Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института энергетики и
автоматизированных систем
_____ С.И. Лукьянов
«27» сентября 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки
09.03.03 Прикладная информатика

Направленность программы
Информационные системы и технологии в управлении ИТ-проектами

Уровень высшего образования – бакалавриат

Программа подготовки – академический бакалавриат

Форма обучения
Очная

Институт	Энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	3
Семестр	6

Магнитогорск
2017 г.

Рабочая программа составлена на основе ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом МОиН РФ от № 207 от 12.03.2015 для профиля «Информационные системы и технологии в управлении ИТ-проектами»

Рабочая программа рассмотрена и одобрена на заседании кафедры Бизнес информатики и информационных технологий «21» сентября 2017 г., протокол № 2.

Зав. кафедрой _____ / Г.Н. Чусавитина/

Рабочая программа одобрена методической комиссией института Энергетики и автоматизированных систем «27» сентября 2017 г., протокол № 2.

Председатель _____ / С.И. Лукьянов/

Рабочая программа составлена: доцентом кафедры БИ и ИТ, кандидатом педагогических наук, доцентом

_____ Е.В. Черновой

Рецензент: начальник бюро разработки тренажеров металлургии и машиностроении отдела обучающих систем SIKE. Корпоративные системы

_____ / А.Е. Соченко/

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата. № протокола заседания кафедры	Подпись зав. кафедрой
1	3,4,7,8,9	Корректировка РПД в соответствии с новым макетом (распоряжение № 10-39/75 от 21.09.2018 «О формировании и актуализации образовательных программ). Актуализация информационно-методического и информационного обеспечения дисциплины. Актуализация материально-технического обеспечения дисциплины	25.09.18, протокол № 2	
2	8,9	О формировании и актуализации образовательных программ. Актуализация информационно-методического и информационного обеспечения дисциплины. Актуализация материально-технического обеспечения дисциплины	02.09.19, протокол № 1	
3	8	Актуализация учебно-методического и информационного обеспечения дисциплины	31.08.20, протокол №1	

1 Цели освоения дисциплины

Цель освоения дисциплины «Информационная безопасность»: овладение бакалаврами основными методами и средствами по обеспечению информационной безопасности в организациях и на предприятиях различных сфер деятельности и форм собственности, основываясь на нормативно-правовых документах, международных и отечественных стандартах в области информационных систем и технологий, на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

2 Место дисциплины в структуре образовательной программы подготовки бакалавра

Дисциплина «Информационная безопасность» входит в вариативную часть блока 1 образовательной программы по направлению 09.03.03 Прикладная информатика.

Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения, полученных студентами в процессе изучения дисциплин «Информатика» «Прикладное программирование», «Алгоритмы на сетях и графах», «Архитектура предприятия», «Основы статистической обработки данных», «Управление проектами внедрения, сопровождения и адаптации ИС», «Стандартизация, сертификация и управление качеством в ИТ-сфере», «Экономика ИТ-проектов», «ИТ-инфраструктура предприятия», «Теория и методология управления проектами», «Программная инженерия», «Управление проектами внедрения, сопровождения и адаптации ИС», «Продвижение научной продукции», «Правоведение».

Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Проектирование информационных систем», «ИТ инфраструктура предприятия», «Информационный менеджмент», «Управление ИТ-рисками», «Оценка эффективности ИТ-проектов», «Финансовая математика», «Математическая экономика», «Управление рисками ИТ-проектов», «Управление качеством в ИТ-проектах», «Основы реинжиниринга бизнес-процессов», «Информационные технологии в управлении проектами», «Корпоративные системы управления проектами», «Гибкие технологии управления ИТ-проектами», производственной – преддипломной практике, производственной - практике по получению профессиональных умений и опыта профессиональной деятельности, подготовке к сдаче и сдача государственного экзамена, а так же при подготовке к защите и защита выпускной квалификационной работы.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения

В результате освоения дисциплины «Информационная безопасность» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ОК-4 – способностью использовать основы правовых знаний в различных сферах деятельности	
Знать	− основные нормативные правовые документы в области информационной безопасности.
Уметь	− применять требования нормативных правовых документов для решения учебных задач дисциплины.
Владеть	− навыками работы с нормативно-правовыми актами, практикой их толкований и применения по вопросам правовых основ информационной

Структурный элемент компетенции	Планируемые результаты обучения
	безопасности, имеющих значение для профессиональной подготовки специалистов в области ИС и ИТ.
ОПК-1 – способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий	
Знать	− основные нормативно-правовые документы, международные и отечественные стандарты в области обеспечения информационной безопасности ИС и ИТ;
Уметь	− распознавать и обсуждать международные и отечественные стандарты в области обеспечения информационной безопасности ИС и ИТ.
Владеть	− навыками работы с нормативно-правовыми документами, международными и отечественными стандартами в области обеспечения информационной безопасности ИС и ИТ, имеющих значение для профессиональной подготовки специалистов прикладной информатики;
ОПК-4 – способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
Знать	− понятийный аппарат в предметной области дисциплины; − требования к защите информации определенного типа, способы защиты информации в автоматизированных системах обработки данных, глобальных и локальных сетях; − методы защиты от вредоносных программ;
Уметь	− подбирать и использовать методы и средства защиты информации
Владеть	− навыками применения средств административного и процедурного уровней защиты информации;
ПК-21 – способностью проводить оценку экономических затрат и рисков при создании информационных систем	
Знать	− методики оценки экономических затрат на обеспечение ИБ на различных этапах жизненного цикла информационных систем;
Уметь:	− осуществлять оценку экономических затрат на обеспечение ИБ;
Владеть:	− методикой оценки совокупной стоимости владения для подсистемы ИБ;
ДПК-2 – способностью принимать участие в управлении проектами, организации ИТ-инфраструктуры и управлении информационной безопасностью	
Знать	− классы мер процедурного уровня обеспечения ИБ (управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ);
Уметь:	− определять требования и мероприятия в области защиты информации по видам обеспечения информационных систем;
Владеть:	− административными, процедурными и программно-техническими мерами обеспечения ИБ на различных этапах жизненного цикла информационных систем;

4 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 65,7 акад. часов:
– аудиторная – 64 акад. часов;
– внеаудиторная – 1,7 акад. часов
– самостоятельная работа – 78,3 акад. часов;

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
Раздел 1. Основы информационной безопасности и защиты информации								
1.1. Сущность и понятие информационной безопасности Основные понятия. Значение информационной безопасности для субъектов информационных отношений. Понятие и сущность защиты информации. Цели и концептуальные основы защиты информации. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации.	6	4	2		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 1 «Надежность и достоверность информации»	ОК-4 – зув ОПК-1 – зув ОПК-4 – зув
1.2. Угрозы информационной безопасности Угрозы информационной безопасности и защиты информации. Дестабилизирующее воздействие на защищаемую информа-	6	4	2		3	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной	Тестирование ЛР «Классификация угроз предметной области»	ОК-4 – зув ОПК-1 – зув ОПК-4 –

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
цию. Классификация видов угроз информационной безопасности по различным признакам. Несанкционированный доступ к информации.						работы		зув ДПК-2 – зув
Итого по разделу		**8**	**4**		**5**			
Раздел 2. Законодательный уровень обеспечения информационной безопасности								
2.1. Правовые основы обеспечения безопасности информационных технологий Назначение и структура правового обеспечения защиты информации. Методы правовой защиты информации. Правовая основа допуска и доступа персонала к защищаемым сведениям. Правовые основы защиты информации в организации. Понятие интеллектуальной собственности, ее виды и основные объекты образования.	6	2	2		5	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 3: проработка научно-методической литературы, доклад и презентация	Тестирование Выступление на семинаре по ЛР 3 «Законодательная и нормативно-правовая база обеспечения информационной безопасности»	ОК-4 – зу ОПК-1 – зув ОПК-4 – зув
2.2. Стандарты и спецификации в области информационной безопасности Международные и национальные стандарты и спецификации в области ИБ. Федеральные критерии безопасности информационных технологий. Профиль защиты. Назначение, структура и этапы разработки	6	2	2		5	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 4: проработка научно-методической литературы, доклад и презентация	Тестирование Выступление на семинаре по ЛР 4 «Стандарты и спецификации в области информационной безопасности»	ОК-4 – зу ОПК-1 – зув ОПК-4 – зув

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
профиля защиты. Ядро безопасности. Современные стандарты в области управления рисками информационной безопасности.								
Итого по разделу		**4**	**4**		**10**			
Раздел 3. Административный и процедурный уровни информационной безопасности								
3.1. Административный уровень обеспечения ИБ Политика безопасности. Программа безопасности. Оценка рисков и базовый уровень защиты.	6	4	2/4И		13	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 5: проработка научно-методической литературы, доклад и презентация Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование Выступление на семинаре по ЛР 5 «Политика информационной безопасности»	ОК-4 – зу ОПК-1 – зув ОПК-4 – зув ДПК-2 – зув
3.2. Классы мер процедурного уровня Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.	6	2	6/2И		13	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 6 «Аудит защищенности сетей» ЛР 7 «Парольная защита и менеджеры паролей» ЛР 8 «Массовая рассылка писем»	ОК-4 – зу ОПК-1 – зув ОПК-4 – зув ДПК-2 – зув

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
Итого по разделу		**6**	**8/6И**		**26**			
Раздел 4. Программно-технические меры обеспечения защиты информации								
4.1. Программные средства защиты информации Защита программного обеспечения от несанкционированного доступа. Краткий обзор существующих на рынке средств защиты информации от несанкционированного доступа. Задача защиты от вмешательства посторонних лиц и аппаратные средства аутентификации	6	2	8/4И		12	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 9 «Защита от несанкционированного доступа к информации» ЛР 10 «Защита информации в документах» ЛР 11 «Удаление информации» ЛР 12 «Восстановление данных»	ОК-4 – зув ОПК-1 – зув ОПК-4 – зув ДПК-2 – зув
4.2. Вирусы и антивирусные средства Определение компьютерных вирусов. Классификация компьютерных вирусов. Признаки заражения. Профилактика заражения. Программные антивирусные средства. Структура антивирусной программы. Принципы выбора сигнатуры компьютерного вируса.	6	2	2/4И		5	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 13: проработка научно-методической литературы, доклад и презентация	Тестирование Выступление на семинаре по ЛР 13 «Современные вредоносные программы для ПК и мобильных устройств»	ОК-4 – зу ОПК-1 – зу ОПК-4 – зу ДПК-2 – зу
4.3. Криптографические методы защиты Методы криптографии. Средства криптографической защиты информации. Криптографические преобразования. Шифро-	6	2	4		8	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 14 «Защита информации с помощью криптографии» ЛР 15 «Защита информации с помощью стеганографии»	ОК-4 – зув ОПК-1 – зув

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
вание и дешифрование информации. Цифровая подпись.						Выполнение заданий лабораторной работы		ОПК-4 – зув ДПК-2 – зув
4.4. Технические средства защиты информации Инженерная защита объектов, защита информации от утечки по техническим каналам.	6	2	2		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 16 «Авторизация на веб-ресурсе»	ОК-4 – зув ОПК-1 – зув ОПК-4 – зув ДПК-2 – зув
4.5. Информационно-психологическая безопасность Понятие информационно-психологической безопасности. Источники информационно-психологического воздействия на человека. Виды информационно-психологических воздействий. НЛП. Секты. Пирамиды. Рассылки. Защита личности от информационно-психологических угроз	6	2	2		0,3	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 17 «Информационно-психологические манипуляции»	ОК-4 – зув ОПК-1 – зув ОПК-4 – зув
Итого по разделу		**10**	**18/8И**		**25,3**			

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
Раздел 5. Экономика защиты информации								
5.1. Экономические проблемы обеспечения информационной безопасности Экономическая безопасность предприятия. Информация как важнейший ресурс экономики. Основные подходы к определению затрат на защиту информации. Система ресурсообеспечения защиты информации. Управление ресурсами в процессе защиты информации.	6	2	-		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы	Тестирование	ОК-4 – зув ОПК-1 – зув ОПК-4 – зув ПК-21 – з
5.2. Методика оценки совокупной стоимости владения для подсистемы ИБ Границы применения методики. Технология оценки затрат на ИБ. Идентификация затрат на безопасность. Внедрение системы учета затрат на ИБ	6	2	2		8	Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	ЛР 18 «Оценка затрат компании на информационную безопасность»	ОК-4 – зув ОПК-1 – зув ОПК-4 – зув ПК-21 – зув
Итого по разделу		**4**	**2**		**10**			
Итого за семестр		**32**	**32/14И**		**78,3**		**зачет с оценкой**	
Итого по дисциплине		**32**	**32/14И**		**78,3**			

5 Образовательные и информационные технологии

При проведении занятий и организации самостоятельной работы студентов используются:

Традиционные технологии обучения, предполагающие передачу информации в готовом виде, формирование учебных умений по образцу: лекция-изложение, лекция-объяснение, лабораторные работы, контрольная работа и др.

Интерактивные формы обучения, предполагающие организацию обучения как продуктивной творческой деятельности в режиме взаимодействия студентов друг с другом и с преподавателем

При проведении лабораторных занятий используются групповая работа, технология коллективной творческой деятельности, технология сотрудничества, Case-study. Данные технологии обеспечивают высокий уровень усвоения студентами знаний, эффективное и успешное овладение умениями и навыками в предметной области, формируют познавательную потребность и необходимость дальнейшего самообразования, позволяют активизировать исследовательскую деятельность, обеспечивают эффективный контроль усвоения знаний.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Информационная безопасность» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа студентов предполагает решение и оформление согласно заданным требованиям заданий лабораторных работ. Требования к оформлению находятся в СМК-О-СМГТУ-42-09 Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления.

Внеаудиторная самостоятельная работа студентов осуществляется в виде изучения учебной и научной литературы по соответствующему разделу с проработкой материала, участие в дистанционном курсе или изучении МООК, предложенном преподавателем и выполнения домашних заданий (подготовка к лабораторным работам) с консультациями преподавателя.

Лабораторная работа 1. Надежность и достоверность информации

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 2. Законодательная и нормативно-правовая база обеспечение информационной безопасности

1. Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Подготовьте доклад и презентацию по выбранной теме.
2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»
3. Презентация и доклад представляются на занятии.

Лабораторная работа 3. Стандарты и спецификации в области информационной безопасности

1. Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Подготовьте доклад и презентацию по выбранной теме.
2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»
3. Презентация и доклад представляются на занятии

Лабораторная работа 4. Классификация угроз предметной области

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Разработайте модель нарушителя и модель угроз ИБ для организации, предложенной преподавателем. Оформите отчет по лабораторной работе в соответствии с требованиями

Лабораторная работа 5. Политика информационной безопасности

1. Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Подготовьте доклад и презентацию по выбранной теме.
2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»

3. Презентация и доклад представляются на занятии.

Лабораторная работа 6. Аудит защищенности сетей

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 7. Парольная защита и менеджеры паролей

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 8. Массовая рассылка писем

Познакомьтесь с рекомендуемым программным средством. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 9. Защита от несанкционированного доступа к информации

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 10. Защита информации в документах

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 11. Удаление информации

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 12. Восстановление данных

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 13. Современные вредоносные программы для ПК и мобильных устройств

1. Подготовить доклад и презентацию по выбранной теме.

2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»

3. Презентация и доклад представляются на занятии.

Лабораторная работа 14. Защита информации с помощью криптографии

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 15. Защита информации с помощью стеганографии

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 16. Авторизация на веб-ресурсе

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 17. Информационно-психологические манипуляции

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 18. Оценка затрат компании на информационную безопасность

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

7 Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОК-4 – способностью использовать основы правовых знаний в различных сферах деятельности		
Знать	− основные нормативные правовые документы в области информационной безопасности.	**Примерные варианты тестовых заданий.** 1. Что такое безопасность данных? a. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение b. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное искажение c. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их преднамеренное получение, изменение или уничтожение d. состояние защищенности национальных интересов РФ во всех сферах человеческой деятельности 2. Что является целью защиты информации? a. защита информации от утечки b. желаемый результат защиты информации c. защита информации от утраты d. предотвращение утраты и утечки конфиденциальной информации **Перечень вопросов для подготовки к зачету** 1. Понятие информационной безопасности. 2. Основные составляющие информационной безопасности 3. Важность и сложность проблемы информационной безопасности 4. Законодательный уровень информационной безопасности 5. Обзор российского законодательства в области информационной безопасности 6. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности 7. Закон «Об информации, информатизации и защите информации» 8. Закон «О лицензировании отдельных видов деятельности» 9. Закон «Об электронной цифровой подписи» 10. .
Уметь	– применять требования нормативных правовых документов для решения учебных задач дисциплины.	**Практическое задание** Оформить результаты практических заданий с соблюдением прав интеллектуальной собственности на информацию

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Владеть	− навыками работы с нормативно-правовыми актами, практикой их толкований и применения по вопросам правовых основ информационной безопасности, имеющих значение для профессиональной подготовки специалистов в области ИС и ИТ.	**Комплексное задание** Подобрать требования существующего законодательства к ситуациям, предложенным преподавателем
ОПК-1 – способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий		
Знать	− основные нормативно-правовые документы, международные и отечественные стандарты в области обеспечения информационной безопасности ИС и ИТ;	**Примерные варианты тестовых заданий.** 1. Согласно рекомендациям X.800, целостность с восстановлением может быть реализована на: a. Сетевом уровне b. Транспортном уровне c. Прикладном уровне d. Логическом уровне 2. Требования «Общих критериев» группируются в: a. Классы b. Подклассы c. Группы d. Подгруппы **Перечень вопросов для подготовки к зачету** 1. Обзор зарубежного законодательства в области информационной безопасности 2. Оценочные стандарты и технические спецификации. 3. Основные понятия административного уровня информационной безопасности 4. Политика безопасности 5. Программа безопасности 6. Синхронизация программы безопасности с жизненным циклом систем
Уметь	− применять требования международные и отечественные стандартов для решения учебных задач дисциплины	**Практическое задание** Оформить результаты практических заданий с соблюдением прав интеллектуальной собственности на информацию
Владеть	− навыками работы с нормативно-правовыми документами, международными	**Комплексное задание** Подобрать требования существующего законодательства к ситуациям, предложенным преподавателем

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	и отечественными стандартами в области обеспечения информационной безопасности ИС и ИТ, имеющих значение для профессиональной подготовки специалистов прикладной информатики;	
ОПК-4 – способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
Знать	− понятийный аппарат в предметной области дисциплины; − требования к защите информации определенного типа, способы защиты информации в автоматизированных системах обработки данных, глобальных и локальных сетях; − методы защиты от вредоносных программ;	**Примерные варианты тестовых заданий.** 1. Укажите некорректное определение нарушителя ИБ: a. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами b. физическое или юридическое лицо, случайно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами c. это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства 2. Что такое защищаемая информация? a. любая информация, которая появляется в СМИ b. информация, которая подлежит защите в соответствии с требованиями правовых документов и обязательно относится к государственной тайне c. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации **Перечень вопросов для подготовки к зачету** 1. Понятие информационной безопасности. 2. Основные составляющие информационной безопасности 3. Важность и сложность проблемы информационной безопасности 4. Основные определения и критерии классификации угроз 5. Наиболее распространенные угрозы доступности 6. Вредоносное программное обеспечение 7. Основные угрозы целостности 8. Основные угрозы конфиденциальности 9. Идентификация и аутентификация 10. Управление доступом

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		11. Ролевое управление доступом 12. Протоколирование и аудит 13. Шифрование 14. Экранирование 15. Классификация межсетевых экранов 16. Анализ защищенности 17. Доступность 18. Отказоустойчивость и зона риска 19. Криптография 20. Вредоносные программы и способы защиты от них 21. Подразделения технической защиты информации. 22. Место и роль аппаратно-программных средств защиты. 23. Требования руководящих документов к средствам защиты информации от несанкционированного доступа. 24. Обнаружение сетевой атаки. 25. Способы обеспечения безопасной работы в Интернет. 26. Принципы функционирования брандмауэров. 27. Перечень информационных ресурсов, подлежащих защите. 28. Основы безопасности web-ресурсов. 29. Способы защиты файлов от постороннего доступа. 30. Эргономические и нормативные требования к организации рабочего места пользователя 31. Вредоносное программное обеспечение. 32. Пути проникновения вредоносного программного обеспечения. *33*. Способы защиты от вредоносного программного обеспечения
Уметь	− подбирать и использовать методы и средства защиты информации	**Практическое задание** Восстановить удаленную информацию Удалить информацию с заданными параметрами Защитить информацию: пароль, криптография, стеганография
Владеть	− навыками применения средств административного и процедурного уровней защиты информации;	**Комплексное задание** Применять специализированное программное обеспечение для сохранения конфиденциальности информации: хранение паролей, удаление информации, сокрытие информации
ПК-21 – способностью проводить оценку экономических затрат и рисков при создании информационных систем		

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Знать	− методики оценки экономических затрат на обеспечение ИБ на различных этапах жизненного цикла информационных систем;	**Примерные варианты тестовых заданий**. 1. Что не входит в основные положения методики ССВ a. Аудит ИБ b. Расчет затрат на ИБ c. Обеспечение физической безопасности d. Обучение персонала **Перечень вопросов для подготовки к зачету** Методика оценки совокупной стоимости владения для подсистемы ИБ.
Уметь	− осуществлять оценку экономических затрат на обеспечение ИБ;	**Практическое задание** Оценить затраты на ИБ по методике совокупной стоимости
Владеть	− методикой оценки совокупной стоимости владения для подсистемы ИБ;	**Комплексное задание** Подобрать комплекс мер для обеспечения ИБ заданной компании
ДПК-2 – способностью принимать участие в управлении проектами, организации ИТ-инфраструктуры и управлении информационной безопасностью		
Знать	− классы мер процедурного уровня обеспечения ИБ (управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ);	**Примерные варианты тестовых заданий.** 1. Главная цель мер, предпринимаемых на административном уровне: a. Сформировать программу безопасности и обеспечить ее выполнение b. Выполнить положения действующего законодательства c. Отчитаться перед вышестоящими инстанциями d. Выявление критически важных функций организации 2. В число принципов управления персоналом входят: a. Минимизация привилегий b. Минимизация зарплаты c. Максимизация привилегий **Перечень вопросов для подготовки к зачету** 1. Управление рисками 2. Основные классы мер процедурного уровня 3. Управление персоналом 4. Физическая защита 5. Поддержание работоспособности 6. Реагирование на нарушения режима безопасности 7. Основные понятия программно-технического уровня информационной безопасности 8. Особенности современных информационных систем, существенные с точки зрения безопасности

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		9. Понятие и сущность защиты информации. 10. Объекты защиты информации. 11. Средства защиты информации. 12. Методы защиты информации.
Уметь	− определять требования и мероприятия в области защиты информации по видам обеспечения информационных систем;	**Практическое задание** Сформировать пароль с заданными критериями устойчивости Рассчитать устойчивость пароля
Владеть	− административными, процедурными и программно-техническими мерами обеспечения ИБ на различных этапах жизненного цикла информационных систем;	**Комплексное задание** Обеспечить защиту информации документов различного типа

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Информационная безопасность» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета м оценкой.

Зачет по данной дисциплине проводится в устной форме по зачетным билетам, каждый из которых включает один теоретический вопрос и одно практическое задание.

Показатели и критерии оценивания зачета:

«Отлично» – оценка знаний студента, который свободно владеет:

1) понятийно-терминологической базой дисциплины и знает значение наиболее часто используемых аббревиатур;

2) четко увязывает теоретическое познание дисциплины с реальной практикой;

3) знаком с широким кругом литературных источников, знает, где их достать, хорошо разбирается в истории становления дисциплины, в оценке ее текущего состояния и перспектив ее развития;

4) полностью владеет материалом практического задания, четко и аргументировано защищает ее положительные результаты, обосновано комментирует и объясняет допущенные недочеты.

«Хорошо» – оценка знаний студента, который владеет понятийно-терминологической базой дисциплины, может увязать теоретическое познание дисциплины с реальной практикой. Владеет материалом практической работы, показал способность к объяснению смысла основных положений;

«Удовлетворительно» – оценка знаний студента, который в большей части владеет, с небольшими изъянами, понятийно-терминологической базой дисциплины, имеет представление о внутренней логике дисциплины, представленной в виде учебной программы, Владеет, но неуверенно, материалом практического задания.

«Неудовлетворительно» – оценка знаний студента, который не владеет понятийно-терминологической базой дисциплины и материалом практического задания.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-450371

б) Дополнительная литература:

1. Чернова Е.В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-cheloveka-449350

2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. – 4-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2019. – 322 с. — (Высшее образование). – ww.dx.doi.org/10.12737/11380. – Текст : электронный. – URL: https://znanium.com/read?id=336219

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/prestupleniya-v-sfere-informacionnoy-bezopasnosti-448295

4. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2019.– 223 с. – (Высшее образование: Бакалавриат). – www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. – Текст : электронный. – URL: https://znanium.com/read?id=342244

4. Инженерный журнал: наука и инновации - http://engjournal.ru/

в) Методические указания:

1. Методические указания по выполнению лабораторной работы «Надежность и достоверность информации» для бакалавров направления 38.03.05 Бизнес-информатика, 09.03.03 «Прикладная информатика», 44.03.05 «Педагогическое образование (Информатика и экономика)». – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2020. – 12 с.

2. Чернова, Е. В. Практикум по информационной безопасности для бакалавров прикладной математики : практикум [для вузов] / Е. В. Чернова ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - Загл. с титул. экрана. - URL : https://magtu.informsystema.ru/uploader/fileUpload?name=4064.pdf&show=dcatalogues/1/1533914/4064.pdf&view=true (дата обращения: 09.10.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 (подписка Imagine Premium)	Д-1227 от 8.10.2018	11.10.2021

MS Windows 10 (подписка Imagine Premium)	Д-1227 от 8.10.2018	11.10.2021
MS Office 2007	№ 135 от 17.09.2007	бессрочная
FAR Manager	свободно распространяемое ПО	бессрочно
7Zip	свободно распространяемое	бессрочная
Lpro	GNU GPL v3	бессрочная
GlassWire	free (бесплатная)	бессрочная
Генератор паролей 1.5	FreeWare	бессрочная
KeePass Password Safe	GNU General Public License	бессрочная
Thunderbird	MPL v1.1/GPL v3/LGPL v3	бессрочная
Recuva	бесплатно	бессрочная
Alternate File Shredder	FreeWare	бессрочная
HDD Low Level Format Tool	FreeWare	бессрочная
Шифратор «Решетка Кардано»	бесплатно	бессрочная
S-Tools	Freeware	бессрочная
Mozilla Firefox для Windows	Mozilla Public License, version 2.0, GNU GPL и GNU LGPL	бессрочная

Интернет-ресурсы:

1. Портал научной электронной библиотеки – URL: http://elibrary.ru/defaultx.asp
2. Электронный фонд правовой и нормативной документации. – URL: http://docs.cntd.ru
3. Справочная правовая система «Консультант плюс» – URL: http://www.consultant.ru/
4. Справочная правовая система «Гарант» – URL: http://www.garant.ru/
5. Positive Hack Days – URL: https://www.phdays.com/ru/
6. Информационная безопасность. Защита данных – URL: https://habr.com/ru/hub/infosecurity/
7. Сервис генерации паролей с заданными требованиями – URL: https://genpas.peter23.com/
8. Сервис проверки пароля на устойчивость ко взлому – URL: https://exploit.in/passcheck/
9. Сервис проверки логина и пароля по базе взломанных паролей – URL: https://haveibeenpwned.com/Passwords
10. Онлайн менеджер паролей – URL: https://passgenerator.ru/menedzher-paroley
11. Сервис генерации токенов – URL: https://www.stationx.net/canary/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Учебные аудитории для проведения занятий лекционного типа	Специализированная (учебная) мебель (столы, стулья, доска аудиторная), мультимедийное оборудование (проектор, компьютер, экран) для презентации учебного материала по дисциплине;
Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами
Аудитории для самостоятельной работы (компьютерные классы; читальные залы библиотеки)	Специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами
Помещение для хранения и профилактического обслуживания учебного оборудования	Мебель (столы, стулья, стеллажи для хранения учебно-наглядных пособий и учебно-методической документации), персональные компьютеры.