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
С.И. Лукьянов
_____
26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МЕТОДЫ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, АТТЕСТАЦИЯ АИС

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

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

Магнитогорск
2019 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Михайлова

Рецензент:
Начальник отдела информационной безопасности АО "КУБ",

_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 1 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 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 2022 - 2023 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 2023 - 2024 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 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

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

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Методы выявления нарушений информационной безопасности, аттестация АИС» является формирование профессиональных навыков аттестационных испытаний ОИ, изучение методик проведения аттестации, овладение методами мониторинга и аудита АС и подготовка к деятельности, связанной с аттестацией АИС в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Методы выявления нарушений информационной безопасности, аттестация АИС» рассматривает базовые теоретические понятия, средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Методы выявления нарушений информационной безопасности, аттестация АИС входит в вариативную часть учебного плана образовательной программы.

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

Организация ЭВМ и вычислительных систем
Введение в специальность
Теория информации
Информатика
Языки программирования
Теория вероятностей, математическая статистика
Математический анализ
Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Основы информационной безопасности
Дискретная математика
Теория графов и ее приложения
Исследование операций и теория игр
Математическая логика и теория алгоритмов
Программно-аппаратные средства обеспечения информационной безопасности
Математическое моделирование распределенных систем
Безопасность систем баз данных
Безопасность сетей ЭВМ
Техническая защита информации

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

Методы мониторинга информационной безопасности АС
Моделирование угроз информационной безопасности
Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Управление информационной безопасностью
Анализ рисков информационной безопасности
Методы проектирования защищенных распределенных информационных систем
Информационная безопасность систем организационного управления
Научно-исследовательская работа
Моделирование систем и процессов защиты информации
Подготовка к защите и защита выпускной квалификационной работы
Производственная-преддипломная практика

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

В результате освоения дисциплины (модуля) «Методы выявления нарушений информационной безопасности, аттестация АИС» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	
Знать	─ Средства анализа информационной безопасности; ─ Классификацию систем защиты информации; ─ Средства организации аттестации по требованиям безопасности информации.
Уметь	─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; ─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.
Владеть	─ Навыками использования средств анализа информационной безопасности; ─ Навыками проведения аттестации в соответствии с существующими нормативами.
ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем	
Знать	─ Источники и классификацию угроз информационной безопасности; ─ Основные принципы построения систем защиты информации; ─ Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.
Уметь	─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; ─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; ─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.
Владеть	─ Методами выявления угроз информационной безопасности автоматизированных систем; ─ Методами аудита уровня защищенности АИС.
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	
Знать	─ Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; ─ Принципы администрирования системы информационной безопасности автоматизированной системы.

Уметь	─ Настраивать систему информационной безопасности автоматизированной системы; ─ Настраивать подсистемы системы информационной безопасности автоматизированной системы; ─ Самостоятельно администрировать систему информационной безопасности автоматизированной системы.
Владеть	─ Навыками работы с системой информационной безопасности автоматизированной системы; ─ Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; ─ Навыками администрирования системы информационной безопасности автоматизированной системы.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

– контактная работа – 89 акад. часов:

– аудиторная – 85 акад. часов;

– внеаудиторная – 4 акад. часов

– самостоятельная работа – 55,3 акад. часов;

– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - экзамен

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. Общие положения проведения аттестационных испытаний								
1.1 Предмет и содержание дисциплины. Методы проверок и испытаний.	7	2	1/1И		1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию	Тестирование	ПК-16, ПК-26, ПСК-7.3
1.2 Цели и задачи аттестационных испытаний.		2	1/1И		1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию;	Тестирование	ПК-16, ПК-26, ПСК-7.3
Итого по разделу		4	2/2И		2			
2. Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте								

2.1 Описание и классификация объектов информатизации.	7	2	3/2И		3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию;	Тестирование	ПК-16, ПК-26, ПСК-7.3
2.2 Работы, выполняемые в ходе аттестационных испытаний АС.		2	4/2И		4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию	Тестирование	ПК-16, ПК-26, ПСК-7.3
Итого по разделу		4	7/4И		7			
3. Методики проведения аттестации								
3.1 Методика проведения аттестации информационной системы по требованиям защиты персональных данных. Подготовка отчетной документации.	7	4	5/2И		5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе	Контрольная работа	ПК-16, ПК-26, ПСК-7.3

3.2 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации.		4	6/2И		6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе	Контрольная работа	ПК-16, ПК-26, ПСК-7.3
Итого по разделу		8	11/4И		11			
4. Методика аттестационных испытаний выделенных помещений по требованиям безопасности информации								
4.1 Условия и порядок проведения аттестационных испытаний ВП.	7	2	5/2И		6,3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе	Контрольная работа	ПК-16, ПК-26, ПСК-7.3
4.2 Объемы испытаний на соответствие требованиям по защите информации для ВП. Подготовка отчетной документации.		4	6/2И		8	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе	Контрольная работа	ПК-16, ПК-26, ПСК-7.3
Итого по разделу		6	11/4И		14,3			
5. Методы выявления нарушений ИБ								

5.1 Системы и методы обнаружения вторжений	7	4	6/2И		6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию;	Тестирование	ПК-16, ПК-26, ПСК-7.3
5.2 Способы построения «образа» нормального функционирования защищаемой системы. Определение общего показателя аномальности.		4	6/2И		7	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе	Контрольная работа	ПК-16, ПК-26, ПСК-7.3
5.3 Анализ методов обнаружения злоупотреблений. Базы сигнатур атак.		4	8/4И		8	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию; подготовка к контрольной работе	Контрольная работа, тестирование	ПК-16, ПК-26, ПСК-7.3
Итого по разделу		12	20/8И		21			
6. Экзамен								

6.1 Подготовка к экзамену	7					Подготовка к экзамену; поиск дополнительной информации (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями); изучение материалов лекций	Экзамен	ПК-16, ПК-26, ПСК-7.3
Итого по разделу								
Итого за семестр		34	51/22И		55,3		экзамен	ПК-16, ПК-26, ПСК-7.3
Итого по дисциплине		34	51/22И		55,3		экзамен	ПК-16, ПК-26, ПСК-7.3

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Методы выявления нарушений информационной безопасности, аттестация АИС» 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.

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

a) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям.

b) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

c) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

d) Проблемные лекции – для ведения диалога обучающихся с преподавателем по сложным темам, для более полного раскрытия содержания проблемы по некоторым темам, а так же для развития исследовательских навыков и изучения способов решения задач;

2) Лекции-визуализации – для наглядного представления материалов курса. Лекционные занятия проводятся с использованием презентационного оборудования (проектор, экран, ноутбук), в качестве наглядных материалов используются: Web-ориентированные программные учебные материалы, электронные плакаты, презентации к лекциям.

3) Модульно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Для формирования у обучающихся основных понятий дисциплины используются:

a) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

4) Интерактивное обучение. Все лабораторные занятия проводятся в интерактивной форме. В рамках интерактивного обучения обучающихся применяются:

a) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.

b) Методы IT – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

c) Проблемное обучение – для стимулирования к самостоятельной «добыче» знаний, необходимых для решения конкретной проблемы. Для этого каждому обучающемуся выдаётся индивидуальная тема, по которой он должен составит реферат.

5) Контекстное обучение – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

a) Междисциплинарное обучение – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

6) Для приобретения новых фактических знаний и практических умений используются лабораторные занятия:

a) компьютерный практикум;

b) разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Методы выявления нарушений информационной безопасности, аттестация АИС» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

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

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, 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.

Примерные задания и вопросы по темам:

Перечень вопросов аудиторных контрольных работ по темам разделов 1-5:

1. Методики проведения аттестации ИС по требованиям защиты ПДн.
2. Цели и задачи аттестационных испытаний.
3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ.
4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ.
5. Условия и порядок проведения аттестационных испытаний объекта ВТ.
6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.
7. Объем испытаний на соответствие требованиям по ЗИ от НСД.
8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации.
9. Условия и порядок проведения аттестационных испытаний ВП.
10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП.

11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.

12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.

13. Обнаружение атак.

14. Захват сетевого трафика (механизмы захвата сетевого трафика, реализованные в специальном программно-аппаратном обеспечении, например, в Cisco Catalyst 6000 IDS Module или Cisco Secure Integrated Software),

15. Фильтрация с помощью свободно распространяемых утилит,

16. Распознавание атак (сигнатуры первого типа) с использованием утилит и библиотек.

17. DFD диаграммы потоков данных.

18. Подсистемы СОВ.

19. Обнаружение аномалий в защищаемой системе.

20. Обнаружение злоупотреблений в защищаемой системе.

21. Накопление наиболее характерной статистической информации для каждого параметра оценки.

22. Обучение нейронных сетей значениями параметров оценки.

23. Статистика Байеса.

24. Использование условной вероятности.

25. Экспертные системы.

26. Методы, основанные на моделировании поведения злоумышленника.

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**
ПК-16 - способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации		
Знать	− Средства анализа информационной безопасности; − Классификацию систем защиты информации; − Средства организации аттестации по требованиям безопасности информации.	1. Методики проведения аттестации ИС по требованиям защиты ПДн. 2. Цели и задачи аттестационных испытаний. 3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Проверка выполнения требований по защите

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		информации от утечки за счет ПЭМИ СВТ. 7. Объем испытаний на соответствие требованиям по ЗИ от НСД. 8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. 9. Условия и порядок проведения аттестационных испытаний ВП. 10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.
Уметь	– Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; – Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.	1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации 2. Произвести анализ информационных потоков, 3. Определить состав использованных для обработки защищаемой информации средств ВТ. 4. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Определить условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ СВТ. 7. Построить DFD диаграмму потоков данных предприятия/организации.
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками проведения аттестации в соответствии с существующими нормативами.	1. Определить объем испытаний на соответствие требованиям по ЗИ от НСД. 2. Произвести проверку ВП на соответствие организационно-техническим требованиям по защите информации. 3. Определить условия и порядок проведения аттестационных испытаний ВП. 4. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		5. Определить объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 6. Произвести проверку выполнения требований по защите информации от утечки по акустическому и виброакустическому каналам для ВП.
ПК-26 - способностью администрировать подсистему информационной безопасности автоматизированной системы		
Знать	− Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; − Принципы администрирования системы информационной безопасности автоматизированной системы.	1. Методики проведения аттестации ИС по требованиям защиты ПДн. 2. Цели и задачи аттестационных испытаний. 3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ. 7. Объем испытаний на соответствие требованиям по ЗИ от НСД. 8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. 9. Условия и порядок проведения аттестационных испытаний ВП. 10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний. 13. Обнаружение аномалий в защищаемой системе. 14. Обнаружение злоупотреблений в защищаемой

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		системе. 15. Накопление наиболее характерной статистической информации для каждого параметра оценки. 16. Обучение нейронных сетей значениями параметров оценки. 17. Статистика Байеса. 18. Использование условной вероятности. 19. Экспертные системы. 20. Методы, основанные на моделировании поведения злоумышленника.
Уметь	− Настраивать систему информационной безопасности автоматизированной системы; − Настраивать подсистемы системы информационной безопасности автоматизированной системы; − Самостоятельно администрировать систему информационной безопасности автоматизированной системы.	1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации. 2. Произвести анализ информационных потоков. 3. Определить состав использованных для обработки защищаемой информации средств ВТ. 4. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Определить условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.
Владеть	− Навыками работы с системой информационной безопасности автоматизированной системы; − Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; − Навыками	1. Определить объем испытаний на соответствие требованиям по ЗИ от НСД. 2. Произвести проверку ВП на соответствие организационно-техническим требованиям по защите информации. 3. Определить условия и порядок проведения аттестационных испытаний ВП. 4. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 5. Определить объем испытаний на соответствие требованиям по защите информации от утечки по

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	администрирования системы информационной безопасности автоматизированной системы.	акустическому и виброакустическому каналам для ВП. 6. Произвести проверку выполнения требований по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 7. Произвести фильтрацию трафика сети с помощью свободно распространяемых утилит
ПСК-7.3 - способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем		
Знать	− Источники и классификацию угроз информационной безопасности; − Основные принципы построения систем защиты информации; − Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	1. Методики проведения аттестации ИС по требованиям защиты ПДн. 2. Цели и задачи аттестационных испытаний. 3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ. 7. Объем испытаний на соответствие требованиям по ЗИ от НСД. 8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. 9. Условия и порядок проведения аттестационных испытаний ВП. 10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.

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

б) 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 экзамена.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Внуков, А.А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е и
доп. — Москва: Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-5
Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772(дата обращения: 24.02

б) Дополнительная литература:

1. Брюхомицкий, Ю.А. Искусственные иммунные системы в информационной безопасн
пособие / Ю. А. Брюхомицкий; Южный федеральный университет. - Ростов-на-Дону; Таганрог
Южного федерального университета, 2019. - 147 с. - ISBN 978-5-9275-3212-4. - Текст: электр
https://new.znanium.com/catalog/product/1088177 (дата обращения: 26.02.2020)

2. Веселов, Г.Е. Менеджмент риска информационной безопасности: Учебное пособие /
Абрамов Е.С., Шилов А.К. - Таганрог: Южный федеральный университет, 2016. - 107 с.: ISBN 978-5
Текст: электронный. - URL: https://new.znanium.com/catalog/product/997108 (дата обращения: 26.02.2

3. Сетевая защита информации. Лабораторный практикум: учебное пособие [для вузов] / Д
др.]; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Н
CD-ROM. - Загл. с титул. экрана. -
https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824
(дата обращения: 22.10.2019). - Макрообъект. - ISBN 978-5-9967-1605-0. - Текст: электронны
доступны также на CD-ROM.

в) Методические указания:

1. Методические указания по выполнению лабораторных работ (Приложение 1)
2. Методические указания по выполнению внеаудиторных самостоятельных работ (Прилож

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
Adobe Audition CS 5.5 Academic Edition	К-615-11 от 12.12.2011	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows Server(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
eTokenSecurLogon for Oracle	К-271-12 от 16.10.2012	бессрочно
СЗИ Страж NT в.3	К-271-12 от 16.10.2012	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название ресурса	Ссылка
Сетевой ресурс (Сайт ФСТЭК)	URL: www.fstec.ru
Сетевой ресурс (Сайт РОССТАНДАРТ)	URL: https://www.rst.gov.ru/port
Банк данных угроз безопасности информации ФСТЭК России	URL: https://bdu.fstec.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)
Компьютерные классы (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)
Лаборатория технической защиты информации, ауд. 226:
-АКС-1301 Анализатор спектра
-Комплекс радиомониторинга "Касандра К6"
-Комплекс радиомониторинга "Касандра К21"
-Генератор шума стационарный "ГШ-1000-М"
-Система виброакустической и акустической защиты "Соната-АВ"
-Устройство защиты телефонных переговоров от про-слушивания и записи "Прокруст-200"

Аудитории для самостоятельной работы (ауд.132а): компьютерные классы; читальные залы библиотеки

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Рекомендации направлены на оказание методической помощи студентам при выполнении лабораторных занятий.

Лабораторное занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение лабораторных навыков решения типовых и прикладных задач.

Целью лабораторных занятий является формирование и отработка лабораторных умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами лабораторных занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных лабораторных знаний по конкретным темам дисциплин различных циклов;
- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных прикладных задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем лабораторных работ определяется рабочей программой дисциплины. План лабораторных занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура лабораторного занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущей лабораторной работы, ставится ее цели и задачи, проводиться инструктаж по технике безопасности выполнения работы, проверяется исходный уровень готовности студентов к лабораторной работе (выполнение тестов, контрольные вопросы и т.п.), выдается порядок и условия выполнения лабораторной работы.

На лабораторном занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении лабораторных работ

Общие правила:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения лабораторных работ

При подготовке к выполнению лабораторных работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Лабораторная работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют лабораторные работы во внеурочное время.

После выполнения каждой лабораторной работы студент демонстрирует результат выполнения преподавателю в виде отчета по лабораторной работе и отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки лабораторных работ.

Правила оформления результатов и оценивания лабораторной работы

Результаты выполненной лабораторной работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагаются следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.