Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

**«УТВЕРЖДАЮ»**
**И.о. проректора**
**_____ А.В. Троицкий**
**«___»_____2023 г.**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ**
**И ТЕХНОЛОГИЙ**
**КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

# РАБОЧАЯ ПРОГРАММА
# ДИСЦИПЛИНЫ (МОДУЛЯ)

# Ф.Т.Д.В.02 «ОРГАНИЗАЦИЯ СПЕЦ ПРОВЕРОК И СПЕЦ ИССЛЕДОВАНИЙ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

**Направление подготовки: 10.04.01 - Информационная безопасность**
**Направленность (профиль): Менеджмент информационной безопасности**
**Уровень высшего образования: Магистратура**
**Форма обучения: очная**

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

**Автор: Вихров А.П.. Рабочая программа дисциплины: Организация спец проверок и спец исследований объектов информационной безопасности. – Королев МО: «Технологический Университет», 2023**

Рецензент: Воронов А.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по 10.04.01 направление подготовки - Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

**Рабочая программа рассмотрена и одобрена на заседании кафедры:**

| | | | | |
|---|---|---|---|---|
| Заведующий кафедрой (ФИО, ученая степень, звание, подпись) | Соляной В.Н. к.в.н., доцент | | | |
| Год утверждения (переутверждения) | 2023 | 2024 | | |
| Номер и дата протокола заседания кафедры | №8 от 29.03.2023г. | | | |

**Рабочая программа согласована:**
**Руководитель ОПОП ВО** Сухотерин А.И.

**Рабочая программа рекомендована на заседании УМС:**

| | | | | |
|---|---|---|---|---|
| Год утверждения (переутверждения) | 2023 | 2024 | | |
| Номер и дата протокола заседания УМС | №5 от 11.04.2023г. | | | |

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

**Целью изучения дисциплины** является углубленное изучение

теоретических и прикладных основ социальной инженерии как научной дисциплины, связанной с созданием средств и методов выработки научно обоснованных управленческих решений в области информационной безопасности

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

**Профессиональные компетенции:**

- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении

- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.

. **Основными задачами дисциплины** являются:

- раскрытие сущности, целей социальной инженерии (СИ) как метода несанкционированного доступа к информации или системам хранения информации без использования технических средств;
- определение общих методологических подходов построения систем защиты информации с учетом возможных атак с использованием технологии социальной инженерии;
- освоение методических подходов, установления состава защищаемой информации и выявления объектов защиты, подверженных атакам со стороны социального хакерства;
- выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников, использующих методы социальной инженерии);
- овладение методами оценки уязвимости защищаемой информации;
- определение методов выявления параметров и структуры систем защиты информации;
- освоение методов установления целесообразного состава мероприятий по защите информации от социального хакерства;

определение методологических подходов оценки эффективности мер по защите информации от воздействия со стороны

Показатель освоения компетенции отражают следующие индикаторы:

**Трудовые действия:**

- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.

- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

**Необходимые умения:**

- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

**Необходимые знания:**

- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

## 1. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина относится к факультативам основной профессиональной образовательной программы подготовки магистров по направлению подготовки «Информационная безопасность».

Дисциплина базируется на ранее изученных дисциплинах «Специальные разделы физики», «Специальные разделы математики», «Защищенные информационные системы», «Основы теории информационной безопасности» и компетенциях: УК-1; УК-2; УК-4; ОПК-1; ОПК-2; и ПК-1; ПК-3.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин общенаучного цикла «Комплексная проверка информационной безопасности», «Концептуальное проектирование технологий обеспечения информационной безопасности», и для написания магистерской диссертации.

## 2. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа

**Таблица 1**

| **Виды занятий** | **Всего часов** | **Семестр 2** | **Семестр …** | **Семестр …** | **Семестр …** |
|---|---|---|---|---|---|
| **Общая трудоемкость** | **72** | **72** | | | |
| **ОЧНАЯ ФОРМА ОБУЧЕНИЯ** | | | | | |
| **Аудиторные занятия** | **40** | **40** | | | |
| Лекции (Л) | **16** | **16** | | | |
| Практические занятия (ПЗ) | **24** | **24** | | | |
| Лабораторные работы (ЛР) | **нет** | **нет** | | | |
| Практическая подготовка | **4** | **4** | | | |
| **Самостоятельная работа** | **32** | **32** | | | |
| *Курсовые работы (проекты)* * | | | | | |
| *Расчетно-графические работы** | | | | | |
| *Контрольная работа* * | | | | | |
| *Текущий контроль знаний* * | **Тест** | **Тест** | | | |
| **Вид итогового контроля** | **Зачет** | **Зачет** | | | |

# 4. Содержание дисциплины

## 4.1.Темы дисциплины и виды занятий

**Таблица 2**

| Наименование тем | Лекции, час. Очно | Практические занятия, час. Очно | Занятия в интерактивной форме, час. Очно | Практическая поготовка ,час | Код компетенций |
|---|---|---|---|---|---|
| Раздел I. Обеспечение безопасного допуска к информационным ресурсам | | | | | |
| Тема 1. Введение. Место и роль дисциплины в процессе подготовки специалиста, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература | 1 | 1 | - | | ПК-2, |
| Тема 2. Функции, состав, структура и задачи государственной системы защиты информации | 1 | 1 | - | | ,ПК-2 |
| Тема 3. Нормативно-методические документы ФСТЭК России в области аттестации объектов информатизации | 1 | 1 | - | | ПК-2, |
| Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств ЗИ (СЗИ) и проведение аттестации объектов информатизации | 1 | 1 | - | | ПК-2;3, |
| Тема 5. Основные положения законодательства в области защиты информации | 1 | 1 | - | | ПК-3, |
| Тема 6. Содержание мероприятий на стадии проектирования и | 1 | 1 | - | | ПК-2;3,5 |

| | | | | | |
|---|---|---|---|---|---|
| создания объекта информатизации и системы защиты информации в его составе | | | | | |
| Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации | 1 | 1 | - | | ПК-2;3, |
| Тема 8. Проведение аттестация объектов информатизации (ОИ) | 1 | - | - | | ПК-3, |
| Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации | 1 | 2 | 1 | | ПК-2;3, |
| Тема 10. Этапы практического проведения работ по аттестации объектов информатизации | 1 | 2 | 1 | | ПК-;3, |
| Тема 11. Проверка и испытание аттестуемого объекта информатизации | 1 | 2 | 1 | | ПК-2;3, |
| Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам | 1 | 2 | 1 | | ПК-2;3, |
| Тема 13. Пассивные и активные методы защиты объектов информатизации | 1 | 2 | - | 1 | ПК-2, |
| Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке | 1 | 2 | - | 1 | ПК-3, |
| Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа | 1 | 2 | 1 | 1 | ПК-2;3, |
| Тема 16. Методики оценки защищённости объектов информатизации | 1 | 2 | 1 | 1 | ПК-2;3, |
| Итого: | 16 | 24 | 6 | 4 | |

## 4.2. Содержание тем дисциплины

**Тема 1. Введение. Место и роль дисциплины в процессе подготовки специалиста, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература**

Значение, предмет изучения и краткое содержание курса «Аттестация объектов информации». Место дисциплины среди других курсов, изучаемых студентами. Методы изучения дисциплины. Названия тем, распределение их по видам аудиторных занятий. Форма проверки знаний. Научная, учебная и периодическая литература по дисциплине. Знания, умения и компетенции, которые должны быть приобретены студентами в процессе изучения дисциплины. Раскрытие основных понятий по аттестации объектов информации применительно к изучению курса. Нормативно-методические документы, регулирующие вопросы аттестации объектов информатизации.

**Тема 2. Функции, состав, структура и задачи государственной системы защиты информации (ГСЗИ).**

Что такое ГСЗИ, ее функции, состав, структура и задачи.

Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.

Функции федерального органа по сертификации и аттестации.

Функции органов по аттестации.

**Тема 3. Нормативно-методические документы ФСТЭК России и национальные стандарты в области аттестации объектов информатизации**

Содержание Положения о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 27.10.1995 № 199.

Содержание Положения по аттестации объектов информатизации по требованиям безопасности информации.

Содержание Положения об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25.11.1994.

Содержание Типового положения об испытательной лаборатории, утвержденное председателем Гостехкомиссии России 25.11.1994.

Содержание руководящих документов Гостехкомиссии России в области аттестации объектов информатизации. Основное содержание Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К). Основное содержание Сборника временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам.

Основное содержание Требований к системам обнаружения вторжений, утверждённых приказом ФСТЭК России от 06.12.2011 № 638.

Основное содержание Сборника методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи, утверждённого приказом ФСТЭК России от 15.03.2012 № 27. Основное содержание Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.

Содержание Положения о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 05.02.2010 № 58 (зарегистрирован Минюстом России 19.02.2010, регистрационный № 16456).

Содержание Порядка проведения классификации информационных систем

персональных данных. Утверждено приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Содержание Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Содержание национальных стандартов в области аттестации объектов информатизации.

**Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств ЗИ и проведение аттестации объектов информатизации**

Содержание Федерального закона от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности».

Содержание Приказа ФСТЭК России от 12.07.2012 № 83 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации". Содержание Приказ ФСТЭК России от 12.07.2012 № 84 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации"

Содержание Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Содержание Положения по аттестации объектов информатизации по требованиям безопасности информации.

**Тема 5. Основные положения законодательства в области защиты информации**

Основное содержание Закона Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности». Основное содержание Закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации». Основное содержание Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Основное содержание Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Содержание Указа Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

**Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе**

Организация работ по защите информации в ходе создания и эксплуатации объектов информатизации и их систем защиты информации.

Выполняемые работы на предпроектной стадии по обследованию объекта информатизации; содержание аналитического обоснования необходимости создания системы защиты информации; содержание технического задания на разработку системы защиты информации; содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе.

**Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации (КИ)**

Основные требования и рекомендации по защите речевой КИ.

Защита КИ, циркулирующей с системах звукоусиления и звукового сопровождения.

Основное содержание и требования СНиП 23-03-2003. Защита от шума.

**Тема 8. Проведение аттестация объектов информатизации (ОИ)**

Порядок проведения аттестации защищаемого помещения по требованиям защиты конфиденциальной информации.

Порядок проведения аттестации объекта вычислительной техники по требованиям защиты конфиденциальной информации.

**Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации**

Перечень работ по подготовке объекта информатизации к аттестации.

Оформление заявки на аттестацию объекта информатизации и документы, предоставляемые для предварительного ознакомления с аттестуемым объектом и разрабатываемые для осуществления начала аттестации.

Перечень документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.

Перечень документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

**Тема 10. Этапы практического проведения работ по аттестации объектов информатизации**

Контрольно-измерительное оборудование, применяемое для аттестации защищаемых помещений по требованиям безопасности информации.

Последовательность проведения работ по аттестации защищаемых помещений.

Контрольно-измерительное оборудование, применяемое для аттестации объектов вычислительной техники по требованиям безопасности информации.

Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

**Тема 11. Проверка и испытание аттестуемого объекта информатизации**

Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.

Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.

Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

**Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам**

Содержание работ по поставке средств защиты информации от утечки по техническим каналам.

Содержание работ по установке средств защиты информации от утечки по техническим каналам и обеспечению эффективности их функционирования в процессе эксплуатации аттестованных объектов информатизации.

**Тема 13. Пассивные и активные методы защиты объектов информатизации**

Содержание Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 № 58.

Рекомендации по обеспечению ЗИ содержащиеся в негосударственных информационных ресурсах при взаимодействии пользователей с информационными сетями общего пользования.

**Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке**

Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

**Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа**

Общие требования и рекомендации по защиты информации (ЗИ) в автоматизированных системах (АС). Основные требования и рекомендации по ЗИ.

Методика формирования комплекса мероприятий по защите информационных систем в условиях возможного воздействия злоумышленников.

Определение структуры и точек доступа сетевого периметра организации с помощью контрольно-измерительной аппаратуры.

Применение сканеров безопасности для поиска уязвимостей сетевого периметра организации.

**Тема 16. Методики оценки защищённости объектов информатизации**

Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.

Методика оценки защищённости ОТСС от утечки конфиденциальной информации (КИ) за счёт наводок на токоведущие коммуникации.

Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований.

## 5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

## 6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Организация спец. проверок и спец исследований объекта информационной безопасности» приведена в Приложении 1.

## 7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

***Основная литература***

1.Математическое моделирование технических систем: учебник / В.П. Тарасик. — Минск: Новое знание; М.: ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат) [электронный ресурс] // Режим доступа: http://znanium.com/catalog/product/952123

***Дополнительная литература***

2.Аверченков В.И. Основы математического моделирования технических систем / В.И. Аверченков, В.П. Федоров, М.Л. Хейфец. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 271 с.: схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93344

3. Голубева Н. В. Математическое моделирование систем и процессов: учебное пособие / Н. В. Голубева. — 2-е изд., стер. — Санкт-Петербург: Лань, 2016. — 192 с. — ISBN 978-5-8114-1424-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/76825

Вариант-2

***Основная литература***

1. Чернышов В.Н. Моделирование информационных процессов и исследование в ИТ / В.Н. Чернышов, Д.В. Образцов, А.В. Платёнкин ; Министерство образования и науки Российской Феде-рации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 98 с.: ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499294

2. Теоретические основы информационных процессов и систем / Душин В.К., - 5-е изд. - М.:Дашков и К, 2018. - 348 с.: ISBN 978-5-394-01748-3 - Режим доступа: http://znanium.com/catalog/product/450784

***Дополнительная литература***

3.Моделирование систем и процессов: учебник для вузов/ В.Н. Волкова [и др.]; под редакцией В.Н. Волковой, В.Н. Козлова.— Москва: Издательство Юрайт, 2020 — 450с. — (Высшее образование). — ISBN 978-5-9916-7322-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450218

## 8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

**Интернет-ресурсы**:

1. http://eup.ru/catalog/all-all.asp **– научно-образовательный портал;**
2. http://informika.ru/ **– образовательный портал;**
3. www.wikIsec.ru **- Энциклопедия информационной безопасности. –**

**Публикации, статьи;**

4. **www.biblioclub.ru** - Универсальная библиотека онлайн;
5. **www.rucont.ru** - ЭБС «Руконт»;
6. http://www.academy.it.ru/ – **академия АЙТИ;**
7. http://www.minfin.ru - **Официальный сайт Министерства финансов Российской Федерации;**
8. http://www.gov.ru/ - **Официальный сервер органов государственной власти Российской Федерации;**
9. http://www.fsb.ru/ - **Официальный сайт Федеральной Службы Безопасности;**
10. http://www.fstec.ru/ - **Официальный сайт Федеральной Службы по Техническому Экспортному Контролю;**
11. http://www.minfin.ru - **Официальный сайт Министерства финансов Российской Федерации;**
12. http://www.gov.ru - **Официальный сервер органов государственной власти Российской Федерации;**
13. http://www.fsb.ru/ - **Официальный сайт Федеральной Службы Безопасности;**
14. http://www.fstec.ru/ - **Официальный сайт Федеральной Службы по Техническому Экспортному контролю.**

## 9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

## 10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice.
- **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы:
   Консультант+;
   Гарант.

## 11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

**Лекционные занятия**:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

**Практические занятия:**

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети

**Приложение 1**

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ**

**И ТЕХНОЛОГИЙ**

**КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

# ОРГАНИЗАЦИЯ СПЕЦ. ПРОВЕРОК И СПЕЦ ИССЛЕДОВАНИЙ ОБЪЕКТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Направление подготовки: 10.04.01 - Информационная безопасность**

**Профиль: Менеджмент информационной безопасности**

**Уровень высшего образования: магистратура**

**Форма обучения: очная**

Королев

2023

# 1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

| № п/п | Индекс компе-тенции | Содержание компетенции | Раздел дисциплины, обеспечивающий формирование компетенции | В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает: | | |
|---|---|---|---|---|---|---|
| | | | | Трудовые действия | Необходимые умения | Необходимые знания |
| 1. | ПК-2 | Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении. | Тема:1 - 16 | ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС. | ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС. | ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС. |
| 2. | ПК-3 | Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД | Тема:1-16 | ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда. | ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении. | ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок. |

**2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

| ***Код компетенции*** | ***Инструменты, оценивающие сформированность компетенции*** | ***Этапы и показатель оценивания компетенции*** | ***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*** |
|---|---|---|---|
| ПК-2,3 | Доклад в форме презентации | ***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов***<br><br>***Б) частично сформирована:***<br><br>• ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;***<br>• ***компетенция освоена на <u>базовом</u> уровне – 3 балла;***<br>***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов*** | Проводится устно с использованием мультимедийных систем, а также с использованием технических средств<br><br>Время, отведенное на процедуру – 10 - 15 мин.<br><br>Неявка – 0.<br><br>Критерии оценки:<br><br>1.Соответствие представленной презентации заявленной тематике (1 балл).<br><br>2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).<br><br>3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).<br><br>4.Качество самой представленной презентации (1 балл).<br><br>5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).<br><br>Максимальная сумма баллов - 5 баллов.<br>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал. |

**3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

**Примерная тематика докладов в презентационной форме:**

1. Вредоносные программы и антивирусные программные средства.
2. Методы программно-аппаратной защиты информации.
3. Аттестация объектов информатизации. 19. Виды защиты информации.
4. Системы защиты информации.
5. Модели разграничения доступа.
6. Криптографические стандарты и их использование в информационных системах.
7. Способы и средства защиты информации от утечки по техническим каналам.
8. Принципы организации информационных систем в соответствии с требованиями по защите информации.
9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.
13. Лицензирование и сертификация в области защиты информации.
14. Комплексные системы защиты информации.

**Примерная тематика индивидуальных заданий:**

1. Ведущие мировые разведки и их деятельность в России.
2. Основы обеспечения безопасности информации в компьютерных системах.
3. Информационная безопасность современной России: угрозы и их отражения.
4. Информационные войны в современном мире.
5. Компьютерная преступность в экономических областях.
6. Мир XXI века: информационное противоборство.
7. Компьютерные вирусы в современных информационных системах.
8. Информационные угрозы современным экономическим объектам.
9. Информатизация России и проблема защиты информации.
10. Безопасность информации в коммерческой деятельности.
11. Разведки России – исторический аспект.
12. Мировой информационный терроризм.
13. Этика защиты информации.
14. Становление и развитие промышленного шпионажа.

## 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Организация спец. проверок и спец. исследований объектов информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

| Неделя текущего контроля | Вид оценочного средства | Код компетенций, оценивающий знания, умения, навыки | Содержание оценочного средства | Требования к выполнению | Срок сдачи (неделя семестра) | Критерии оценки по содержанию и качеству с указанием баллов |
|---|---|---|---|---|---|---|
| Согласно учебному плану | тестирование | ПК-2,3 | 20 вопросов | Компьютерное тестирование ; время отведенное на процедуру - 30 минут | Результаты тестирования предоставляются в день проведения процедуры | ***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%.*** |
| Согласно учебному плану | тестирование | ПК-2,3 | 20 вопросов | Компьютерное тестирование; время отведенное на процедуру – 30 минут | Результаты тестирования предоставляются в день проведения процедуры | ***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%.*** |

| | | | | | | |
|---|---|---|---|---|---|---|
| Согласно учебному плану | Зачет | ПК-2,3 | 3 вопроса | Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут. | Результаты предоставляются в день проведения зачета | Критерии оценки:<br>**«Зачтено»:**<br>1. знание лексического и грамматического материала;<br>2. умение использовать и применять полученные знания на практике;<br>3. работа на практических занятиях в течение семестра;<br>4. ответ на вопросы зачета.<br>**«Не зачтено»:**<br>1. демонстрирует частичные знания по темам дисциплин;<br>2. незнание лексического и грамматического материала;<br>3. неумение использовать и применять полученные знания;<br>4. не работал на практических занятиях;<br>5. не отвечает на вопросы зачета. |

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

### 4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.

6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

*Тестовые задания для контроля остаточных знаний*

1. Что понимается под аттестацией объектов информатизации?
    - контрольная проверка объекта информатизации, по результатам которой выдается сертификат соответствия требованиям по безопасности информации;
    - оснащение объекта информатизации средствами защиты, по результатам которой выписывается паспорт или паспорт соответствия требованиям по безопасности информации;
    - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - аттестата соответствия подтверждается, что объект соответствует требованиям стандартов;
    - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - лицензии подтверждается, что объект соответствует требованиям стандартов.
2. Какие объекты информатизации подлежат обязательной аттестации?
    - объекты информатизации, предназначенные для обработки конфиденциальной информации в коммерческих организациях;

- объекты информатизации, предназначенные для обработки конфиденциальной информации в бюро кредитных историй;
- объекты информатизации, предназначенные для обработки информации, составляющие государственную тайну, управления экологически опасными объектами, ведения секретных переговоров ;
- объекты информатизации, предназначенные для обработки информации, составляющей коммерческую тайну.

3. Какие документы разрабатывает и утверждает орган по аттестации в процессе аттестации объекта информатизации?

- технический паспорт объекта информатизации;
- матрицу доступа к объекту вычислительной техники, аттестованному по требованиям безопасности информации;
- протоколы испытаний и заключение по результатам проведения специальных исследований объекта информатизации;
- аттестат соответствия объекта информатизации требованиям по безопасности информации.

4. Какие классы защищенности от несанкционированного доступа реализуют для защиты конфиденциальной информации на объектах вычислительной техники, аттестованных по требованиям безопасности информации?

- 1А, 1Б, 1В;
- 2А, 3А;
- 2Б, 3Б;
- 1Г, 1Д.

5. Когда проводят испытания несертифицированной продукции, используемой на объекте информатизации, подлежащем обязательной аттестации?

- в ходе проведения аттестационных испытаний объекта информатизации;
- после предварительного ознакомления с объектом аттестации;
- после оформления, регистрации и выдачи аттестата соответствия;
- до подачи и рассмотрения заявки на аттестацию объекта информатизации.

### 1.2.Типовые вопросы, выносимые на зачет

1. Функции, состав, структура и задачи государственной системы защиты информации (ГСЗИ).
2. Основные нормативно-методические документы ФСТЭК России в области аттестации объектов информатизации.
3. Состав, особенности применения и характеристики контрольно-измерительного оборудования, применяемого для аттестации защищаемых помещений по требованиям безопасности информации.

4. Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

5. Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

6. Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

7. Последовательность проведения работ по аттестации защищаемых помещений.

8. Состав, особенности применения и характеристики контрольно-измерительного оборудования, применяемого для аттестации объектов вычислительной техники по требованиям безопасности информации.

9. Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

10. Какие документы разрабатывает и утверждает орган по аттестации в процессе аттестации объекта информатизации?

11. Перечислить и пояснить классы защищенности от несанкционированного доступа, которые реализуют для защиты конфиденциальной информации на объектах вычислительной техники, аттестованных по требованиям безопасности информации.

12. Порядок проведения аттестации объекта информатизации.

13. Перечень и содержание документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.

14. Перечень и содержание документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

15. Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.

16. Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.

17. Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

18. Документы, оформляемые и разрабатываемые при проверках и испытаниях аттестуемого объекта информатизации в процессе его эксплуатации.

19. Основные положения методики оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации; оценка защищенности помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.

20. Контрольно-измерительная аппаратура и оборудование, используемые для оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации.

21. Основные положения методики оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание.

22. Контрольно-измерительная аппаратура и оборудование, используемые для оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации.

23. Перечень и содержание документов, устанавливающих правила лицензирования деятельности в области защиты информации (ЗИ).

24. Перечень и основное содержание документов, устанавливающих правила сертификации СЗИ.

25. Перечень и основное содержание документов, устанавливающих правила проведения аттестации объектов информатизации.

26. Основное содержание Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К).

27. Основное содержание Сборника временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам.

28. Основное содержание Требований к системам обнаружения вторжений, утвержденных приказом ФСТЭК России от 06.12.2011 № 638.

29. Основное содержание Сборника методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи, утвержденного приказом ФСТЭК России от 15.03.2012 № 27.

30. Основное содержание Положения о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 05.02.2010 № 58 (зарегистрирован Минюстом России 19.02.2010, регистрационный № 16456).

31. Основное содержание Порядка проведения классификации информационных систем персональных данных. Утверждено приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

32. Основное содержание Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

33. Основное содержание Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008.

34. Основное содержание Приказа ФСТЭК России от 12.07.2012 № 83 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации".

35. Основное содержание Приказа ФСТЭК России от 12.07.2012 № 84 "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации"

36. Основное содержание ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.

37. Основное содержание ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования

**Приложение 2**

**Методические указания для обучающихся по освоению дисциплины (модуля)**

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ***

***И ТЕХНОЛОГИЙ***

***КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

# ОРГАНИЗАЦИЯ СПЕЦ. ПРОВЕРОК И СПЕЦ. ИССЛЕДОВАНИЙ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Направление подготовки: 10.04.01 - Информационная безопасность**

**Направленность (профиль): Менеджмент информационной безопасности**

**Уровень высшего образования: магистратура**

**Форма обучения: очная**

Королев

2023

## 1. Общие положения

**Целью изучения дисциплины является** формирование у студентов базовых знаний и практических навыков в области проведения аттестации объектов информатизации по требованиям безопасности информации.

**Задачи дисциплины:**

- формирование у студентов базовых знаний в области аттестации объектов информатизации по требованиям безопасности информации, проведению специального обследования (СО), специальных проверок (СП) и специальных исследований, проводимых в ходе аттестации;
- ознакомление с основными нормативно-правовыми и методическими документами в области проведения специальных исследований и аттестации объектов информатизации по требованиям безопасности информации;
- привитие навыков практической работы с контрольно-измерительной аппаратурой, применяемой для аттестации объектов информатизации;
- привитие навыков разработки организационно-распорядительных документов, оформляемых по результатам аттестации объектов информатизации.

### 2. Указания по проведению практических занятий

**Тема 1- 2. Введение. Функции, состав, структура и задачи государственной системы защиты информации**

**Вид практического занятия:** занятие в смешанной форме

**Практическое занятие 1**.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: беседа

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

*Основные положения темы занятия*:

- базовые составляющие концепции информационной безопасности информационного объекта.
- основные направления обеспечения информационной безопасности.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Функции государственной системы защиты информации в соответствии с основными правовыми и нормативно методическими документами.

2. Состав, структура и задачи государственной системы защиты информации в соответствии с основными правовыми и нормативно методическими документами.

Продолжительность занятия: 1 ч.

**Тема 3. Нормативно-методические документы ФСТЭК России и национальные стандарты в области аттестации объектов информатизации**

**Вид практического занятия:** занятие в смешанной форме

**Практическое занятие 2**.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки моделирования основных криптографических методов защиты информации.

*Основные положения темы занятия*:

- базовые составляющие криптографической защиты информации.
- криптосистемы и блочные шифры.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Положение о сертификации средств защиты информации по требованиям безопасности информации.
2. Руководящие документы Гостехкомиссии России, используемые при аттестации объектов информатизации, и их содержание.
3. Основное содержание национальных стандартов в области аттестации объектов информатизации.

Продолжительность занятия: 1 ч.

**Тема 4. Правила лицензирования деятельности в области защиты информации (ЗИ), сертификации средств защиты информации (СЗИ) и проведение аттестации объектов информатизации**

**Вид практического занятия:** занятие в смешанной форме

**Практическое занятие 3**.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки моделирования основных криптографических протоколов защиты информации.

*Основные положения темы занятия*:

- базовые протоколы криптографической защиты информации.

- квантовая криптография.

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Перечень и содержание документов, устанавливающих правила лицензирования деятельности в области защиты информации (ЗИ).
2. Перечень и основное содержание документов, устанавливающих правила сертификации СЗИ.
3. Перечень и основное содержание документов, устанавливающих правила проведения аттестации объектов информатизации.

Продолжительность занятия: 1 ч.

## Тема 5. Основные положения законодательства в области защиты информации

**Вид практического занятия:** занятие в смешанной форме

**Практическое занятие 4**.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *беседа*.

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки управления ключами.

*Основные положения темы занятия*:

- Управление ключами.
- Взаимодействие с УЦ.

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

Учебные вопросы

1. Конституция РФ, федеральные законы, Указы Президента РФ, постановления и распоряжения Правительства РФ об информационной безопасности общества и его граждан.
2. Основное содержание Закона Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности».
3. Основное содержание Закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».
4. Основное содержание Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Основное содержание Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».
6. Содержание Указа Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при

использовании информационно-телекоммуникационных сетей международного информационного обмена».
Продолжительность занятия: 1 ч.

**Тема 6. Содержание мероприятий на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе**

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *практическая работа в группах*.

**Практическое занятие 5.**

Учебные вопросы

1. Организация работ по защите информации в ходе создания и эксплуатации объектов информатизации и их систем защиты информации.
2. Выполняемые работы на предпроектной стадии по обследованию объекта информатизации;
3. Содержание аналитического обоснования необходимости создания системы защиты информации;
4. Содержание технического задания на разработку системы защиты информации;
5. Содержание работ на стадии проектирования и создания объекта информатизации и системы защиты информации в его составе.

Продолжительность занятия: 2 ч.

**Тема 7. Требования и рекомендации по защите речевой конфиденциальной информации (КИ)**

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *беседа*.

**Практическое занятие 6.**

Учебные вопросы

1. Основные требования и рекомендации по защите речевой КИ.
2. Защита КИ, циркулирующей с системах звукоусиления и звукового сопровождения.

Продолжительность занятия: 2 ч.

**Тема 8. Проведение аттестация объектов информатизации (ОИ)**

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

**Практическое занятие 7.**

Учебные вопросы

1. Порядок проведения аттестации защищаемого помещения по требованиям защиты конфиденциальной информации.
2. Порядок проведения аттестации объекта вычислительной техники по требованиям защиты конфиденциальной информации.

Продолжительность занятия: 2 ч.

**Тема 9. Перечень документов и работ по подготовке объекта информатизации к аттестации**

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

**Практическое занятие 8.**

Учебные вопросы

1. Перечень работ по подготовке объекта информатизации к аттестации.
2. Оформление заявки на аттестацию объекта информатизации и документы, предоставляемые для предварительного ознакомления с аттестуемым объектом и разрабатываемые для осуществления начала аттестации.
3. Перечень документов, которые разрабатывает и утверждает заказчик или владелец объекта информатизации по результатам аттестации.
3. Перечень документов, которые разрабатывает и утверждает орган по аттестации по результатам выполненных аттестационных испытаний.

Продолжительность занятия: 2 ч.

**Тема 10. Этапы практического проведения работ по аттестации объектов информатизации**

Вид практического занятия: *подготовка реферата*

Образовательные технологии: *беседа*

**Практическое занятие 9.**

Учебные вопросы

1. Контрольно-измерительное оборудование, применяемое для аттестации защищаемых помещений по требованиям безопасности информации.
2. Последовательность проведения работ по аттестации защищаемых помещений.
3. Контрольно-измерительное оборудование, применяемое для аттестации объектов вычислительной техники по требованиям безопасности информации.
4. Последовательность проведения работ по аттестации объектов вычислительной техники по требованиям безопасности информации.

Продолжительность занятия: 2 ч.

**Тема 11. Проверка и испытание аттестуемого (аттестованного) объекта информатизации**

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

**Практическое занятие 10.**

Учебные вопросы

1. Способы контроля и их содержание для проверки и испытаний аттестуемого (аттестованного) объекта информатизации.

2. Основные комплексы контрольно-измерительной аппаратуры, используемой для проверки и испытаний аттестуемого (аттестованного) объекта информатизации, и их технические характеристики.

3. Перечень работ по проверке и испытаниям аттестуемого (аттестованного) объекта информатизации в процессе его эксплуатации.

Продолжительность занятия: 2 ч.

**Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам**

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

**Практическое занятие 11.**

Учебные вопросы

1. Содержание работ по поставке средств защиты информации от утечки по техническим каналам.

2. Содержание работ по установке средств защиты информации от утечки по техническим каналам и обеспечению эффективности их функционирования в процессе эксплуатации аттестованных объектов информатизации.

Продолжительность занятия: 2 ч.

**Тема 13. Пассивные и активные методы защиты объектов информатизации**

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

**Практическое занятие 12.**

Учебные вопросы

1. Содержание Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 № 58.

2. Рекомендации по обеспечению ЗИ содержащиеся в негосударственных информационных ресурсах при взаимодействии пользователей с информационными сетями общего пользования.

Продолжительность занятия: 2 ч.

**Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке**

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

**Практическое занятие 13.**

Учебные вопросы

1. Типы и перечень объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

2. Возможные угрозы объектам информатизации, подлежащих аттестационным испытаниям в обязательном порядке.

3. Порядок проведения классификации информационных систем персональных данных в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Продолжительность занятия: -2 ч.

**Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа**

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

**Практическое занятие 14.**

Учебные вопросы

1. Определение структуры и точек доступа сетевого периметра организации с помощью контрольно-измерительной аппаратуры.
2. Применение сканеров безопасности для поиска уязвимостей сетевого периметра организации.

Продолжительность занятия: 2 ч.

**Тема 16. Методики оценки защищённости объектов информатизации**

Вид практического занятия: *подготовка реферата.*

Образовательные технологии: *беседа.*

**Практическое занятие 15.**

Учебные вопросы

1. Методика оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание; оценка защищенности помещений от утечки речевой конфиденциальной информации по акустическому, виброакустическому и акустоэлектрическому каналам.
2. Контрольно-измерительная аппаратура и оборудование, используемое для оценки защищённости помещения, аттестованного по требованиям безопасности конфиденциальной информации.
3. Методика оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации, и ее содержание.
4. Контрольно-измерительная аппаратура и оборудование, используемое для оценки защищённости объекта вычислительной техники, аттестованного по требованиям безопасности конфиденциальной информации.

Продолжительность занятия: 2 ч.

**3. Указания по проведению лабораторных работ**

Не предусмотрено учебным планом.

**4. Указания по проведению самостоятельной работы студентов**

| № п/п | Наименование блока (раздела) дисциплины | Виды СРС |
|---|---|---|
| 1. | Тема 10. Этапы практического проведения работ по аттестации объектов информатизации | *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*<br>Примерная тематика *рефератов (докладов, письменных работ и т.д.): … (разрабатывается самостоятельно преподавателем на основе рабочей программы).*<br>1. Место информационной безопасности в системе национальной безопасности.<br>2. Современная концепция информационной безопасности.<br>3. Цели и концептуальные основы защиты информации.<br>4. Критерии, условия и принципы отнесения информации к защищаемой.<br>5. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.<br>6. Понятие и структура угроз защищаемой информации.<br>7. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию |
| 2. | Тема 11. Проверка и испытание аттестуемого объекта информатизации | *Подготовка рефератов, письменная работа, самостоятельное изучение тем, работа с программным обеспечением, создание презентаций.*<br>Примерная тематика *рефератов (докладов, письменных работ и т.д.): … (разрабатывается самостоятельно преподавателем на основе рабочей программы).*<br>1. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.<br>2. Виды уязвимости информации и формы ее проявления.<br>3. Каналы и методы несанкционированного доступа к конфиденциальной информации.<br>4. Модель нарушителя.<br>5. Модель угроз.<br>6. Критерии оценки безопасности информационных технологий.<br>7. Методы защиты информации от несанкционированного доступа.<br>8. Риски информационной безопасности. |
| | Тема 12. Поставка и установка средств защиты информации от утечки по техническим каналам | 1. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.<br>2. Виды уязвимости информации и формы ее проявления.<br>3. Каналы и методы несанкционированного доступа к конфиденциальной информации.<br>4. Модель нарушителя.<br>5. Модель угроз.<br>6. Критерии оценки безопасности информационных технологий. |

| | | |
|---|---|---|
| | | 7. Методы защиты информации от несанкционированного доступа.<br>8. Риски информационной безопасности. |
| | Тема 13. Пассивные и активные методы защиты объектов информатизации | ***Подготовка докладов и презентаций по темам:***<br>Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения.<br>Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.<br>Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. |
| | Тема 14. Виды объектов информатизации, подлежащих аттестационным испытаниям в обязательном порядке | ***Подготовка докладов и презентаций по темам:***<br>Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения.<br>Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.<br>Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. |
| | Тема 15. Методы тестирования системы защиты информации автоматизированных систем от несанкционированного доступа | ***Подготовка докладов и презентаций по темам:***<br>Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости |

| | | |
|---|---|---|
| | | АС.<br><br>Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.<br><br>Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков. |
| | Тема 16. Методики оценки защищённости объектов информатизации | ***Подготовка докладов и презентаций по темам:***<br><br>Перечень основных документов ФСТЭК России по вопросам защиты информации.<br><br>Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД.<br><br>**Примерные темы докладов**<br>1. Вредоносные программы и антивирусные программные средства.<br>2. Методы программно-аппаратной защиты информации.<br>3. Аттестация объектов информатизации. 19. Виды защиты информации.<br>4. Системы защиты информации.<br>5. Модели разграничения доступа.<br>6. Криптографические стандарты и их использование в информационных системах.<br>7. Способы и средства защиты информации от утечки по техническим каналам.<br>8. Принципы организации информационных систем в соответствии с требованиями по защите информации.<br>9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.<br>10. Отечественные и зарубежные стандарты в области компьютерной безопасности.<br>11. Принципы и методы организационной защиты информации.<br>12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.<br>13. Лицензирование и сертификация в области защиты информации. |

## 5. Перечень основной и дополнительной учебной литературы

***Основная литература***

1.Математическое моделирование технических систем: учебник / В.П. Тарасик. — Минск: Новое знание; М.: ИНФРА-М, 2018. — 592 с. — (Высшее

образование: Бакалавриат) [электронный ресурс] // Режим доступа: http://znanium.com/catalog/product/952123

***Дополнительная литература***

2.Аверченков В.И. Основы математического моделирования технических систем / В.И. Аверченков, В.П. Федоров, М.Л. Хейфец. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 271 с.: схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93344

3. Голубева Н. В. Математическое моделирование систем и процессов: учебное пособие / Н. В. Голубева. — 2-е изд., стер. — Санкт-Петербург: Лань, 2016. — 192 с. — ISBN 978-5-8114-1424-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/76825

Вариант-2

***Основная литература***

1. Чернышов В.Н. Моделирование информационных процессов и исследование в ИТ / В.Н. Чернышов, Д.В. Образцов, А.В. Платёнкин ; Министерство образования и науки Российской Феде-рации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 98 с.: ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499294

2. Теоретические основы информационных процессов и систем / Душин В.К., - 5-е изд. - М.:Дашков и К, 2018. - 348 с.: ISBN 978-5-394-01748-3 - Режим доступа: http://znanium.com/catalog/product/450784

***Дополнительная литература***

3.Моделирование систем и процессов: учебник для вузов/ В.Н. Волкова [и др.]; под редакцией В.Н. Волковой, В.Н. Козлова.— Москва: Издательство Юрайт, 2020 — 450с. — (Высшее образование). — ISBN 978-5-9916-7322-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450218

## 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины (модуля)

**Интернет-ресурсы**:

1. **Электронные ресурсы образовательной среды Университета.**
2. http://eup.ru/catalog/all-all.asp **– научно-образовательный портал.**
3. http://informika.ru/ **– образовательный портал.**
4. www.wikIsec.ru - **Энциклопедия информационной безопасности. – Публикации, статьи.**
5. **www.biblioclub.ru** - Универсальная библиотека онлайн.
6. **www.rucont.ru** - ЭБС «Руконт».
7. http://www.academy.it.ru/ - **академия АЙТИ.**

**8.** http://www.minfin.ru/ **- Официальный сайт Министерства финансов Российской Федерации**

**9.** http://www.gov.ru/ **- Официальный сервер органов государственной власти Российской Федерации.**

**10.** http://www.fsb.ru/ **- Официальный сайт Федеральной Службы Безопасности**

11. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

12. Электронные ресурсы образовательной среды Университета

**13.** http://www.minfin.ru **- официальный сайт Министерства финансов Российской Федерации.**

**14.** http://www.gov.ru **- сервер органов государственной власти Российской Федерации.**

## 7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

**Перечень программного обеспечения:** *MSOffice, Multisim.*

**Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы:
   Консультант+;
   Гарант.