности организации. - способы контроля эффективности реализации политики информационной безопаности	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.		
Владеть	- навыками разработки политик безопасности различных уровней. - навыками и методами контроля эффективности сформированной политики информационной безопасности		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. 44) Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - принципы формирования политики информационной безопасности организации. - способы контроля эффективности реализации политики информационной безопаности	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.		
Владеть	- навыками разработки политик безопасности различных уровней. - навыками и методами контроля эффективности сформированной политики информационной безопасности		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-23	**способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа**		
Знать	- правила, процедуры, практические приемы для обеспечения информационной безопасности операционных систем - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей ОС;	Перечень вопросов: 1. Классификация уязвимостей ОС, методы их нейтрализации 2. Критерии надежности средств защиты информации (СЗИ) для операционных систем 3. Методы разработки политики безопасности для автоматизированных систем	Б1.Б.23 Безопасность операционных систем
Уметь	- реализовывать политику учетных записей пользователей операционной системы; - сформировать комплекс мер защиты информации ограниченного доступа для операционной системы;	1. Разработать комплекс организационных и технических мер для реализации политики безопасности для операционной системы; 2. Разработать политику внедрения мер, направленных на повышения безопасности информации при эксплуатации ОС	
Владеть	- навыками формальной постановки задачи обеспечения информационной безопасности операционной системы. - навыками эксплуатации операционных систем и программных систем с учетом требований по защиты информации	1. Разработать сценарий администрирования подсистемы безопасности операционных систем семейств Windows и UNIX/Linux 2. Произвести базовые настройки и конфигурирование ОС семейств Windows и UNIX/Linux 3. Разработать сценарий установки и настройки средств	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	ограниченного доступа; - навыками использования программно-аппаратных средств обеспечения информационной безопасности	защиты информации для ОС семейств Windows и UNIX/Linux 4. Используя встроенные средства ОС произвести настройку журнала событий	
Знать	- Характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним; - Основные принципы методик противодействия перехвату и несанкционированному съему информации при ее передаче по каналам связи сетей ЭВМ; - Классификацию и основные принципы действия оборудования и ПО, предназначенного для организации защищенных каналов передачи информации.	Перечень вопросов: 1. Характерные уязвимости, присущие каналами связи различной физической природы (проводные электрические, волоконно-оптические, беспроводные) при передаче информации по ним. 2. Методы перехвата информации при передаче ее по различным каналам связи. 3. Основные принципы действия методик по противодействию перехвату и несанкционированному съему информации при ее передаче по каналам связи. 4. Методы защиты информации (криптографические и некриптографические) при ее передаче по незащищенным каналам связи (каналам связи общего пользования). 5. Классификация и основные принципы действия оборудования и программного обеспечения, предназначенного для организации защищенных каналов передачи информации. 6. Принципы применения средств криптографической защиты информации (СКЗИ) при передаче информации по каналам связи.	Б1.Б.24 Безопасность сетей ЭВМ
Уметь	─ Применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ; ─ Определять основные угрозы безопасности в сетях ЭВМ; ─ Контролировать безотказное функционирование средств защиты информации в сетях ЭВМ; ─ Осуществлять подбор инструментальных и программных средств тестирования систем защиты сетей ЭВМ; ─ Разрабатывать комплекс организационных и технических мероприятий для предотвращения несанкционированного доступа к защищаемой	1. Самостоятельно диагностировать неисправность или аномалию работы сети ЭВМ или канала связи с целью своевременной диагностики сетевой атаки и оперативного ей противодействия. 2. Сделать самостоятельное заключение о возможности или невозможности несанкционированного доступа к информации при данной неисправности сети из сетей общего пользования. 3. Предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к информации в сети ЭВМ со стороны сетей общего пользования. 4. Разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информации в сетях ЭВМ.		
Владеть	─ Методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ; ─ Навыками настройки протоколов безопасности на современном сетевом оборудовании; ─ Приемами определения и классификации сетевых атак; ─ Методологией составления политик сетевой безопасности.	1. Произвести проверку организации системы защиты информации вычислительной сети на соответствие организационно-техническим требованиям по защите информации. 2. Использовать известные методики для определения наличия уязвимостей вычислительной сети и их характера. 3. Произвести фильтрацию трафика вычислительной сети с помощью свободно распространяемых программ-анализаторов WireShark или Ethereal 4. Определить характерные признаки сетевой атаки на основе анализа сетевого трафика	
Знать	Методы формирования требований по защите информации, обрабатываемой в СУБД. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Организационные меры по защите информации, обрабатываемой в СУБД.	Вопросы к экзамену: 1. Процедуры, выполняемые при регистрации пользователя в системе. 2. Перечислить элементы аутентификации. 3. Привести примеры факторов аутентификации. 4. Для чего служит механизм управления доступом? 5. Структура команд APDU. Примеры команд APDU. 6. Для чего необходимы парольные политики? 7. Методы парольной аутентификации. 8. Привести примеры атак на системы данных, в которых используется аутентификация на основе пароля, и способы защиты от них. 9. Привести примеры атак на системы данных, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от них.	Б1.Б.25 Безопасность систем баз данных
Уметь	Использовать методы формирования требований по защите информации, обрабатываемой в СУБД. Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД. Организовывать безопасность АРМ, на которых установлена СУБД.	1. Построить СКУД на базе контактных смарт-карт. 2. Построить СКУД на базе бесконтактных RFID смарт-карт. 3. Построить СКУД на базе биометрических систем. 4. Построить СКУД на базе ключей eToken. 5. Построить СКУД на базе ключей iButton. 6. Настроить систему видеонаблюдения помещения, в котором находиться ОИ.	
Владеть	Методами формирования требований по	1. Обеспечить конфиденциальности и контроль целостности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	защите информации, обрабатываемой в СУБД. Навыками анализа методов формирования требований по защите информации, обрабатываемой в СУБД.	информации в БД с использованием СКЗИ «Крипто БД» по требованиям ИБ. 2. Провести мониторинг и аудит доступа к зашифрованным данным БД.	
Знать	- Методы формирования требований по защите информации ограниченного доступа - Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. - Организационные меры по защите информации ограниченного доступа	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- Использовать методы формирования требований по защите информации ограниченного доступа - Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа		
Владеть	- Методами формирования требований по защите информации ограниченного доступа - Навыками анализа методов формирования требований по защите информации ограниченного доступа		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети?	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Методы формирования требований по защите информации ограниченного доступа - Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. - Организационные меры по защите информации ограниченного доступа	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- Использовать методы формирования требований по защите информации ограниченного доступа - Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа		
Владеть	- Методами формирования требований по защите информации ограниченного доступа - Навыками анализа методов формирования требований по защите информации ограниченного доступа		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	– основные меры по защите информации в автоматизированных системах; – особенности защиты информации в автоматизированных системах управления технологическими процессами; – угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах.	13. Описать технологический процесс обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 14. Проверить выполнение требований по защите информации от утечки за счет ПЭМИ СВТ. 15. Перечислить испытания на соответствие требованиям по ЗИ от НСД. 16. Перечислить требования при создании (модернизации) автоматизированной системы в защищенном исполнении 17. Дать понятие политики информационной безопасности организации	ФТД.02 Разработка эксплуатационной документации на системы защиты информации автоматизированных систем
Уметь	– определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; – Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.	13. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации; 14. Составить инструкцию по антивирусному контролю; 15. Разработать организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам автоматизированной системы; 16. Составить предписание на эксплуатацию СВТ; 17. Составить инструкцию по эксплуатации СЗИ (по выбору) в соответствии с ГОСТ 2.610-2006	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	– методами анализа защищенности информационной инфраструктуры автоматизированной системы; – навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач;	58. Составить инструкцию о мерах по обеспечению информационной безопасности 59. Составить технический паспорт на систему защиты автоматизированной системы с приложениями: a) состав технических и программных средств, входящих в систему защиты АС; b) места установки СЗИ и технических средств; c) параметры и порядок настройки средств защиты информации, программного обеспечения и технических средств.	
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности			
Знать	- методы повышения уровня безопасности программного обеспечения;	1. Управление учетными записями пользователей. 2. Мониторинг процессов и приложений 3. Аудит событий в локальной системе 4. Объекты групповой политики (GPO). Создание. Редактирование. Хранение. 5. Сетевая информационная система NIS (NIS+) и ее конфигурирование. 6. Доступ к удаленным компьютерам 7. Виртуальные частные сети 8. Выбор режима проверки подлинности. 9. Авторизация пользователей. 10. Системные процедуры администрирования учетных записей Windows. 11. Системные процедуры администрирования учетных записей SQL Server.	Б1.В.09 Анализ уязвимостей программного обеспечения
Уметь	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять компоненты программного обеспечения, не обеспечивающие требуемый уровень информационной безопасности;	При помощи утилиты htop определить PID процессов, созданных экземпляром исследуемого ПО. Определить иерархию процессов. Определит права с которыми запущены процессы. Соотнести задачи процессов и предоставленные им права.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Ограничить права процессов при помощи средств ОС.	
Владеть	- навыками определения возможных векторов атаки на программное обеспечение;	Проанализировать конфигурацию программного обеспечения и определить какие параметры конфигурации снижают защищенность ПО.	
Знать	-Технические требования к испытательной лаборатории - Методологией тестирования безопасности информационных технологий	1.Укажите минимальные аппаратные требования к испытательной лаборатории 2.Какие платформы виртуализации мы можем использовать для создания виртуальных машин? 3.Какое дополнительное программное обеспечение потребуется для сборки сервера Metasploitable 3 с нуля? 4. Какой тип анализа безопасности применяется перед вводом в эксплуатацию ИТ ресурсов? 5. Укажите порядок действий при проведении тестирования по стандарту NIST 800-115	Б1.В.ДВ.03.01 Анализ безопасности информационных технологий
Уметь	- развертывать уязвимые информационно-технологических ресурсов автоматизированной системы	1.Создать виртуальную машину Kali Linux 2. Установить Metasploitable 3. 3. Установить apache	
Владеть	-навыками анализа безопасности информационно-технологических ресурсов автоматизированной системы	1. Используя Nmap выполнить сканирование сети с целью определения конфигурации сети. 2. Используя Nmap выполнить сканирование портов виртуальной маши. 3. Используя Nmap определить установленное сетевое ПО на виртуальной машине	
Знать	-основные понятия предметной области построения систем организационного управления – основные критерии оценки защищенности систем организационного управления, источники угроз и нормативные документы в области защиты информации -основные информационные технологии, используемые в автоматизированных системах;	Теоретические вопросы к экзамену: 1. Понятие Система организационного управления, ее виды и характерные отличия. 2. Показатели надежности системы ОУ 3. Организационные меры по обеспечению безопасности информации при работе персонала с системой ОУ 4. Предотвращение преднамеренных или непреднамеренных помех правильной работы системы управления технологическими	Б1.В.ДВ.03.02 Информационная безопасность систем организационного управления

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	передовой опыт по внедрению современных организационно-технических мер, средств и способов защиты информации с целью повышения их эффективности	процессами предприятия 5. Необходимость защиты информации на предприятии 6. Угрозы безопасности информации СОУ 7. Аудит системы информационной безопасности предприятия 8. Организация системы информационной безопасности предприятия	
Уметь	-применять современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем организационного управления - моделировать потоки информации и документооборот, в корпоративных информационных системах и осуществлять их оценивание с точки зрения информационной безопасности -разрабатывать эксплуатационную документацию для систем организационного управления с учетом требований информационной безопасности	1. В автоматизированной системе управления технологическими процессами предприятия определить оборудование с ЧПУ и АРМы являющиеся критически важными и подлежащими защите. 2. В автоматизированной системе организационного управления предприятия определить потоки информации конфиденциального характера.	
Владеть	-навыками применения современных информационных технологий с учетом требований информационной безопасности в системах организационного управления (ОУ) -навыками подготовки инструкций по эксплуатации систем организационного управления с учетом требований информационной безопасности	1. Провести анализ защищенности автоматизированной системы управления технологическими процессами; 2. Разработать инструкции для персонала различных уровней доступа по эксплуатации систем организационного управления с учетом требований информационной безопасности.	
Знать	-Информационно-технологические ресурсы автоматизированных систем -Базовые правила построения виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований	Перечень вопросов: 1. Информационно-технологические ресурсы автоматизированных систем. Состав и назначение. 2. Уязвимости информационно-технологических ресурсов автоматизированных систем 3. Информационно-коммуникационные технологии в	Б1.В.ДВ.04.01 Виртуальные сети

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной безопасности	информационно-технологические ресурсы автоматизированных систем. Обеспечение требований информационной безопасности. 4.Протокол заголовка идентификации AH. Обеспечение целостности защищенной части пакета данных 5. Инкапсулирующий протокол безопасности ESP. Режим транспорта и инкапсуляции 6. IKE протокол. Обмен ключами между узлами VPN 7. Способ идентификации узла в виртуальных частных сетях 8. Организация VPN-туннеля и его шифрование 9. Криптографические карты общедоступных интерфейсов 10. Организация работы динамического VPN сервера 11. Применение виртуализации в частных сетях для обеспечения защиты информации ограниченного доступа 12. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика для обеспечения защиты информации ограниченного доступа? 13. Ключевые аспекты построения набора правил межсетевого экрана 14. Система обнаружения и предотвращения вторжений IDS/IPS. 15. Основные варианты организации виртуальных частных сетей 16. Протоколы формирования каналов для защиты информации ограниченного доступа передаваемой по сети 17. Согласование параметров защищенных каналов и распределение криптографических ключей	
Уметь	- Создавать виртуальные сети для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности -Конфигурировать сетевое оборудование в соответствии с проектом виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	1.Выполнить конфигурирование VPN концентратора для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности 2.Определить настройки ACL в соответствии с поставленной задачей для виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах . 3. Создать виртуальную сеть с применением динамического VPN сервера, учитывая требования информационной безопасности 4. Произвести анализ сети программными сканерами сетевых протоколов и сетевых уязвимостей (например, свободно распространяемые сканеры WireShark и Ethereal)	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		5. Настроить протокол обмена ключами для установки автоматического VPN соединения в виртуальных сетях обеспечивающих эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом	
Владеть	-Информационно-технологические ресурсы автоматизированных систем -Базовые правила построения виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Перечень вопросов: 1. Информационно-технологические ресурсы автоматизированных систем. Состав и назначение. 2. Уязвимости информационно-технологических ресурсов автоматизированных систем 3. Информационно-коммуникационные технологии в информационно-технологические ресурсы автоматизированных систем. Обеспечение требований информационной безопасности. 4.Протокол заголовка идентификации AH. Обеспечение целостности защищенной части пакета данных 5. Инкапсулирующий протокол безопасности ESP. Режим транспорта и инкапсуляции 6. IKE протокол. Обмен ключами между узлами VPN 7. Способ идентификации узла в виртуальных частных сетях 8. Организация VPN-туннеля и его шифрование 9. Криптографические карты общедоступных интерфейсов 10. Организация работы динамического VPN сервера 11. Применение виртуализации в частных сетях для обеспечения защиты информации ограниченного доступа 12. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика для обеспечения защиты информации ограниченного доступа? 13. Ключевые аспекты построения набора правил межсетевого экрана 14. Система обнаружения и предотвращения вторжений IDS/IPS. 15. Основные варианты организации виртуальных частных сетей 16. Протоколы формирования каналов для защиты информации ограниченного доступа передаваемой по сети 17. Согласование параметров защищенных каналов и распределение криптографических ключей	
Знать	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам	1. Управление учетными записями пользователей. 2. Мониторинг процессов и приложений	Б1.В.ДВ.05.01 Методы

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	автоматизированной системы;	3. Аудит событий в локальной системе 4. Объекты групповой политики (GPO). Создание. Редактирование. Хранение. 5. Сетевая информационная система NIS (NIS+) и ее конфигурирование. 6. Доступ к удаленным компьютерам 7. Виртуальные частные сети 8. Выбор режима проверки подлинности. 9. Авторизация пользователей. 10. Системные процедуры администрирования учетных записей Windows. 11. Системные процедуры администрирования учетных записей SQL Server.	мониторинга информационной безопасности АС
Уметь	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;	1. На виртуальной машине по управление ОС Linux настроить iptable. 2. Настроить шаблон по которому весь трафик с заданного IP проходящий через порт 23 будет записан в файл. 3. При помощи утилиты Metasploit выполнить анализ узлов сети.	
Владеть	- навыками определения возможных векторов атаки на автоматизированную систему;	Проанализировать конфигурацию узла автоматизированной системы и определить какие параметры конфигурации узла снижают его защищенность.	
Знать	- основные понятия предметной области систем электронного документооборота -основные информационные технологии, используемые в автоматизированных системах; − принципы построения и функционирования, примеры реализаций систем электронного документооборота; нормативные правовые акты в области защиты информации	1. Теоретические вопросы к экзамену: 2. Принципы построения и функционирования СЭД 3. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. 4. ГОСТ Р ИСО 7498-2-99 Государственный стандарт Российской Федерации Информационная технология взаимосвязь открытых систем базовая эталонная модель 5. ГОСТ Р 51241-98 Средства и системы контроля и управления доустпом. Классификация. Общие технические требования. Методы испытаний. 6. ГОСТ Р 50.1.053- 2005 Информационные технологии, основные термины и определения в области технической защиты информации 7. Классификация угроз безопасности информации	Б1.В.ДВ.05.02 Защита электронного документооборота

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		8. Источники угроз ЭД 9. Каналы утечки информации 10. Надежное хранение электронной документации 11. Рекомендации для долговременного хранения документов в электронном виде 12. Современные ECM системы электронного документооборота 13. Использование docflow-систем для хранения, поиска и маршрутизацию документов 14. Безопасность информации при осуществлении документооборота 15. Особенности защиты информации, составляющей коммерческую тайну компании.	
Уметь	-применять современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем электронного документооборота - моделировать потоки информации и документов, в корпоративных информационных системах и осуществлять их оценивание с точки зрения информационной безопасности -готовить научно-технические отчеты, обзоры, публикации по теме предметной области - готовить научно-технические отчеты, обзоры, публикации по теме предметной области	1. Составить обзор современного состояния российского рынка ECM систем электронного документооборота. Провести анализ встроенных средств защиты информации от несанкционированного доступа и искажений. 2. По описанию информационных ресурсов предприятия составить правила доступа ко всем информационным ресурсам организации, ранжирование систем доступа применительно к аппаратному обеспечению программных средств, базам данных.	
Владеть	-навыками применения современных информационных технологий для поиска, прохождения, обработки, учета и рассылки документов внутри систем электронного документооборота -навыками моделирования потоков информации и документооборота, в корпоративных информационных системах и построения моделей угроз ИБ	Провести классификацию информационных ресурсов выбранного предприятия; - составить модель потенциального злоумышленника; - провести анализ уязвимостей; - провести идентификацию и оценку угроз нарушения информационной безопасности; - оценить уровень рисков нарушения информационной безопасности.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Знать	- понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; - общие требования по обеспечения безопасности значимых объектов КИИ; - подходы категорирования значимости объектов КИИ;	Теоретические вопросы: 1. Требования к созданию систем безопасности значимых объектов КИИ РФ. 2. Обеспечение функционирования систем безопасности значимых объектов КИИ РФ. 3. Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ. 4. Правила и порядок категорирования объектов КИИ. 5. Реестр значимых объектов КИИ. 6. Правила формирования комиссии по категорирования объектов КИИ.	Б1.В.11 Обеспечение информационной безопасности критической информационной инфраструктурой
Уметь	- определять категории значимых объектов КИИ и оформлять полученные результаты; - определять структуру системы безопасности значимого объекта КИИ; - определят требования по обеспечения безопасности значимых объектов КИИ; - определять требования к параметрам настройки программных и программно-аппаратных средств защиты информации (СЗИ);	Задания: 1. Для выбранного предприятия/организации определить перечень объектов КИИ с обоснованием. 2. Для выбранного предприятия/организации сформировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения одной из таких категорий. 3. Для выбранного объекта КИИ сформировать требования к параметрам настройки программных и программно-аппаратных СЗИ.	
Владеть	- навыками установки и настройки СЗИ, обрабатываемой объектами КИИ; - навыками подбора средств СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ;	Задания: 1. Провести тестирование работоспособности СЗИ «Страж NT» с учетом сформированных требований к объекту КИИ. 2. Для выбранного объекта КИИ сформировать перечень необходимых программных и программно-аппаратных СЗИ с учетом их стоимости.	
Знать	методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;	*перечень вопросов на защите отчета НИР:* 1. Какая научно-исследовательская задача решалась в ходе выполнения НИР? 2. Какие методы исследования применялись при выполнении НИР? 3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки	Б2.Б.02(Н) Научно-исследовательская работа
Уметь	выполнять работы по оптимизации схем управления автоматизированной системой; - применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	ресурсов автоматизированной системы выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;	и техники в РФ? 4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований? 5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований? 6. Укажите области применения предложенной Вами разработки? 7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ? 8. Какими способами осуществлялась проверка достоверности полученных результатов? 9. Какие инновационные решения были разработаны в ходе выполнения НИР? Какие охранные документы были получены в ходе выполнения НИР?	
Владеть	навыками определения возможных векторов атаки на автоматизированную систему; и осуществлять выбор средств защиты информации		
Знать	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень защиты информации		
Владеть	- навыками определения возможных векторов атаки на автоматизированную систему и осуществлять выбор средств защиты информации;		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень защиты информации		
Владеть	- навыками определения возможных векторов атаки на автоматизированную систему и осуществлять выбор средств защиты информации;		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций			
Знать	- иметь представление об основных средствах защиты ОС в составе информационно-технологических ресурсов автоматизированной системы; - критерии защищенности ОС и сети ЭВМ; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	Перечень вопрос: 1. Принципы функционирования средств защиты информации при их эксплуатации в составе информационных систем 2. Современные технологии построения средств и систем защиты информации и их применение в составе систем защиты автоматизированных систем и сетей ЭВМ 3. Дискреционная и мандатная модели подсистем безопасности 4. Дать определение понятиям «политика безопасности», «контекст безопасности», «бюджет безопасности»	Б1.Б.23 Безопасность операционных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - проводить мониторинг угроз безопасности операционных систем - обеспечивать защиту сетевых подключений средствами операционной системы;	1. Произвести средствами мониторинга анализ уязвимостей операционной системы 2. Разработать методику нейтрализации обнаруженных уязвимостей операционных систем 3. Настроить администрирование подсистемы информационной безопасности автоматизированных систем; 4. Обосновать принимаемые меры по устранению неисправностей ОС;	
Владеть	- профессиональной терминологией в области информационной безопасности; - навыками работы с конкретными программными и аппаратными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС; - навыками конфигурирования встроенных средств защиты информации ОС; - навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;	1. Произвести настройку встроенных средств защиты информации ОС, предназначенных для нейтрализации угрозы типа «недоверенная загрузка» 2. Произвести настройку встроенных средств защиты информации ОС, предназначенных для нейтрализации угрозы типа «несанкционированный доступ»	
Знать	Принципы работы баз данных. Основные средства обеспечения безопасности данных. Принципы администрирования баз данных. Средства обеспечения безопасности данных. Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных.	Вопросы к экзамену: 10. Описать принципы работы биометрических систем. 11. Описать принцип работы OTP-токена. 12. Способы аутентификации пользователя при использовании OTP-токена. 13. Привести примеры атак на системы данных, использующие аутентификацию с помощью OTP-токенов, и способы защиты от них. 14. Применение криптографии с открытым ключом для шифрования сообщения. 15. ЭЦП. Примеры использования. 16. Реализуемые алгоритмы криптографического	Б1.Б.25 Безопасность систем баз данных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		преобразования в СКЗИ «Крипто БД». 17. Архитектура СКЗИ «Крипто БД». 18. Этапы эксплуатации СКЗИ «Крипто БД» и задачи, выполняемые на каждом этапе.	
Уметь	Анализировать работоспособность базы данных. Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД. Самостоятельно применять средства обеспечения безопасности данных. Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций. Организовывать безопасность систем баз данных.	1. Провести анализ инцидентов безопасности с использованием СКЗИ «Крипто БД». 2. Настроить СКЗИ «Крипто БД».	
Владеть	Основными средствами обеспечения безопасности данных. Навыками работы с нормативными документами по администрированию баз данных. Средствами обеспечения безопасности данных. Навыками разработки и администрирования базы данных. Навыками организации безопасности систем баз данных. Средствами обеспечения безопасности данных и АИС.	1. Для сервера базы данных и для каждого пользователя, включая администраторов безопасности, создать по одной ключевой паре (открытый и закрытый ключи) с использованием СКЗИ «Крипто БД». 2. Настроить доступ Администраторов СУБД к хранящейся в базе информации согласно матрице доступа с использованием СКЗИ «Крипто БД».	
Знать:	-требования к организационным и техническим мерам для обеспечения безопасности значимых объектов КИИ; - основные принципы организации государственного контроля состояния защищенности значимых объектов КИИ; - процедуру категорирования объектов КИИ; - требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования;	Теоретические вопросы: 1. Понятие ГосСОПКА 2. Понятие СОБИ КСИИ 3. Основные подсистемы СОБИ КСИИ 4. Этапы разработки СОБИ КИИ 5. Требования к организационным и техническим мерам для обеспечения безопасности объектов КИИ 6. Ответственность за нарушение законодательства в области обеспечения безопасности КИИ РФ.	Б1.В.11 Обеспечение информационной безопасности критической информационной инфраструктурой

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь:	- осуществлять выбор СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ; - определять СЗИ для реализации технических мер обеспечения безопасности информации в рамках системы безопасности значимого объекта КИИ;	Задания: 1. Для выбранного объекта КИИ сформировать перечень необходимых технических СЗИ с учетом их стоимости и категории значимости объекта КИИ. 2. Проанализировать этапы жизненного цикла системы безопасности значимого объекта КИИ и выявить слабые места.	
Владеть:	- навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; - навыками разработки организационно-распорядительными документов по безопасности значимых объектов КИИ; - навыками проведения работ по контролю состояния безопасности объектов КИИ;	Задания: 1. Составить майнд-карту мероприятий по реагированию на компьютерные инцинденты для выбранного значимого объекта КИИ в ходе его эксплуатации. 2. Разработать необходимые документы для обеспечения функционирования выбранного значимого объекта КИИ в рамках созданной системы безопасности.	
Знать	- Принципы администрирования баз данных. Средства обеспечения безопасности данных. - Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- Анализировать работоспособность базы данных. - Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД. - Самостоятельно применять средства обеспечения безопасности данных. - Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций. - Организовывать безопасность систем баз данных - Выявлять инциденты и реагировать на них - Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Владеть	- Основными средствами обеспечения безопасности данных. - Навыками работы с нормативными документами по администрированию баз данных. - Средствами обеспечения безопасности данных. - Навыками разработки и администрирования базы данных. - Навыками организации безопасности систем баз данных. - Средствами обеспечения безопасности данных и АИС. - Навыками сопровождения функционирования системы защиты информации информационной системы в ходе ее эксплуатации - Навыками анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	- Принципы администрирования баз данных. Средства обеспечения безопасности данных. - Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	- Анализировать работоспособность базы данных. - Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД. - Самостоятельно применять средства обеспечения безопасности данных. - Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций. - Организовывать безопасность систем баз данных		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- Выявлять инциденты и реагировать на них - Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации	информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации?	
Владеть	- Основными средствами обеспечения безопасности данных. - Навыками работы с нормативными документами по администрированию баз данных. - Средствами обеспечения безопасности данных. - Навыками разработки и администрирования базы данных. - Навыками организации безопасности систем баз данных. - Средствами обеспечения безопасности данных и АИС. - Навыками сопровождения функционирования системы защиты информации информационной системы в ходе ее эксплуатации - Навыками анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-26	**способностью администрировать подсистему информационной безопасности автоматизированной системы**		
Знать	─ Основные принципы работы системы обнаружения вторжений; ─ Основные подсистемы системы обнаружения вторжений;	Теоретические вопросы: 1. Использование условной вероятности. 2. Экспертные системы. 3. Методы, основанные на моделировании поведения злоумышленника. 4. Механизм функционирования системы обнаружения атак на уровне сети	Б1.В.04 Методы выявления нарушений информационной безопасности
Уметь	─ Управлять инцидентами ИБ; ─ Администрировать систему выявления нарушений информационной безопасности.	1. Написать алгоритм администрирования выбранной системы выявления нарушений информационной безопасности в виде майнд-карты с учетом требований безопасности информации.	
Владеть	─ Навыками работы с системой выявления нарушений информационной безопасности;	**Задание:** 5. Произвести фильтрацию трафика сети с помощью свободно	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	─ Навыками работы с подсистемами системы выявления нарушений информационной безопасности;	распространяемых утилит.	
Знать	─ Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; ─ Принципы администрирования системы информационной безопасности автоматизированной системы.	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	─ Настраивать систему информационной безопасности автоматизированной системы; ─ Настраивать подсистемы системы информационной безопасности автоматизированной системы; ─ Самостоятельно администрировать систему информационной безопасности автоматизированной системы.		
Владеть	─ Навыками работы с системой информационной безопасности автоматизированной системы; ─ Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; ─ Навыками администрирования системы информационной безопасности автоматизированной системы.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
Знать	─ Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; ─ Принципы администрирования системы информационной безопасности автоматизированной системы.	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	─ Настраивать систему информационной безопасности автоматизированной системы; ─ Настраивать подсистемы системы информационной безопасности автоматизированной системы; ─ Самостоятельно администрировать систему информационной безопасности автоматизированной системы.		
Владеть	─ Навыками работы с системой информационной безопасности автоматизированной системы; ─ Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; ─ Навыками администрирования системы информационной безопасности автоматизированной системы.		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы			
Знать	Принципы построения современных защищенных распределенных АС. Способы разработки политики безопасности распределенных ИС. Нормативные документы по стандартизации и сертификации программной защиты. Способы управления разработкой политики безопасности распределенных ИС. Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.	Вопросы к экзамену: 1. Математические методы оценки эффективности гипотетической СЗИ. 2. Методика выбора контрмер, обеспечивающих ИБ объекта. 3. Методика выбор варианта ЗИ, в наибольшей степени удовлетворяющий заказчика. 4. Методика CRAMM. 5. Стандарты, используемые при проведении аудита безопасности ИС.	Б1.Б.36Информационная безопасность распределенных информационных систем
Уметь	Разрабатывать частные политики безопасности распределенных ИС. Проводить мониторинг и аудит защищенности информационно-технологических ресурсов распределенных	1. Разработайте частную политику безопасности для выбранного предприятия. 2. Сформируйте совокупность вариантов построения СЗИ, которые характеризуются различными значениями показателей эффективности.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	ИС. Руководить разработкой и реализацией частных политики безопасности РИС. Осуществлять мониторинг и аудит безопасности АС.	3. Составьте перечень детальной информация о структуре ИС необходимой для аудита выбранного предприятия.	
Владеть	Методиками анализа политики безопасности РИС. Методиками разработки политики безопасности РИС. Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС. Методиками руководства разработкой политики безопасности РИС. Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС.	1. Сформируйте совокупность правовых, организационных и инженерно-технических мероприятий, для формирования частной политики безопасности выбранного предприятия. 2. Проведите анализ данных аудита выбранного предприятия, используя подход основанный на использовании стандартов ИБ. 3. Сформируйте примерную структуры аудиторского отчета по результатам анализа рисков, связанных с осуществлением угроз безопасности в отношении обследуемой ИС.	
Знать	– способы обработки исключительных ситуаций; современные технологии и методы программирования, предназначенные для создания прикладных программ; – Нормативные документы по стандартизации и сертификации программной защиты. – Цели и задачи разработки политики информационной безопасности – Методы и средства анализа достаточности мер по обеспечению ИБ ПО	1. Аудит баз данных и его виды: стандартный, на основе значений, детализированный 2. Аудит администратора БД. 3. Обслуживание журнала аудита. 4. Обновления системы безопасности 5. Обслуживание базы данных Оптимизаторы БД. 6. Сбор статистики оптимизатора и управление ею. 7. Автоматический репозиторий рабочей нагрузки и управление им. 8. Монитор автоматической диагностики баз данных. 9. Диспетчер и консультанты БД. 10. Автоматические задачи обслуживания. 11. Предупреждения сервера, их типы и реагирование на них.	Б1.В.ДВ.04.02 Защита программного обеспечения

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
Уметь	– Разрабатывать порядок эксплуатации программного обеспечения – Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения – Проводить мониторинг и аудит защищенности ПО	1. Провести анализ защищенности исходного кода ПО 2. Провести анализ защищенности ПО от дизассемблирования 3. Разработать частную политику для реализуемой БД 4. Провести детализованный аудит БД 5. Провести аудит транзакций реализуемой БД 6. Провести анализ разграничения доступа пользователей БД	
Владеть	– Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО – Методами контроля соблюдения политики учетных записей – Навыками регламентации обслуживания и осуществления модификации программного обеспечения	1. Разработать частную политику администрирования реализуемой БД 2. Провести анализ разграничения доступа пользователей БД 3. Провести анализ сбора данных транзакций БД используя встроенные средства СУБД 4. Используя встроенные средства Windows провести анализ исходного кода ПО 5. Используя встроенные утилиты администрирования Windows провести анализ событий по указанному программному обеспечению	
Знать	– Способы обработки исключительных ситуаций – Нормативные документы по стандартизации и сертификации программной защиты. – Цели и задачи разработки политики информационной безопасности – Методы и средства анализа достаточности мер по обеспечению ИБ ПО –Порядок контроля (мониторинга) за обеспечением уровня защищенности информации	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Разрабатывать порядок эксплуатации программного обеспечения – Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения – Проводить мониторинг и аудит защищенности ПО –Осуществлять контроль за событиями безопасности и действиями пользователей в		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной системе	информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации?	
Владеть	─ Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО ─ Методами контроля соблюдения политики учетных записей ─ Навыками регламентации обслуживания и осуществления модификации программного обеспечения		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. Раскрыть особенности образования электромагнитных каналов утечки информации.	
Знать	─ Способы обработки исключительных ситуаций ─ Нормативные документы по стандартизации и сертификации программной защиты. ─ Цели и задачи разработки политики информационной безопасности ─ Методы и средства анализа достаточности мер по обеспечению ИБ ПО ─Порядок контроля (мониторинга) за обеспечением уровня защищенности информации	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	─ Разрабатывать порядок эксплуатации программного обеспечения ─ Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения ─ Проводить мониторинг и аудит защищенности ПО ─Осуществлять контроль за событиями безопасности и действиями пользователей в		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационной системе	– изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц	
Владеть	Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО – Методами контроля соблюдения политики учетных записей – Навыками регламентации обслуживания и осуществления модификации программного обеспечения		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации. 43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	
ПК-28	**способностью управлять информационной безопасностью автоматизированной системы**		
Знать	- основные угрозы безопасности информации и модели нарушителя в ИС; - основные меры по ЗИ в АС.	1. Назовите основные угрозы безопасности информации. 2. Дайте описание внешнего нарушителя. 3. Кто относится к внутренним нарушителям. 4. На какие группы разделяют инциденты ИБ.	Б1.Б.34Управление информационной безопасностью
Уметь	- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - расследовать инциденты ИБ.	**1.** Описать процесс расследования инцидента **2.** Составить заключение по проведенному расследованию. **3.** Подготовить типовой комплект документов СУИБ.	
Владеть	- навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС; - терминологией и процессным подходом	Разработать Профиль защиты для автоматизированной банковской системы	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	построения СУИБ.		
Знать	- отечественные и международные стандарты по информационной безопасности; - требования в области ИБ для создания, развития и поддержания системы менеджмента информационной безопасности (СМИБ)	Теоретические вопросы: 1. Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования.» 2. Требования к аудиту ИБ. Международные стандарты. Нормативные документы РФ. Практика регуляторов. 3. Усиление защиты домена через групповые политики в соответствии с рекомендациями SCM.	Б1.В.10 Системы управления информационной безопасностью
Уметь	- разрабатывать техническое задание на проектирование СУИБ с учетом выявленных рисков ИБ - выбирать и анализировать технические решения для СУИБ;	Задания: 1. Выбрать и проанализировать необходимые компоненты для защиты корпоративной инфраструктуры (IDS/IPS, Firewall, AV, Monitoring) 2. Разработать ТЗ на проектирование СУИБ для выбранной корпоративной инфраструктуры.	
Владеть	- навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям международных стандартов; - навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям стандартов и законодательства РФ;	Задания: 1. Проанализировать методики, документацию, инструменты и технологии в области безопасности веб – приложений на Project Application Security Open Web (OWASP). 2. Проанализировать существующие облачные платформы для использования в выбранной корпоративной инфраструктуре с учетом ее особенностей и требованиям обеспечения безопасности.	
	- принцы получения OSINT информации	1. Перечислите источники для получения OSINT информации. 2. При помощи какой утилиты возможно получить информацию о домене DNS. 3. Укажите специализированное ПО необходимое для получения OSINT информации в автоматизированном режиме.	Б1.В.ДВ.03.01 Анализ безопасности информационных технологий
	- выполнять тестирование автоматизированной системы с целью получения OSINT информации.	1. Выполнить сканирование заданного сайта при помощи Deepmagic Information Gathering Tool. 2. Получить информацию о целевом домене при помощи host и dig 3. Выполнить сканирование заданного сайта при помощиMaltego.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	- навыками формирования отчета о текущем уровни безопасности автоматизированной системы	1. Укажите основные типы отчетов. 2. Перечислите основные пункты общего отчета. 3. При помощи Dradis выполнить тестирование безопасности по методологии OWASP и сгенерировать автоматический отчет.	
Знать	-методы и средства контроля охраняемых сведений - программные средства, поддерживающие управление информационной безопасностью -отечественный и зарубежный опыт в области управления информационной безопасностью	Теоретические вопросы: 1. Цели и задачи организационной защиты информации. 2. Основные направления организационной защиты на объекте. 3. Структура сил и средств организационной защиты информации. 4. Принципы организации службы безопасности объекта. 5. Типовая структура службы безопасности. 6. Основные документы, регламентирующие деятельность службы безопасности. 7. Требования к сотрудникам организации, допущенным к секретной (конфиденциальной) информации. 8. Основные критерии приема на работу, связанную с сохранением тайны. 9. Проверки сотрудников, принимаемых на работу, связанную с сохранением тайны. 10. Организация работы с персоналом предприятия 11. Подбор и подготовка сотрудников отдела информационной безопасности 12. Правовые вопросы организации защиты информации	Б1.В.ДВ.03.02 Информационная безопасность систем организационного управления
Уметь	-разрабатывать политики безопасности для элементов системы ОУ -расследовать инциденты ИБ -разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ -готовить предложения для актуализации организационных мер по защите информационных систем ОУ	1. На примере отдела управления персоналом предприятия определить состав информационной системы. Составить схему информационных потоков. Определить входные и выходные данные системы управления. Определить основные угрозы в соответствии с техническими характеристиками сетевой инфраструктуры.	
Владеть	-терминологией и процессным подходом построения СУИБ. -навыками определения актуальных угроз и применения мер их нейтрализации	1. Для АСУ по варианту определить актуальные угрозы ИБ, оценить текущее состояние ИБ ИС, 2. Разработать предложения по совершенствованию системы управления информационной безопасностью	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		автоматизированной системы.	
Знать	-нормативные акты, используемые при разработке политики информационной безопасностью организации; – основные критерии оценки защищенности систем электронного документооборота, источники угроз методические рекомендации отраслевых регуляторов по обеспечению информационной безопасности	Теоретические вопросы к экзамену: 1. Стандарты информационной безопасности и методическое обеспечение ГОСТ Р ИСО/МЭК 15408 2. Стандарты ISO/IEC 27001-2005 3. Стандарты ISO/IEC 17799-2005 4. Стандарты ISO/IEC TR 13335. 5. Средства обнаружения атак и защиты программного обеспечения 6. Безопасность систем электронной почты 7. Безопасность корпоративной информации при использовании средств связи и различных коммуникаций 8. Защита от съема информации электронными средствами 9. Организационные меры защиты информации на предприятии 10. Методики обоснования выбора средств технической и криптографической защиты информации. 11. Выбор, установка, настройка и эксплуатация средств антивирусной защиты.	Б1.В.ДВ.05.02 Защита электронного документооборота
Уметь	- проводить сбор и анализ данных о состоянии защиты информации в организации; оценку рисков ИБ; применять государственные стандарты и методические рекомендации для построения СЗИ организации разрабатывать политики информационной безопасности для систем электронного документооборота	В консоли администратора dlp- системы настроить перечни контролируемых мессенджеров, браузеров, облачных хранилищ контроль файлов, передаваемых по протоколам FTP, FTPS, HTTP и HTTPSB профилях пользователей Указать два способа настройки перехвата. Преимущества и недостатки каждого способа. На каком этапе необходимо определиться со способом перехвата данных с контролируемых рабочих станций.	
Владеть	- навыками разработки политик информационной безопасности для систем электронного документооборота -методами моделирования потоков информации, документооборота АИС - навыками анализа данных о состоянии систем защиты информации в организации; оценки	Настроить менеджер словарей в консоли администратора. Как учесть при настройке словаря все морфологические словоформы. Методы настройки словаря для уменьшения количества ложных срабатываний. Каким образом влияют ли агенты dlp- системы на производительность рабочих станций, на которые они установлены.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
	информационных оценки рисков;		
Знать	-методы и средства контроля охраняемых сведений - программные средства, поддерживающие управление информационной безопасностью -отечественный и зарубежный опыт в области управления информационной безопасностью - основные принципы создания системы управления информационной безопасностью	**индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований;	Б2.Б.03(П) Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-разрабатывать политики безопасности для элементов системы ОУ -расследовать инциденты ИБ -разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ -готовить предложения для актуализации организационных мер по защите информационных систем - разрабатывать профили защиты		
Владеть	- терминологией и процессным подходом построения СУИБ. -навыками определения актуальных угроз и применения мер их нейтрализации - навыками составления технических политик безопасности		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		– изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		предприятия? 14) Какие операционные системы используются на ПК персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		28) Ответственность за нарушение законодательства в информационной сфере. 29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		Раскрыть особенности образования электромагнитных каналов утечки информации.	
Знать	-методы и средства контроля охраняемых сведений - программные средства, поддерживающие управление информационной безопасностью -отечественный и зарубежный опыт в области управления информационной безопасностью - основные принципы создания системы управления информационной безопасностью	**индивидуальное задание на производственную преддипломную практику:** *Цель прохождения практики:* – закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; – изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; – изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. *Задачи практики:* – ознакомиться с нормативно-правовой документацией организации; – изучить структуру организации; – изучить и провести анализ должностных инструкций сотрудников организации; – изучить и провести анализ решений по обеспечению ИБ предприятия; – изучить и провести анализ методов контроля за исполнением принятых решений; – проведение статистических исследований; – изучение комплексного применения методов	Б2.Б.04(Пд) Производственная-преддипломная практика
Уметь	-разрабатывать политики безопасности для элементов системы ОУ -расследовать инциденты ИБ -разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ -готовить предложения для актуализации организационных мер по защите информационных систем - разрабатывать профили защиты		
Владеть	- терминологией и процессным подходом построения СУИБ. -навыками определения актуальных угроз и применения мер их нейтрализации - навыками составления технических политик безопасности		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		и средств обеспечения информационной безопасности объекта защиты; *Вопросы, подлежащие изучению:* 1) Род деятельности предприятия, на котором проходила практика. 2) Какие способы защиты информации используются на предприятии? 3) Какие программные средства используются для обеспечения информационной безопасности на предприятии? 4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности? 5) Какая топология используется в локальных сетях на предприятии? 6) Как обеспечивается безопасность беспроводных сетей? 7) Как обеспечивается безопасность по виброакустическим каналам передачи информации? 8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии. 9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей. 10) Опишите способы контроля трафика по локальным сетям предприятия. 11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть. 12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети? 13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия? 14) Какие операционные системы используются на ПК	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		персонала предприятия? 15) Какие операционные системы используются на серверах предприятия? 16) Понятие и виды защищаемой информации по законодательству РФ. 17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки. 18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну. 19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности. 20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации. 21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации. 22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права. 23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации). 24) Основное содержание разработки Политики безопасности предприятия (организации). 25) Принципы, основные задачи и функции обеспечения информационной безопасности. 26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации. 27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну. 28) Ответственность за нарушение законодательства в информационной сфере.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		29) Основные мероприятия по защите информации при проведении совещаний и переговоров. 30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных). 31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников. 32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП). 33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации. 34) Сформулировать основные правила безопасной работы в компьютерной системе. 35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД. 36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты. 37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам. 38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения. 39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики. 40) Рассмотреть особенности разграничения доступа и аудита в СЗИ 41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа. 42) Раскрыть особенности образования электромагнитных каналов утечки информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Оценочные средства*	*Структурный элемент образовательной программы*
		43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации. Сформулировать основные особенности построения периметровой охраны особо важных объектов	