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

03.02.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

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

Магнитогорск
2026 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
22.01.2026, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
03.02.2026 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры кафедры ИиИБ, _____ Д.Н. Мазнин

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО) ,

_____ М.М. Близнецов

Лист актуализации рабочей программы

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

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

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

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

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

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2031 - 2032 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2032 - 2033 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью освоения дисциплины (модуля) «Технологии обеспечения информационной безопасности» является приобретение обучающимися навыков разработки проектных решений по защите информации (ЗИ) в автоматизированных системах (АС), в том числе навыков

1. разработки организационно-распорядительной и технической документации по защите информации в АС;
2. определения направления информационных технологий, для которых необходимо производить работы по защите информации в рамках защищаемой АС;
3. определения требуемый состав СЗИ и СКЗИ, необходимых для нейтрализации угроз, и разрабатывать сценарии их применения;
4. разработки и реализации сценариев подготовки и тренировки ИБ-персонала посредством киберучений.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Технологии обеспечения информационной безопасности входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Безопасность сетей ЭВМ

Безопасность систем баз данных

Моделирование угроз информационной безопасности

Безопасность Интернета вещей

Технология построения защищенных распределенных приложений

Программно-аппаратные средства обеспечения информационной безопасности

Теория информации

Сети и системы передачи информации

Информационные технологии. Базы данных

Организация ЭВМ и вычислительных систем

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

Анализ рисков информационной безопасности

Методы и стандарты оценки защищенности компьютерных систем

Разработка Siem систем

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Управление информационной безопасностью

Аттестация АИС

Защита программного обеспечения

Защита электронного документооборота

Методы выявления нарушений информационной безопасности

Методы проектирования систем защиты распределенных информационных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Форензика

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

В результате освоения дисциплины (модуля) «Технологии обеспечения информационной безопасности» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 69,8 акад. часов:

– аудиторная – 68 акад. часов;

– внеаудиторная – 1,8 акад. часов;

– самостоятельная работа – 74,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

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. 1. Угрозы безопасности в информационных системах								
1.1 Понятие "угрозы безопасности" в информационных системах. Виды угроз, классификация угроз. Определение предмета угрозы безопасности в информационных системах и вычислительных сетях. Понятие "нарушитель" в информационной системе. Модели нарушителей в информационных системах. Классификация нарушителей. Внешний и внутренний нарушитель.	7	4		4	8,2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
1.2 Планирование работ по обеспечению безопасности в информационных системах. Этапы, объем и содержание работ. Организационно-распорядительная и техническая документация для выполнения работ по защите автоматизированной системы. Техническое задание на разработку системы защиты информации и технический проект						Выполнение самостоятельного задания "Разработка технического задания на разработку системы защиты информации"	Защита самостоятельного задания "Разработка технического задания на разработку системы защиты информации"	

системы защиты информации.								
Итого по разделу		4		4	8,2			
2. 2. Виды информационной безопасности								
2.1 Виды информационной безопасности: 1. Сетевая безопасность. 2. Безопасность веб-приложений. 3. Безопасность данных. 4. Безопасность конечных устройств. 5. Облачная безопасность. 6. Безопасность интернета вещей. 7. Устойчивость к целевым кибератакам APT-группировок	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) по каждому из видов информационной безопасности с примерами реализации	Устный опрос по теме "Примеры реализации информационной безопасности"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		4		4	8			
3. 3. Безопасность конечных устройств								
3.1 Безопасность конечных устройств (рабочих мест). Угрозы безопасности рабочих мест - недоверенная загрузка, несанкционированный доступ и т.д. Модели нарушителя информационной безопасности при защите конечных устройств. Требования к комплексной защите конечных устройств.	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Рубежный контроль №1	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
3.2 Средства защиты информации для конечных устройств.		4			8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическая работа "Развертывание средства защиты информации от несанкционированного доступа"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		8		4	16			
4. 4. Сетевая безопасность								
4.1 Безопасность вычислительных сетей	7	4		4	4	Поиск дополнительной информации по заданной теме (работа с	Практическая работа "Развертывание средства межсетевого	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4

						библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	экранирования"	
4.2 Безопасность Web-приложений	7					Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическая работа "Использование Web Application Firewall (WAF)"	
4.3 Безопасность интернета вещей						Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)		
Итого по разделу		4		4	4			
5. 5. Безопасность данных								
5.1 Безопасность систем управления базами данных	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическое занятие "Безопасность данных в СУБД - защита и разграничение доступа"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
5.2 Безопасность облачных данных						Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиям	Рубежный контроль №2	

						и)		
Итого по разделу		4		4	8			
6. 6. Применение средств криптографической защиты информации (СКЗИ)								
6.1 Нормативно-правовые и методические документы, регламентирующие применение СКЗИ для защиты информации в автоматизированных системах. Состав применяемых СКЗИ и сценарии их возможного применения.	7	4		4	8	Изучение методических рекомендаций и приказов организаций-регуляторов в области криптографической защиты информации	Устный опрос	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
6.2 Использование СКЗИ для обеспечения защиты информации в автоматизированных системах						Изучение учебных пособий и технической документации по использованию СКЗИ ViPNet	Выполнение практической работы "Использование СКЗИ ViPNet Office"	
Итого по разделу		4		4	8			
7. 7. Устойчивость к целевым кибератакам APT-группировок								
7.1 Целевая кибератака как самый сложный вариант компьютерной атаки. Киберпреступность, цели киберпреступности. Наиболее распространенные сценарии и инструментарий целевых кибератак. Киберучения - командная игра по моделированию целевой кибератаки и ее отражению.	7	4		4	8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Практическое задание "Командная игра "Киберучения". Разработка сценария целевой кибератаки и методов противодействия ей"	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		4		4	8			
8. 8. Организационно-правовое обеспечение информационной безопасности								
8.1 Определение необходимого набора организационно-правовых документов и мер защиты, состава и видов средств защиты информации в соответствии с требованиями модели угроз и нормативно-правовой базы для обеспечения информационной безопасности автоматизированной системы	7	2		6	14	Выполнение индивидуального задания "Разработка перечня организационно-распорядительной документации" с решением задачи определения набора компенсирующих мер защиты	Защита индивидуального задания	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4

						информации и необходимых средств защиты информации		
Итого по разделу		2		6	14			
Итого за семестр		34		34	74,2		зао	
Итого по дисциплине		34		34	74,2		зачет с оценкой	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Технологии обеспечения информационной безопасности» 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.

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. Баланов, А. Н. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 680 с. — ISBN 978-5-507-52709-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/457463 (дата обращения: 10.03.2026). — Режим доступа: для авториз. пользователей.

2. 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: 10.03.2026).

б) Дополнительная литература:

Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 31.01.2024)

МАКРООБЪЕКТЫ:

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). - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/1858 (дата обращения: 31.01.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

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
Kaspersky Endpoint Security для бизнеса-Стандартный	Д-165-23 от 27.03.2023	27.03.2025
Ред ОС	Сертификат №01-04\22 от 06.05.2022	06.05.2025
Linux Calculate	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно
Электронные плакаты по дисциплине "Сети ЭВМ"	Д-903-13 от 14.06.2013	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Double Commander	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
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
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://host.megaprolib.net/MP0109/Web
Электронная база периодических изданий ООО «ИВИС»	https://eivis.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- 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.

Помещения для самостоятельной работы обучающихся:

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

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Технологии обеспечения информационной безопасности» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает выполнение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Контрольные вопросы и задания для проведения текущего контроля

1. Угрозы информационной безопасности в автоматизированных системах.
2. Инцидент безопасности – что это такое. Цели и задачи обработки и анализа инцидентов безопасности в автоматизированных системах.
3. Нарушитель информационной безопасности – виды и способы противодействия.
4. Организация работ по защите информации в автоматизированных системах. Этапы работ и необходимые документы.
5. Техническое задание на разработку системы защиты информации. Основные элементы.
6. Технический проект системы защиты информации.
7. Основные направления работ по защите информации в автоматизированных системах.
8. Основные угрозы для конечных устройств.
9. СЗИ для защиты конечных устройств и сценарии их применения.
10. Угрозы информационной безопасности в современных вычислительных сетях и способы их нейтрализации.
11. СЗИ для защиты вычислительной сети и сценарии их применения.
12. Безопасность Web-приложений – основные угрозы, способы и технологии организации защиты.
13. СЗИ для защиты Web-приложений и сценарии их применения.
14. Безопасность интернета вещей – основные угрозы и способы защиты от них.

15. Организация безопасной работы при использовании СУБД. Защита доступа к СУБД. Разграничение доступа к СУБД.

16. Использование и сценарии применения средств криптографической защиты информации (СКЗИ) в автоматизированных системах.

17. Применение СКЗИ для построения защищенной сети передачи данных на примере технологии ViPNet.

18. Безопасность данных при использовании облачных технологий – средства защиты информации и сценарии их применения.

19. Целевая APT-атака как самый сложный сценарий компьютерной атаки.

20. Противодействие APT-атаке. Киберучения и их формат.

Примеры практических заданий

1. Проведите аудит безопасности предложенного веб-приложения (например, используя OWASP ZAP или Burp Suite). Выявите уязвимости и разработайте рекомендации по их устранению. Определите, какие типы средств защиты информации (например, WAF, SAST/DAST инструменты) могут быть использованы для предотвращения подобных уязвимостей в будущем.

2. Оцените эффективность реализованных мер защиты информации в автоматизированной системе на примере конкретного сценария атаки (например, фишинговой атаки, атаки типа «человек посередине», SQL-инъекции). Предложите способы повышения эффективности защиты и укажите, какие дополнительные меры необходимо принять.

3. Проведите анализ соответствия системы защиты информации автоматизированной системы требованиям Федерального закона №152-ФЗ «О персональных данных» и Постановления Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Выявите несоответствия и разработайте план мероприятий по их устранению.

Вопросы к рубежному контролю

Рубежный контроль №1

1. **Основные понятия.** Дайте определения: информационная безопасность (ИБ), угроза, уязвимость, атака, риск.
2. **Свойства информации.** Раскройте триаду CIA (Конфиденциальность, Целостность, Доступность). Приведите примеры нарушения каждого свойства.
3. **Нормативное регулирование.** Какие основные законы РФ регулируют сферу ИБ? (Конституция, ГК, УК, ФЗ-149, ФЗ-152, ФЗ-187).
4. **Персональные данные (ПДн).** Что такое персональные данные по ФЗ-152? Какие требования предъявляются к операторам ПДн?
5. **Государственные регуляторы.** Функции ФСТЭК, ФСБ и Минцифры в области обеспечения ИБ.
6. **Стандартизация.** Назначение стандартов ISO/IEC 27000, ГОСТ Р серии 57558 (ISO/IEC 27001), PCI DSS.
7. **Политики и процедуры.** Роль организационно-распорядительной документации в ИБ. Из чего состоит Политика информационной безопасности?
8. **Управление инцидентами.** Что такое инцидент ИБ? Этапы реагирования на инцидент (Detection, Triage, Analysis, Containment, Eradication, Recovery, Lessons Learned).
9. **Управление уязвимостями (Vulnerability Management).** Процесс выявления, оценки и устранения уязвимостей. Сканеры уязвимостей.
10. **Пентест и Red Teaming.** Чем тестирование на проникновение отличается от аудита? Этичный хакинг.
11. **Остаточные риски и риск-менеджмент.** Понятие риска. Методы обработки риска: уклонение, снижение, передача (страхование), принятие.
12. **Физическая безопасность.** Контроль доступа в помещения, видеонаблюдение, защита от НСД к серверам.

Рубежный контроль №2

1. **Идентификация и аутентификация.** Разница понятий. Факторы аутентификации (знать, владеть, быть).

2. **Аутентификация по паролю.** Достоинства, недостатки, методы компрометации. Политика сложности паролей.

3. **Биометрическая аутентификация.** Виды (статическая, динамическая), достоинства, проблемы (частота ложных срабатываний, невозможность смены биометрических данных).

4. **Двухфакторная аутентификация (2FA/MFA).** Назначение, примеры реализации (SMS, TOTP, Push-уведомления, токены).

5. **Управление доступом (Access Control).** Модели: дискреционная (DAC), мандатная (MAC), ролевая (RBAC). Примеры реализации.

6. **Единый вход (SSO).** Понятие, протоколы (Kerberos, SAML, OAuth 2.0, OpenID Connect).

7. **Межсетевые экраны (Firewall).** Назначение, типы: пакетные фильтры, stateful inspection, Next-Generation Firewall (NGFW).

8. **Системы обнаружения и предотвращения вторжений (IDS/IPS).** Разница между IDS и IPS. Методы обнаружения (сигнатурный, поведенческий).

9. **Политики и процедуры.** Роль организационно-распорядительной документации в ИБ. Из чего состоит Политика информационной безопасности?

10. **Управление инцидентами.** Что такое инцидент ИБ? Этапы реагирования на инцидент (Detection, Triage, Analysis, Containment, Eradication, Recovery, Lessons Learned).

11. **Управление уязвимостями (Vulnerability Management).** Процесс выявления, оценки и устранения уязвимостей. Сканеры уязвимостей.

12. **Пентест и Red Teaming.** Чем тестирование на проникновение отличается от аудита? Этичный хакинг.

13. **Остаточные риски и риск-менеджмент.** Понятие риска. Методы обработки риска: уклонение, снижение, передача (страхование), принятие.

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
ПК-7: Способен разрабатывать проектные решения по защите информации в автоматизированных системах: ПК-7.1: Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах ПК-7.2: Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы ПК-7.3: Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации ПК-7.4: Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем		
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах	**Теоретические вопросы:** 1. Угрозы информационной безопасности в автоматизированных системах. 2. Инцидент безопасности – что это такое. Цели и задачи обработки и анализа инцидентов безопасности в автоматизированных системах. 3. Нарушитель информационной безопасности. Виды и способы противодействия. **Практические задания:** 1. Разработайте модель угроз безопасности информации и модель нарушителя для веб-приложения интернет-магазина, обрабатывающего персональные данные клиентов. Определите наиболее вероятные угрозы (например, SQL-инъекции, XSS, подделка межсайтовых запросов (CSRF), атаки типа «отказ в обслуживании» (DoS), кража учетных данных) и опишите потенциальные возможности и мотивацию нарушителя. Используйте методику STRIDE или аналогичную для систематизации угроз. Результат представьте в виде таблицы угроз с описанием, вероятностью и потенциальным ущербом. 2. Разработайте модель нарушителя для автоматизированной системы управления технологическим процессом (АСУ ТП) на примере системы управления электростанцией или водоканалом. Определите возможные цели и мотивы нарушителя (например, саботаж, шпионаж, вымогательство), а также его потенциальные возможности и ресурсы. Укажите, какие критические компоненты АСУ ТП могут быть подвержены атакам и какие последствия могут возникнуть.

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	**Теоретические вопросы:** 4. Организация работ по защите информации в автоматизированных системах. Этапы работ и необходимые документы. 5. Техническое задание на разработку системы защиты информации. Основные элементы. 6. Технический проект системы защиты информации. 7. Основные направления работ по защите информации в автоматизированных системах. **Практические задания:** 3. Разработайте политику парольной защиты для пользователей автоматизированной системы обработки персональных данных. Определите требования к длине, сложности, сроку действия паролей, а также правила хранения и передачи паролей. Обоснуйте выбранные требования с точки зрения обеспечения безопасности информации. 4. Определите и обоснуйте выбор комплекса мер защиты информации, подлежащих реализации в системе защиты информации корпоративной сети, включающей серверы, рабочие станции, сетевое оборудование и беспроводную сеть. Учитывайте следующие аспекты: конфиденциальность, целостность и доступность информации. Включите меры, направленные на защиту от вредоносного ПО, несанкционированного доступа, сетевых атак и утечек данных. Обоснуйте выбор каждой меры защиты и укажите соответствующие типы средств защиты информации (например, антивирусное ПО, межсетевой экран, система обнаружения вторжений, DLP-система, средства шифрования).
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	**Теоретические вопросы:** 8. Основные угрозы для конечных устройств. 9. СЗИ для защиты конечных устройств и сценарии их применения. 10. Угрозы информационной безопасности в современных вычислительных сетях и способы их нейтрализации. 11. СЗИ для защиты вычислительной сети и сценарии их применения. 12. Безопасность Web-приложений – основные угрозы, способы и технологии организации защиты. 13. СЗИ для защиты Web-приложений и сценарии их применения. 14. Безопасность интернета вещей – основные угрозы и способы защиты от них. 15. Организация безопасной работы при использовании СУБД. Защита доступа к СУБД. Разграничение доступа к СУБД.

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		Практические задания: 5. Опишите три различных типа средств защиты от DDoS-атак (например, облачные сервисы защиты, аппаратные устройства, программные решения) и сравните их по следующим критериям: стоимость, производительность, масштабируемость, сложность настройки и обслуживания. Обоснуйте, какое средство защиты будет наиболее подходящим для защиты веб-сайта крупной компании с высоким объемом трафика.
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	**Теоретические вопросы:** 16. Использование и сценарии применения средств криптографической защиты информации (СКЗИ) в автоматизированных системах. 17. Применение СКЗИ для построения защищенной сети передачи данных на примере технологии ViPNet. 18. Безопасность данных при использовании облачных технологий – средства защиты информации и сценарии их применения. 19. Целевая APT-атака как самый сложный сценарий компьютерной атаки. 20. Противодействие APT-атаке. Киберучения и их формат. **Практические задания:** 8. Разработайте структуру системы защиты информации автоматизированной системы, обрабатывающей конфиденциальную информацию. Определите состав подсистем (например, подсистема идентификации и аутентификации, подсистема контроля доступа, подсистема защиты от вредоносного ПО, подсистема мониторинга и аудита безопасности), а также взаимодействие между ними. Укажите, какие нормативные правовые документы в области защиты информации автоматизированных систем были учтены при разработке структуры. 9. Разработайте план реагирования на инциденты безопасности для организации. Определите этапы реагирования (например, обнаружение, анализ, сдерживание, восстановление, уроки), роли и обязанности сотрудников, а также процедуры оповещения и взаимодействия с внешними организациями (например, правоохранительными органами, CERT).

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

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания,

выявляющие степень сформированности умений и владений, проводится в форме зачета с оценкой.

Показатели и критерии оценивания зачета с оценкой:

– на оценку **«отлично»** – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку **«удовлетворительно»** – обучающийся прошел запланированные рубежные контроли и в ходе промежуточной аттестации должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«неудовлетворительно»** – обучающийся не прошел запланированные рубежные контроли и не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.