МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

04.02.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ

Направление подготовки (специальность)
27.03.01 Стандартизация и метрология

Направленность (профиль/специализация) программы
Стандартизация, менеджмент и контроль качества

Уровень высшего образования - бакалавриат

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7

Магнитогорск
2025 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 27.03.01 Стандартизация и метрология (приказ Минобрнауки России от 07.08.2020 г. № 901)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
03.02.2025 г., протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
04.02.2025 г., протокол № 3

Председатель _____ В.Р. Храмшин

Согласовано:
Зав. кафедрой Технологий, сертификации и сервиса автомобилей

_____ **И.Ю.Мезин**

Рабочая программа составлена:
ст. преподаватель кафедры ИиИБ _____ Ю.А. Мазнина

Рецензент:
Проректор по цифровизации, канд. техн. наук _____ К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры ПИЛОТЫ

Протокол от _____20__г. № ___
Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры ПИЛОТЫ

Протокол от _____20__г. № ___
Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры ПИЛОТЫ

Протокол от _____20__г. № ___
Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры ПИЛОТЫ

Протокол от _____20__г. № ___
Зав. кафедрой _____

1 Цели освоения дисциплины (модуля)

1) определение и оценка угроз, разработка моделей угроз в ходе создания и эксплуатации информационных систем;

2) выявление, анализ и устранение уязвимостей в ходе создания и эксплуатации

3) выявление источников угроз несанкционированного доступа (НСД)

4) определение типа нарушителя

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Угрозы кибербезопасности входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Цифровая грамотность

Персональная эффективность

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Проектная деятельность

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

В результате освоения дисциплины (модуля) «Угрозы кибербезопасности» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ДПК-004-5 Способен обеспечить функционирование средств защиты информации в информационно-аналитических системах	
ДПК-004-5.1	Применяет знания в области безопасности вычислительных сетей в информационных системах
ДПК-004-5.2	Применяет знания в организации мер по защите информации в процессе эксплуатации информационных системах

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 36,1 акад. часов:

– аудиторная – 36 акад. часов;

– внеаудиторная – 0,1 акад. часов;

– самостоятельная работа – 71,9 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Нормативные и правовые акты в области защиты информации								
1.1 Основные понятия и задачи моделирования угроз кибербезопасности. База данных угроз ФСТЭК РФ.	7			4	2	Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме.	Текущий контроль успеваемости: – устный опрос (собеседование); – семинарские занятия;	ДПК-004-5.2
Итого по разделу				4	2			
2. Этапы моделирования угроз ИБ								
2.1 Выявление объектов информационной системы, подлежащих защите. Определение источников угроз	7			4	6	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – контрольные работы; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
2.2 Наиболее часто реализуемые угрозы. Выявление способов				4	20	Подготовка к практическому занятию.	Текущий контроль успеваемости:	ДПК-004-5.1, ДПК-004-5.2

реализации угроз						Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – проверка индивидуальных заданий	
2.3 Угрозы мобильным устройствам.	7			4	10,9	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
Итого по разделу				12	36,9			
3. Модель угроз ИСПДн информационной системы персональных данных								
3.1 Угрозы безопасности ПДн. Каналы реализации угроз безопасности ПДн.	7			8	17	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
3.2 Классификация угроз безопасности персональных данных по способу реализации				6	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
Итого по разделу				14	27			

4. Методики построения дерева угроз								
4.1 Разработка модели информационной безопасности с учетом реализованных защитных мер. Формирование перечня активов, определение их значимости для компании	7			6	6	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
Итого по разделу				6	6			
Итого за семестр				36	71,9		зачёт	
Итого по дисциплине				36	71,9		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

Формы учебных занятий с использованием традиционных технологий:

– информационные – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;

– семинар – практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

– практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков;

– практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности; обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них; кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации;

– подготовка тематических рефератов, содержащих разделы, частично или полностью выносимые на самостоятельное изучение.

Формы учебных занятий с использованием игровых технологий:

– учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого;

– деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Технологии проектного обучения:

– творческий проект – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.);

– информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313 (дата обращения: 09.05.2025).

2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140566 (дата обращения: 09.05.2025). – Режим доступа: по подписке.

3. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / под науч. ред. И.А. Калиниченко. — Москва : ИНФРА-М, 2024. — 642 с. — (Высшее образование: Специалитет). —. - ISBN 978-5-16-017838-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2121606 (дата обращения: 09.05.2025). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебник для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561314 (дата обращения: 09.05.2025).

2. Неверов, Д. Идём по кибersледу : анализ защищенности Active Directory с помощью утилиты BloodHound : практическое руководство / Д. Неверов. - Москва : Альпина ПРО, 2025. - 304 с. - ISBN 978-5-206-00398-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2206535 (дата обращения: 09.05.2025). – Режим доступа: по подписке.

3. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/1858. - ISBN 978-5-9967-1031-7. - Текст : электронный. - дата обращения: 09.05.2025.

в) Методические указания:

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

	Наименование ПО	№ договора	Срок действия лицензии	
	MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно	
	7Zip	свободно распространяемое ПО	бессрочно	

LibreOffice	свободно распространяемое ПО	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лаборатория программно-аппаратных средств обеспечения информационной безопасности:

– компьютер Destene Volution i560 на базе Windows Server 2008 R2(Standart) MSDN;

– ПЭВМ на базе Windows 7 – 12 шт.;

– мультимедийные средства хранения, передачи и представления информации.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

– персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета;

– мультимедийные средства хранения, передачи и представления информации;

– комплекс тестовых заданий для проведения промежуточных и рубежных контролей.

Помещения для самостоятельной работы обучающихся:

– персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для хранения и профилактического обслуживания учебного оборудования:

– шкафы для хранения учебно-методической документации, учебного оборудования и учебно-наглядных пособий.

Помещения для самостоятельной работы обучающихся:

– персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для хранения и профилактического обслуживания учебного оборудования:

– шкафы для хранения учебно-методической документации, учебного оборудования и учебно-наглядных пособий.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося с использованием методов IT.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а так же с применением кейс-технологий.

а) Контрольные вопросы и задания для проведения текущего контроля

1. Что такое кибербезопасность и почему она важна?
2. Какие основные цели преследуют злоумышленники в киберпространстве?
3. Какие существуют основные принципы обеспечения кибербезопасности?
4. Опишите основные категории угроз кибербезопасности.
5. Что такое уязвимость, угроза и риск в контексте кибербезопасности?
6. Какие существуют этапы жизненного цикла угрозы?
7. Объясните разницу между активными и пассивными атаками.
8. Какие основные методы защиты информации используются для противодействия угрозам?
9. Что такое политика безопасности и какова ее роль в обеспечении кибербезопасности?
10. Какие существуют основные международные и национальные стандарты в области кибербезопасности?
11. Какие основные типы средств защиты информации используются в информационно-аналитических системах?
12. Каковы основные функции межсетевого экрана (firewall)? Какие типы межсетевых экранов существуют?
13. Что такое система обнаружения вторжений (IDS) и как она работает? Какие типы IDS существуют?
14. Что такое система предотвращения вторжений (IPS) и чем она отличается от IDS?
15. Опишите принципы работы антивирусного программного обеспечения.
16. Что такое SIEM (Security Information and Event Management) система и какова ее роль в обеспечении кибербезопасности?
17. Каковы основные принципы работы систем контроля доступа? Какие модели контроля доступа существуют?
18. Что такое шифрование и для чего оно используется? Какие алгоритмы шифрования вы знаете?
19. Объясните принципы работы VPN (Virtual Private Network).
20. Что такое двухфакторная аутентификация и почему она важна?
21. Опишите основные типы сетевых атак (например, DDoS, MITM, sniffing).
22. Что такое сканирование портов и как оно используется злоумышленниками?
23. Объясните, как работает протокол TCP/IP и какие уязвимости могут быть связаны с его использованием.
24. Что такое DNS-спуфинг и как от него защититься?
25. Какие существуют методы защиты беспроводных сетей (Wi-Fi)?
26. Опишите основные принципы построения безопасной сетевой архитектуры.
27. Что такое сегментация сети и зачем она нужна?
28. Какие инструменты используются для мониторинга сетевого трафика и обнаружения аномалий?

29. Каковы основные этапы управления рисками в кибербезопасности?
30. Опишите основные меры по обеспечению физической безопасности информационных систем.
31. Какова роль обучения и повышения осведомленности пользователей в области кибербезопасности?
32. Какие процедуры необходимо выполнять при обнаружении инцидента кибербезопасности?
33. Что такое план восстановления после аварии (Disaster Recovery Plan) и какова его цель?
34. Как обеспечить безопасность облачных сред?
35. Что такое тестирование на проникновение (пентест) и как оно используется для оценки уровня безопасности ИС?
36. Как обеспечить безопасность веб-приложений? Какие типы уязвимостей веб-приложений наиболее распространены?
37. Как обеспечить безопасность баз данных?
38. Что такое аудит безопасности и как он проводится?
39. Как обеспечить соответствие требованиям регуляторов в области кибербезопасности?
40. Что такое управление уязвимостями и как оно осуществляется?

б) Примеры индивидуальных домашних заданий

1. Используя Nmap, проведите сканирование заданной сети и определите открытые порты, работающие службы и операционные системы хостов. Сформируйте отчет о результатах сканирования.
2. Настройте заданный межсетевой экран для защиты заданной системы. Разрешите только необходимые соединения и заблокируйте все остальные, сформируйте скрипт. Составьте отчет о проделанной работе с с описанием правил и обоснованием их необходимости.
3. Используя сканер уязвимостей Nessus (или OpenVAS), проведите сканирование заданной системы и определите имеющиеся уязвимости. Сформируйте отчет о результатах сканирования с указанием обнаруженных уязвимостей, их уровня опасности и рекомендаций по устранению.
4. Настройте web application firewall для защиты заданного веб-приложения от распространенных атак. Составьте отчет о проделанной работе, описав правила конфигурации и их назначение.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

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

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ДПК-004-5 Способен обеспечить функционирование средств защиты информации в информационно-аналитических системах – ДПК-004-5.1 Применяет знания в области безопасности вычислительных сетей в информационных системах – ДПК-004-5.2 Применяет знания в организации мер по защите информации в процессе эксплуатации информационных системах		
ДПК-004-5.1	Применяет знания в области безопасности вычислительных сетей в информационных системах	Теоретические вопросы к зачету: 1. Что такое кибербезопасность и почему она важна? 2. Какие основные цели преследуют злоумышленники в киберпространстве? 3. Какие существуют основные принципы обеспечения кибербезопасности? 4. Опишите основные категории угроз кибербезопасности. 5. Что такое уязвимость, угроза и риск в контексте кибербезопасности? 6. Какие существуют этапы жизненного цикла угрозы? 7. Объясните разницу между активными и пассивными атаками. 8. Какие основные методы защиты информации используются для противодействия угрозам? 9. Что такое политика безопасности и какова ее роль в обеспечении кибербезопасности? 10. Какие существуют основные международные и национальные стандарты в области кибербезопасности? 11. Какие основные типы средств защиты информации используются в информационно-аналитических системах? 12. Каковы основные функции межсетевого экрана (firewall)? Какие типы межсетевых экранов существуют? 13. Что такое система обнаружения вторжений (IDS) и как она работает? Какие типы IDS существуют? 14. Что такое система предотвращения вторжений (IPS) и чем она отличается от IDS? 15. Опишите принципы работы антивирусного программного обеспечения. 16. Что такое SIEM (Security Information and Event Management) система и какова ее роль в обеспечении кибербезопасности? 17. Каковы основные принципы работы систем контроля доступа? Какие модели контроля доступа существуют?

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		18. Что такое шифрование и для чего оно используется? Какие алгоритмы шифрования вы знаете? 19. Объясните принципы работы VPN (Virtual Private Network). 20. Что такое двухфакторная аутентификация и почему она важна? 21. Опишите основные типы сетевых атак (например, DDoS, MITM, sniffing). 22. Что такое сканирование портов и как оно используется злоумышленниками? 23. Объясните, как работает протокол TCP/IP и какие уязвимости могут быть связаны с его использованием. 24. Что такое DNS-спуфинг и как от него защититься? 25. Какие существуют методы защиты беспроводных сетей (Wi-Fi)? 26. Опишите основные принципы построения безопасной сетевой архитектуры. 27. Что такое сегментация сети и зачем она нужна? 28. Какие инструменты используются для мониторинга сетевого трафика и обнаружения аномалий? Примеры практических заданий для зачета: 1. С помощью программы-анализатора трафика для компьютерных сетей Wireshark перехватите и проанализируйте сетевой трафик. Определите типы протоколов, используемых в сети, и выявите потенциально опасные соединения. Сформируйте отчет о результатах анализа. 2. Проанализируйте лог-файлы веб-сервера, системы контроля доступа или межсетевого экрана. Выявите подозрительные события и попытки несанкционированного доступа. Сформируйте отчет о проделанной работе с описанием выявленных подозрительных событий, их возможными последствиями и рекомендациями по защите.
ДПК-004-5.2	Применяет знания в организации мер по защите информации в процессе эксплуатации информационн ых системах	Теоретические вопросы к зачету: 1. Каковы основные этапы управления рисками в кибербезопасности? 2. Опишите основные меры по обеспечению физической безопасности информационных систем. 3. Какова роль обучения и повышения осведомленности пользователей в области кибербезопасности? 4. Какие процедуры необходимо выполнять при обнаружении инцидента кибербезопасности? 5. Что такое план восстановления после аварии (Disaster Recovery Plan) и какова его цель? 6. Как обеспечить безопасность облачных сред? 7. Что такое тестирование на проникновение (пентест) и как оно используется для оценки уровня

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		безопасности ИС? 8. Как обеспечить безопасность веб-приложений? Какие типы уязвимостей веб-приложений наиболее распространены? 9. Как обеспечить безопасность баз данных? 10. Что такое аудит безопасности и как он проводится? 11. Как обеспечить соответствие требованиям регуляторов в области кибербезопасности? 12. Что такое управление уязвимостями и как оно осуществляется? Примеры практических заданий для зачета: 1. Используя Hydra, проведите bruteforce атаку на заданную службу. Настройте защиту от bruteforce атак. Сформируйте отчет о проделанной работе, описав проведенную bruteforce атаку, оценив эффективность защиты и дав рекомендации по ее усилению. 2. Получите хэш пароля. Подберите пароль, используя различные словари и техники. Оцените стойкость пароля. Составьте отчет о проделанной работе, дав рекомендации по созданию надежных паролей. 3. На основе смоделированного инцидента безопасности создайте отчет об инциденте, включающий описание инцидента, его последствия и принятые меры. 4. Проведите оценку рисков безопасности для заданной информационной системы. Определите активы, угрозы, уязвимости и возможные последствия. Предложите меры по снижению рисков.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания

Показатели и критерии оценивания зачета:

− «зачтено» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

− «не зачтено» – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.