МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## МЕТОДЫ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, АТТЕСТАЦИЯ АИС

наименование дисциплины

Специальность
**10.05.03 Информационная безопасность автоматизированных систем**
шифр наименование специальности

Специализация программы
**Обеспечение информационной безопасности распределенных информационных систем**
наименование специализации

Уровень высшего образования
**специалитет**

Форма обучения
**очная**

| | |
|---|---|
| Институт | Энергетики и автоматизированных систем |
| Кафедра | Информатики и информационной безопасности |
| Курс | 4 |
| Семестр | 7 |

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
*(наименование кафедры - разработчика)*

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
*(подпись) (И.О. Фамилия)*

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
*(наименование факультета (института) - исполнителя)*

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
*(подпись) (И.О. Фамилия)*

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
*(должность, ученая степень, ученое звание)*

_____ / И.И. Баранкова /
*(подпись) (И.О. Фамилия)*

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
*(должность, ученая степень, ученое звание)*

_____ / Г.Н. Чусавитина/
*(подпись) (И.О. Фамилия)*

**Лист регистрации изменений и дополнений**

| № п/п | Раздел программы | Краткое содержание изменения/дополнения | Дата, № протокола заседания кафедры | Подпись зав. кафедрой |
|---|---|---|---|---|
| 1. | 7 | Переработка фонда оценочных средств | № 1 от 07.09.2019 | |
| 2. | 8 | Обновление списка основной и дополнительной литературы | № 1 от 07.09.2019 | |
| 3. | 7 | Переработка фонда оценочных средств | № 1 от 04.09.2020 | |
| 4. | 8 | Обновление списка основной и дополнительной литературы | № 1 от 04.09.2020 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

1. **Цели освоения дисциплины**

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 в структуре образовательной программы подготовки специалиста**

Дисциплина «Методы выявления нарушений информационной безопасности, аттестация АИС» входит в вариативную часть блока 1 образовательной программы.

Успешное усвоение материала предполагает знание обучающимися основных положений курсов «Введение в специальность», «Основы информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Техническая защита информации», «Безопасность сетей ЭВМ».

Дисциплина является предшествующей для изучения дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем», «Моделирование угроз информационной безопасности», «Информационная безопасность распределенных информационных систем».

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

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

| Структурный элемент компетенции | Планируемые результаты обучения |
|---|---|
| **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;<br>– Классификацию систем защиты информации;<br>– Средства организации аттестации ВП по требованиям безопасности информации. |
| **Уметь** | – Принимать участие в исследованиях аттестации системы защиты информации;<br>– Принимать участие в исследованиях и анализе аттестации системы защиты информации;<br>– Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности. |
| **Владеть** | – Навыками использования средств анализа информационной безопасности;<br>– Навыками участия в проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности;<br>– Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами. |
| **ПК-26 - способностью администрировать подсистему информационной безопасности автоматизированной системы.** | |
| **Знать** | – Основные принципы работы системы информационной безопасности автоматизированной системы;<br>– Основные принципы работы всех подсистем системы информационной безопасности автоматизированной системы;<br>– Принципы администрирования системы информационной безопасности автоматизированной системы. |
| **Уметь** | – Настраивать систему информационной безопасности автоматизированной системы;<br>– Настраивать подсистемы системы информационной безопасности автоматизированной системы;<br>– Самостоятельно администрировать систему информационной безопасности автоматизированной системы. |
| **Владеть** | – Навыками работы с системой информационной безопасности автоматизированной системы;<br>– Навыками работы с подсистемами системы информационной безопасности автоматизированной системы;<br>– Навыками администрирования системы информационной безопасности |

| Структурный элемент компетенции | Планируемые результаты обучения |
|---|---|
| | автоматизированной системы. |
| **ПСК-7.3 - способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем.** | |
| **Знать** | – Источники и классификацию угроз информационной безопасности;<br>– Основные принципы построения систем защиты информации;<br>– Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. |
| **Уметь** | – Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;<br>– Участвовать в проведении мониторинга угроз безопасности автоматизированных систем;<br>– Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем. |
| **Владеть** | – Методами выявления угроз информационной безопасности автоматизированных систем;<br>– Методами мониторинга и аудита угроз информационной безопасности автоматизированных систем;<br>– Методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. |

**Структура 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. часов;

Форма аттестации:

- 7 семестр – экзамен.

| Раздел/ тема дисциплины | Семестр | Аудиторная | | Самостоятельная работа (в акад. часах) | Вид самостоятельной работы | Форма текущего контроля успеваемости и промежуточной аттестации | Код и структурный элемент компетенции |
|---|---|---|---|---|---|---|---|
| | | Лекции | Лаборат. Занятия | | | | |
| **Раздел 1. Общие положения проведения аттестационных испытаний** | | | | | | | |
| Тема 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 библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию | тестирование | ПК-16 з ПК-26 з ПСК-7.3 з |
| Тема 1.2. Цели и задачи аттестационных испытаний. | 7 | 2 | 1/1И | 1 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-1, тестирование | ПК-16 з ПК-26 з ПСК-7.3 з |
| Итого по разделу | | 4 | 2/2И | 2 | | | |
| **Раздел 2. Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте** | | | | | | | |

| Раздел/ тема дисциплины | Семестр | Аудиторная | | Самостоятельная работа (в акад. | Вид самостоятельной работы | Форма текущего контроля успеваемости и промежуточной аттестации | Код и структурный элемент |
|---|---|---|---|---|---|---|---|
| | | Лекции | Лаборат. Занятия | | | | |
| Тема 2.1. Описание и классификация объектов информатизации. | 7 | 2 | 3/2И | 3 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-2; тестирование | ПК-16 зу ПК-26 зу ПСК-7.3 зу |
| Тема 2.2. Работы, выполняемые в ходе аттестационных испытаний АС. | 7 | 2 | 4/2И | 4 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию | тестирование | ПК-16 зу ПК-26 зу ПСК-7.3 зу |
| Итого по разделу | | 4 | 7/4И | 7 | | | |
| **Раздел 3. Методики проведения аттестации** | | | | | | | |
| Тема 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 библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-3; тестирование | ПК-16 зу ПК-26 зу ПСК-7.3 зу |
| Тема 3.2. Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации. | 7 | 4 | 6/2И | 6 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-4; тестирование | ПК-16 зув ПК-26 зув ПСК-7.3 зув |
| Итого по разделу | | 8 | 11/4И | 11 | | | |
| **Раздел 4. Методика аттестационных** | | | | | | | |

| Раздел/ тема дисциплины | Семестр | Аудиторная | | Самостоятельная работа (в акад. | Вид самостоятельной работы | Форма текущего контроля успеваемости и промежуточной аттестации | Код и структурный элемент |
|---|---|---|---|---|---|---|---|
| | | Лекции | Лаборат. Занятия | | | | |
| **испытаний выделенных помещений по требованиям безопасности информации** | | | | | | | |
| Тема 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 библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-5; тестирование | ПК-16 зу ПК-26 зу ПСК-7.3 зу |
| Тема 4.2 Объемы испытаний на соответствие требованиям по защите информации для ВП. Подготовка отчетной документации. | 7 | 4 | 6/2И | 8 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-6; тестирование | ПК-16 зув ПК-26 зув ПСК-7.3 зув |
| Итого по разделу | | 6 | 11/4И | 14,3 | | | |
| **Раздел 5. Методы выявления нарушений ИБ** | | | | | | | |
| Тема 5.1 Системы и методы обнаружения вторжений | | 2 | 3/1И | 3 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-7; тестирование | ПК-16 зу ПК-26 зу ПСК-7.3 зу |
| Тема 5.2 Методы обнаружения вторжений | | 2 | 3/1И | 3 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной | АКР-8; тестирование | ПК-16 зув ПК-26 зув ПСК-7.3 зув |

| Раздел/ тема дисциплины | Семестр | Аудиторная | | Самостоятельная работа (в акад. | Вид самостоятельной работы | Форма текущего контроля успеваемости и промежуточной аттестации | Код и структурный элемент |
|---|---|---|---|---|---|---|---|
| | | Лекции | Лаборат. Занятия | | | | |
| | | | | | работе | | |
| Тема 5.3 Способы построения «образа» нормального функционирования защищаемой системы | | 2 | 3/1И | 3 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-9; тестирование | ПК-16 зув ПК-26 зув ПСК-7.3 зув |
| Тема 5.4 Определение общего показателя аномальности | | 2 | 3/1И | 4 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-10; тестирование | ПК-16 зув ПК-26 зув ПСК-7.3 зув |
| Тема 5.5 Анализ методов обнаружения злоупотреблений | | 2 | 4/2И | 4 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-11; тестирование | ПК-16 зув ПК-26 зув ПСК-7.3 зув |
| Тема 5.6 Базы сигнатур атак. | | 2 | 4/2И | 4 | Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе | АКР-12; тестирование | ПК-16 зув ПК-26 зув ПСК-7.3 зув |
| Итого по разделу | | 12 | 20/8И | 21 | | | |
| Подготовка к экзамену | | | | 35,7 | | **Промежуточная аттестация** | |

| Раздел/ тема дисциплины | Семестр | Аудиторная | | Самостоятельная работа (в акад. | Вид самостоятельной работы | Форма текущего контроля успеваемости и промежуточной аттестации | Код и структурный элемент |
|---|---|---|---|---|---|---|---|
| | | Лекции | Лаборат. Занятия | | | | |
| | | | | | | (экзамен) | |
| **Итого за семестр** | | **34** | **51/22 И** | **91** | | **Промежуточная аттестация (экзамен)** | ПК-16 зув ПК-26 зув ПСК-7.3 зув |
| **Итого по дисциплине** | | **34** | **51/22 И** | **91** | | **Промежуточная аттестация (экзамен)** | ПК-16 зув ПК-26 зув ПСК-7.3 зув |

## 5 Образовательные и информационные 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 | 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;<br>– Классификацию систем защиты | 1. Методики проведения аттестации ИС по требованиям защиты ПДн.<br>2. Цели и задачи аттестационных испытаний.<br>3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, |

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

| Структурный элемент | Планируемые результаты обучения | Оценочные средства |
|---|---|---|
| | АС с учетом требований к обеспечению информационной безопасности;<br>– Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами. | информации от утечки за счет ПЭМИ ОТСС для ВП.<br>5. Определить объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.<br>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;<br>– Основные принципы работы всех подсистем системы информационной безопасности автоматизированной системы;<br>– Принципы администрирования системы информационной безопасности автоматизированной системы. | 1. Методики проведения аттестации ИС по требованиям защиты ПДн.<br>2. Цели и задачи аттестационных испытаний.<br>3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ.<br>4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ.<br>5. Условия и порядок проведения аттестационных испытаний объекта ВТ.<br>6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.<br>7. Объем испытаний на соответствие требованиям по ЗИ от НСД.<br>8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации.<br>9. Условия и порядок проведения аттестационных испытаний ВП.<br>10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП.<br>11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.<br>12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.<br>13. Обнаружение аномалий в защищаемой системе.<br>14. Обнаружение злоупотреблений в защищаемой системе.<br>15. Накопление наиболее характерной статистической информации для каждого параметра оценки.<br>16. Обучение нейронных сетей значениями параметров оценки. |

| Структурный элемент | Планируемые результаты обучения | Оценочные средства |
|---|---|---|
| | | 17. Статистика Байеса.<br>18. Использование условной вероятности.<br>19. Экспертные системы.<br>20. Методы, основанные на моделировании поведения злоумышленника. |
| **Уметь** | – Настраивать систему информационной безопасности автоматизированной системы;<br>– Настраивать подсистемы системы информационной безопасности автоматизированной системы;<br>– Самостоятельно администрировать систему информационной безопасности автоматизированной системы. | 1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации.<br>2. Произвести анализ информационных потоков.<br>3. Определить состав использованных для обработки защищаемой информации средств ВТ.<br>4. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ.<br>5. Определить условия и порядок проведения аттестационных испытаний объекта ВТ.<br>6. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ СВТ. |
| **Владеть** | – Навыками работы с системой информационной безопасности автоматизированной системы;<br>– Навыками работы с подсистемами системы информационной безопасности автоматизированной системы;<br>– Навыками администрирования системы информационной безопасности автоматизированной системы. | 1. Определить объем испытаний на соответствие требованиям по ЗИ от НСД.<br>2. Произвести проверку ВП на соответствие организационно-техническим требованиям по защите информации.<br>3. Определить условия и порядок проведения аттестационных испытаний ВП.<br>4. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП.<br>5. Определить объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.<br>6. Произвести проверку выполнения требований по защите информации от утечки по акустическому и виброакустическому каналам для ВП.<br>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 | 1. Методики проведения аттестации ИС по требованиям защиты ПДн.<br>2. Цели и задачи аттестационных испытаний.<br>3. Описание технологического процесса обработки и хранения |

| Структурный элемент | Планируемые результаты обучения | Оценочные средства |
|---|---|---|
| | безопасности;<br>– Основные принципы построения систем защиты информации;<br>– Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. | конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ.<br>4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ.<br>5. Условия и порядок проведения аттестационных испытаний объекта ВТ.<br>6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.<br>7. Объем испытаний на соответствие требованиям по ЗИ от НСД.<br>8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации.<br>9. Условия и порядок проведения аттестационных испытаний ВП.<br>10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП.<br>11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.<br>12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний. |
| **Уметь** | – Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;<br>– Участвовать в проведении мониторинга угроз безопасности автоматизированных систем;<br>– Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем. | 1. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации<br>2. Произвести анализ информационных потоков<br>3. Определить состав использованных для обработки защищаемой информации средств ВТ.<br>4. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ.<br>5. Определить условия и порядок проведения аттестационных испытаний объекта ВТ.<br>6. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ СВТ. |
| **Владеть** | – Методами выявления угроз информационной безопасности автоматизированных систем;<br>– Методами мониторинга и | 1. Определить объем испытаний на соответствие требованиям по ЗИ от НСД.<br>2. Произвести проверку ВП на соответствие организационно-техническим требованиям по защите информации.<br>3. Определить условия и порядок проведения аттестационных испытаний ВП.<br>4. Произвести проверку выполнения требований по защите |

| Структурный элемент | Планируемые результаты обучения | Оценочные средства |
|---|---|---|
| | аудита угроз информационной безопасности автоматизированных систем;<br>– Методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. | информации от утечки за счет ПЭМИ ОТСС для ВП.<br>5. Определить объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.<br>6. Произвести проверку выполнения требований по защите информации от утечки по акустическому и виброакустическому каналам для ВП. |

***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)

### Основная литература

**а) Основная литература:**

**1.** Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - Режим доступа: http://znanium.com/bookread.php?book=405000. - Загл. с экрана. - ISBN 978-5-369-01178-2.

**б) Дополнительная литература:**

**1.** Информационная безопасность и защита информации [Текст]: учеб.пособ. / Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова, Н. Г. Шахов. - Старый Оскол: ТНТ, 2010.

**2.** Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 101 с. - Режим доступа: http://znanium.com/bookread.php?book=463061 .- Загл. с экрана.

**3.** Агапов, А. В. Обработка и обеспечение безопасности электронных данных [Электронный ресурс]: учеб. пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. - М.: МФПУ Синергия, 2012. - 592 с. - (Сдаем госэкзамен). - Режим доступа: http://znanium.com/bookread.php?book=451354 .- Загл. с экрана. - ISBN 978-5-4257-0074-2.

**в) Программное обеспечение и Интернет-ресурсы:**

**1.** Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.

**2.** Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

**3.** Государственная публичная научно-техническая библиотека России [Электронный ресурс] – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.

**4.** Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз. рус.

**5.** Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.

**6.** Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.

**7.** ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/.– Загл. с экрана. Яз. рус.

## 9. Материально-техническое обеспечение дисциплины

| Тип и название аудитории | Оснащение аудитории |
|---|---|
| Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.) | Мультимедийные средства хранения, передачи и представления информации |
| Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.) | Персональные компьютеры с ПО:<br>- Операционная система MS Windows - *Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021* ;<br>- Пакет MS Office 2007 (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*;<br>- Архиватор 7zip - *GNU LGPL, бессрочная*;<br>- Система компьютерной математики MathCad - *43813518 D-1662-13 от 22.11.2013*;<br>- выход в Интернет. |
| Лаборатория радиомониторинга и | Комплекс радиомониторинга «Касандра К-6»; |

| Тип и название аудитории | Оснащение аудитории |
|---|---|
| контроля утечек информации, ауд. 226 | Комплекс радиомониторинга «Касандра К-21»;<br>Анализатор спектра «АКС-1301»;<br>Комплект учебного оборудования «Беспроводные компьютерные сети ЭВМ»; |
| Аудитории для самостоятельной работы (ауд.132а): компьютерные классы; читальные залы библиотеки | Персональные компьютеры с ПО:<br>- Операционная система MS Windows - *Microsoft Imagine - Premium D-1227-18 от 08.10.2018 до 08.10.2021* ;<br>- Пакет MS Office 2007 (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*;<br>- Архиватор 7zip - *GNU LGPL, бессрочная*;<br>- Выход в Интернет и с доступ в электронную информационно-образовательную среду университета |

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03 Информационная безопасность автоматизированных систем. Специализация «Обеспечение информационной безопасности распределенных информационных систем».*