МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ»

Программа согласована
с федеральным учебно-методическим
объединением в системе высшего
образования по УГСНП 10.00.00
«Информационная безопасность»
06 апреля 2022 года


Программа согласована
с ФСТЭК России
15 апреля 2022 г.

**ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ**
**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Москва, 2022

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Программа переподготовки разработана на основе федерального образовательного стандарта высшего образования по направлению 10.03.01 Информационная безопасность (бакалавриат).

## 1.1. Цель реализации программы

Цель программы – формирование у слушателей профессиональных компетенций, необходимых для выполнения нового вида профессиональной деятельности – деятельности в области защиты информации.

## 1.2. Характеристика нового вида профессиональной деятельности

**Область профессиональной деятельности**:
06 Связь, информационные и коммуникационные технологии

**Вид экономической деятельности**:
74.90.99 – Деятельность в области защиты информации прочая

**Наименование нового вида профессиональной деятельности**:
1) техническая защита информации;
2) криптографическая защита информации.

**Объекты профессиональной деятельности:**
средства и системы информатизации;
помещения, предназначенные для ведения конфиденциальных переговоров (далее – защищаемые помещения);
средства защиты информации (защищенные технические средства обработки информации, технические средства защиты информации, программные и программно-технические средства защиты информации, средства контроля эффективности защиты информации).

**Укрупненная группа специальностей**:
10.00.00 Информационная безопасность.

## Задачи профессиональной деятельности в соответствии с трудовыми функциями профессиональных стандартов и лицензируемыми видами выполняемых работ

| Виды деятельности | Задачи профессиональной деятельности | Трудовая функция (код, уровень квалификации) | Лицензируемые виды выполняемых работ |
|---|---|---|---|
| **Эксплуатационный вид деятельности** | Проведение работ по установке, настройке и техническому обслуживанию средств технической защиты информации | A/01.5. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок[1].<br>A/02.5. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам[1].<br>A/03.5. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа[1]. | Пункт 4 е Положения, утвержденного Постановлением Правительства РФ №79[3] |
| | Проведение работ по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации | B/01.6. Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации[1].<br>B/02.6. Проведение работ по техническому обслуживанию защищенных технических средств обработки информации [1]. | Пункт 4 е Положения, утвержденного Постановлением Правительства РФ №79[3] |
| | Проведение работ по установке, настройке и техническому обслуживанию средств криптографической защиты информации в автоматизированных системах | C/01.6. Установка и настройка средств защиты информации в автоматизированных системах[2].<br>A/01.5. Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем[2]. | Пункты 12, 13, 20 к приложению Положения, утвержденного Постановлением РФ № 313[4] |
| **Организационно-управленческий вид деятельности** | Разработка организационно-распорядительных документов по защите | C/02.6. Разработка организационно-распорядительных документов по | Пункт 4 е Положения, утвержденного Постановлением |

| Виды деятельности | Задачи профессиональной деятельности | Трудовая функция (код, уровень квалификации) | Лицензируемые виды выполняемых работ |
|---|---|---|---|
| | информации в автоматизированных системах | защите информации в автоматизированных системах[2]. | Правительства РФ №79[3] Пункты 12, 13, 20 Положения, утвержденного Постановлением № 313[4] |

Примечание:
[1]Профессиональный стандарт 06.034 «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.
[2]Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах», утверждённый приказом Минтруда России от 15.09.2016 № 522н. Регистрационный № 843.
[3]Положение о лицензировании деятельности по технической защите конфиденциальной информации (утв. постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79, в ред. от 30.11.2020 г.).
[4] Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) (утв. постановлением Правительства РФ Постановление Правительства Российской Федерации от 16 апреля 2012 г. №313, в ред. от 21.12.2020).

## 1.3. Требования к результатам освоения программы

Слушатель должен получить знания, умения и опыт деятельности, которые позволяют сформировать соответствующие компетенции для его нового вида профессиональной деятельности и решения задач при осуществлении лицензируемых видов деятельности:

| Виды деятельности | Код и наименование профессиональной компетенции | Трудовая функция (код, уровень квалификации, наименование) на основе которой сформулирована компетенция |
|---|---|---|
| **Эксплуатационный вид деятельности** | ПК-1. Способен проводить работы по установке и настройке средств технической защиты информации и защищенных технических средств обработки информации. | А/01.5. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок[1]. А/02.5. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам[1]. |

| Виды деятельности | Код и наименование профессиональной компетенции | Трудовая функция (код, уровень квалификации, наименование) на основе которой сформулирована компетенция |
|---|---|---|
| | | A/03.5. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа[1].<br>B/01.6. Проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации[1]. |
| | ПК-2. Способен проводить работы по установке и настройке средств криптографической защиты информации в автоматизированных системах. | C/01.6. Установка и настройка средств защиты информации в автоматизированных системах[2]. |
| | ПК-3. Способен проводить работы техническому обслуживанию средств защиты информации и защищенных технических средств обработки информации | B/02.6. Проведение работ по техническому обслуживанию защищенных технических средств обработки информации [1].<br>A/01.5. Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем[2]. |
| **Организационно-управленческий вид деятельности** | ПК-4. Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах | C/02.6. Разработка организационно-распорядительных документов по защите информации в автоматизированных системах[2]. |

Примечание:
[1]Профессиональный стандарт 06.034 «Специалист по технической защите информации», утверждённый приказом Минтруда России от 01.11.2016 № 599н. Регистрационный № 844.
[2]Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах», утверждённый приказом Минтруда России от 15.09.2016 № 522н. Регистрационный № 843.

## Индикаторы сформированности профессиональных компетенций

| Код и наименование профессиональной компетенции | Индикаторы сформированности профессиональных компетенций |
|---|---|
| ПК-1. Способен проводить работы по установке и настройке средств технической защиты информации и защищенных технических средств обработки информации. | **Знания:**<br>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа.<br>Технические каналы утечки информации, возникающие при обработке информации средствами вычислительной техники (СВТ).<br>Технические каналы утечки акустической речевой информации.<br>Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок.<br>Способы и средства защиты информации акустической речевой информации от утечки по техническим каналам.<br>Защищенные технические средства обработки информации. |

| Код и наименование профессиональной компетенции | Индикаторы сформированности профессиональных компетенций |
|---|---|
| | Методы и средства контроля эффективности защиты информации от утечки по техническим каналам.<br>Угрозы несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах.<br>Методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее.<br>Методы и средства контроля защищенности информации от несанкционированного доступа и специальных программных воздействий.<br>**Умения:**<br>Проводить установку и настройку средств защиты информации от утечки по каналам побочных электромагнитных излучений и наводок.<br>Производить установку и настройку средств защиты акустической речевой информации от утечки по техническим каналам.<br>Производить установку и настройку средств защиты информации от несанкционированного доступа.<br>Проводить установку и настройку антивирусных программ.<br>Проводить установку и настройку защищенных технических средств обработки информации.<br>Проводить испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами.<br>**Опыт деятельности:**<br>По установке и настройке средств технической защиты информации и защищенных технических средств обработки информации. |
| ПК-2. Способен проводить работы по установке и настройке средств криптографической защиты информации в автоматизированных системах. | **Знания:**<br>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа.<br>Основные понятия криптографии.<br>Основные криптографические алгоритмы и протоколы, используемые для защиты информации в средствах и системах информатизации.<br>Общие принципы функционирования средств криптографической защиты информации.<br>Принципы функционирования средств защиты информации в автоматизированных системах, в том числе использующих криптографические алгоритмы.<br>Типовые методы и протоколы аутентификации в автоматизированных системах.<br>Номенклатуру, функциональное назначение и основные характеристики средств и систем защиты информации от несанкционированного доступа (НСД).<br>Требования к составу и содержанию средств и систем защиты информации от НСД.<br>Принципы построения защищенного документооборота.<br>**Умения:**<br>Проводить настройку автоматизированных систем, защищенных с использованием криптографических средств, в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами.<br>Использовать криптографические средства защиты информации. |

| Код и наименование профессиональной компетенции | Индикаторы сформированности профессиональных компетенций |
|---|---|
| | Корректно эксплуатировать средства электронной подписи.<br>Устанавливать, настраивать и эксплуатировать программные и программно-аппаратные средства защиты информации различных производителей (в том числе средства электронной подписи и программно-аппаратные компоненты PKI).<br>Формировать ключи и сертификаты с использованием различных средств электронной подписи;<br>**Опыт деятельности:**<br>По установке и настройке средств криптографической защиты информации в автоматизированных системах. |
| ПК-3. Способен проводить работы техническому обслуживанию средств защиты информации и защищенных технических средств обработки информации | **Знания:**<br>Организация технического обслуживания средств защиты информации (в том числе криптографических) и технических средств обработки информации в защищенном исполнении.<br>Организация ремонта средств защиты информации (в том числе криптографических) и технических средств обработки информации в защищенном исполнении.<br>**Умение:**<br>Проводить техническое обслуживание средств защиты информации (в том числе криптографических) и защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.<br>Проводить устранение выявленных неисправностей средств защиты информации (в том числе криптографических) и защищенных технических средств обработки информации.<br>Организовывать ремонт средств защиты информации (в том числе криптографических) и защищенных технических средств обработки информации с привлечением производителей.<br>**Опыт деятельности:**<br>По техническому обслуживанию средств защиты информации (в том числе криптографических) и защищенных технических средств обработки информации. |
| ПК-4. Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах | **Знания:**<br>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа в автоматизированных системах.<br>Технические каналы утечки информации, возникающие при обработке информации в автоматизированных системах.<br>Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок.<br>Угрозы несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах. Модели нарушителей. Методику оценки угроз безопасности информации.<br>Методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее.<br>Методы и средства криптографической защиты информации.<br>Организацию защиты информации на объектах информатизации. |

| Код и наименование профессиональной компетенции | Индикаторы сформированности профессиональных компетенций |
|---|---|
| | Состав и содержание организационно-распорядительных документов по защите информации в автоматизированных системах и на объектах информатизации.<br>**Умения:**<br>Проводить оценку угроз безопасности информации и разрабатывать модель угроз.<br>Разрабатывать концепцию информационной безопасности.<br>Разрабатывать организационно-распорядительные документы по защите информации (в том числе с использованием криптографических средств) в автоматизированных системах.<br>**Опыт деятельности:**<br>Разработки организационно-распорядительных документов по защите информации (в том числе с использованием криптографических средств) в автоматизированных системах. |

## 1.4. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

Наличие высшего образования или получающего высшее образование (при наличии соответствующей справки с указанием года окончания).

Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

## 1.5. Трудоемкость обучения

Нормативная трудоемкость обучения по данной программе – 576 часов (16 зачетных единиц), включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

## 1.6. Форма обучения

Форма обучения очная и очно-заочная. Сроки обучения устанавливаются при наборе группы слушателей и фиксируются в договорах с заказчиками на оказание образовательных услуг.

При реализации программы возможно использование дистанционных образовательных технологий и электронного обучения.

Объем занятий с применением дистанционных образовательных технологий и электронного обучения определяется разработчиком конкретного учебного плана рабочей программы при наборе группы слушателей и фиксируются в договорах с заказчиками на оказание образовательных услуг.

Не допускается проведение лабораторных занятий с применением исключительно электронного обучения и дистанционных образовательных технологий.

При реализации программы может быть использована сетевая форма, в том числе в части, касающейся использования необходимого лабораторного оборудования.

### 1.7. Режим занятий

При любой форме обучения учебная нагрузка устанавливается не более 54 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя. Продолжительность одного часа занятий 45 минут.

При контактной форме работы – 40 академических часов всех видов занятий в неделю.

## 2. СОДЕРЖАНИЕ ПРОГРАММЫ

### 2.1. Учебный план программы переподготовки

| № п/п | Наименование модулей и учебных дисциплин | Общая трудоемкость, час | Контактная работа, час | | | | СРС, час | Промежуточная аттестация |
|---|---|---|---|---|---|---|---|---|
| | | | Всего | Лекции | Лабораторные занятия | Практические занятия | | |
| **1.** | **Модуль 1. «Техническая защита информации»** | **360** | **274** | **126** | **80** | **68** | **86** | |
| 1.1. | Учебная дисциплина «Правовые основы защиты информации» | 40 | 32 | 24 | - | 8 | 8 | Зачет с оценкой |
| 1.2. | Учебная дисциплина «Защита информации от утечки по техническим каналам» | 114 | 86 | 34 | 36 | 16 | 28 | Зачет с оценкой |
| 1.3. | Учебная дисциплина «Защита информации от несанкционированного доступа» | 108 | 84 | 40 | 44 | – | 24 | Зачет с оценкой |
| 1.4. | Учебная дисциплина «Организация защиты информации» | 98 | 72 | 28 | - | 44 | 26 | Зачет с оценкой |
| **2.** | **Модуль 2. «Криптографическая защита информации»** | **180** | **132** | **52** | **48** | **32** | **48** | |
| 2.1. | Учебная дисциплина «Методы и средства криптографической защиты информации» | 180 | 132 | 52 | 48 | 32 | 48 | Зачет с оценкой |
| | **Итоговая аттестация (междисциплинарный экзамен)** | **36** | **6** | **-** | **-** | **-** | **30** | |
| | **Итого по программе** | **576** | **412** | **178** | **128** | **100** | **164** | |

### 2.2. Календарный учебный график

*График учебных занятий разрабатывается для каждой учебной группы. Примерная форма может представляться в следующем виде*[1].

| **Месяц** | **Сентябрь** | | | | **Октябрь** | | | | **Ноябрь** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Числа | 5-10 | 12-17 | 19-24 | 26-1 | 3-8 | 10-15 | 17-22 | 24-29 | 31-5 | 7-12 | 14-19 |
| Учебная дисциплина 1.1 | | | | | | | | | | | |
| Учебная дисциплина 1.2 | | | | | | | | | | | |
| Учебная дисциплина 1.3 | | | | | | | | | | | |
| Учебная дисциплина 1.4 | | | | | | | | | | | |
| Учебная дисциплина 2.1 | | | | | | | | | | | |
| Экзамен | | | | | | | | | | | |

## 3. РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ ДИСЦИПЛИН

## МОДУЛЬ 1 «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

### 3.1. Рабочая программа учебной дисциплины «Правовые основы защиты информации»

#### 3.1.1. Цели и задачи дисциплины

**Цель дисциплины** – сформировать у слушателей профессиональные компетенции, позволяющие осуществлять деятельность по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

**Задачи дисциплины** – формирование знаний, умений и опыта деятельности в области правового обеспечения защиты информации.

[1] Разработчик вправе установить в календарном графике области пересечения учебных дисциплин, которые могут быть прочитаны в любом порядке или параллельно друг другу. Для каждой формы обучения приводится свой календарный график.

### 3.1.2. Требования к результатам освоения учебной дисциплины

**Планируемые результаты освоения программы:**

Учебная дисциплина «Правовое обеспечение защиты информации» участвует в формировании компетенций: ПК-4 «Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах».

**В результате изучения дисциплины слушатель должен иметь:**

**Знания**:

виды и носители информации;

содержание правового обеспечения информационной безопасности;

федеральные законы и Указы Президента Российской Федерации в области информационной безопасности (ИБ) и защиты информации (ЗИ);

постановления Правительства Российской Федерации в области ИБ и ЗИ;

нормативные и методические документы ФСБ России и ФСТЭК России в области ИБ и ЗИ.

государственная система обеспечения информационной безопасности и защиты информации в Российской Федерации;

правовые основы лицензирования, сертификации и аттестации в области защиты информации в Российской Федерации;

виды ответственности за нарушение законодательства в области защиты информации;

основы государственного контроля (надзора) в области защиты информации;

правовые основы защиты государственной тайны;

правовые основы защиты информации, являющейся государственным информационным ресурсом;

правовые основы защиты коммерческой тайны;

правовые основы защиты персональных данных.

**Умения**:

использовать в профессиональной деятельности нормативные правовые акты Российской Федерации в области обеспечения информационной безопасности и защиты информации;

готовить документы для получения лицензии на деятельность по защите конфиденциальной информации.

**Опыт деятельности**:

разработки документов для получения лицензии на деятельность по защите конфиденциальной информации.

### 3.1.3. Учебно-тематический план дисциплины

| № | Наименование разделов и тем | Общая трудоёмкость (часы) | Контактная работа, час | | | | Самостоятельная работа, час |
|---|---|---|---|---|---|---|---|
| | | | Всего | Лекции | Лабораторные занятия | Практические занятия | |
| 1 | Правовые основы защиты информации | 40 | 32 | 24 | – | 8 | 8 |
| | **Всего** | **40** | **32** | **24** | **–** | **8** | **8** |

### 3.1.4. Содержание дисциплины

**Перечень лекций**

| № модуля дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 2 | **Информация, как объект защиты.**<br>Информация (определение). Виды информации. Информационные отношения. Носители информации. Классификация защищаемой информации. Общедоступная информация. Информация ограниченного доступа (сведения, составляющие государственную тайну, сведения конфиденциального характера). |
| | 2. | 2 | **Содержание правового обеспечения информационной безопасности**<br>Сущность основных понятий в области обеспечения информационной безопасности (ИБ) и защиты информации (ЗИ).<br>Информация как объект права собственности.<br>Предмет, субъект, методы информационного права, информационные отношения.<br>Функции и принципы правового регулирования в области ИБ и ЗИ. |

| № модуля дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | 3. | 2 | **Система нормативных правовых актов Российской Федерации по обеспечению информационной безопасности и защиты информации**<br>Иерархия нормативных правовых актов в области ИБ и ЗИ.<br>Федеральные законы и Указы Президента Российской Федерации в области ИБ и ЗИ.<br>Постановления Правительства Российской Федерации в области ИБ и ЗИ.<br>Нормативные и методические документы ФСБ России и ФСТЭК России в области ИБ и ЗИ. |
| | 4. | 2 | **Государственная система обеспечения информационной безопасности и защиты информации в Российской Федерации.**<br>Структура органов государственного управления в области ИБ и ЗИ.<br>Полномочия, права и обязанности Президента Российской Федерации и Совета безопасности в области ИБ и ЗИ.<br>Задачи, полномочия, обязанности и права ФСБ России в области ИБ и ЗИ.<br>Задачи, полномочия, обязанности и права ФСТЭК России в области ИБ и ЗИ. |
| | 5. | 2 | **Правовые основы лицензирования и сертификации в области защиты информации в Российской Федерации.**<br>Лицензирование деятельности в области технической защиты информации (ТЗИ).<br>Лицензирование деятельности в области криптографической защиты информации.<br>Лицензирование деятельности по выявлению электронных устройств, предназначенных для негласного получения информации.<br>Сертификация средств защиты информации. |
| | 6. | 2 | **Виды ответственности за нарушение законодательства в области защиты информации.**<br>Уголовная ответственность.<br>Административная ответственность.<br>Гражданско-правовая ответственность.<br>Дисциплинарная ответственность. |

| № модуля дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | 7. | 2 | **Основы государственного контроля (надзора) в области защиты информации.**<br>Правовые основы государственного контроля (надзора) в области защиты информации.<br>Виды проверок, их содержание.<br>Ответственность за нарушения законодательства в области государственного контроля (надзора). |
| | 8. | 2 | **Правовые основы защиты государственной тайны**<br>Органы защиты государственной тайны.<br>Уровни секретности сведений. Перечень сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне.<br>Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну<br>Порядок и организация допуска должностных лиц и граждан к сведениям, составляющим государственную тайну<br>Порядок засекречивания и рассекречивания сведений, составляющих государственную тайну и их носителей. |
| | 9. | 2 | **Правовые основы защиты коммерческой тайны.**<br>Сущность и содержание коммерческой тайны.<br>Подходы к определению уровней конфиденциальности сведений, составляющих коммерческую тайну.<br>Порядок отнесения сведений к коммерческой тайне.<br>Режим коммерческой тайны. Меры по охране конфиденциальности информации, составляющей коммерческую тайну.<br>Права и обязанности работника и работодателя по защите коммерческой тайне. |
| | 10. | 2 | **Правовые основы защиты персональных данных.**<br>Сущность и содержание обработки и защиты персональных данных.<br>Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.<br>Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. |
| | 11. | 2 | **Правовые основы защиты коммерческой тайны** |

| № модуля дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Сущность и содержание коммерческой тайны. Подходы к определению уровней конфиденциальности сведений, составляющих коммерческую тайну.<br>Порядок отнесения сведений к коммерческой тайне.<br>Права и обязанности работника и работодателя по защите коммерческой тайне. |
| | 12. | 2 | **Правовые основы защиты информации в информационных системах Российской Федерации**<br>Правовые основы защиты информации в информационных системах критической информационной инфраструктуры. Обзор Федерального закона 187-ФЗ.<br>Правовые основы защиты информации в государственных информационных системах. |

**Перечень лабораторных работ**

*Не предусмотрены*

**Перечень практических занятий**

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 4 | **Практическое занятие (семинар). Нормативные правовые акты Российской Федерации в области обеспечения информационной безопасности и защиты информации.**<br>Федеральные законы и Указы Президента Российской Федерации в области ИБ и ЗИ. |

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Постановления Правительства Российской Федерации в области ИБ и ЗИ.<br>Приказы ФСБ России и ФСТЭК России в области ИБ и ЗИ. |
| | 2. | 4 | **Практическое занятие (групповое упражнение). Порядок подготовки документов для получения лицензии на деятельность по технической защите конфиденциальной информации.**<br>Лицензионные требования, предъявляемые к соискателю лицензии на осуществление деятельности по технической защите информации (ТЗИ).<br>Перечень документов, предоставляемых для получения лицензии.<br>Порядок подготовки сведений, подтверждающих квалификацию специалистов по защите информации (с указанием реквизитов дипломов, удостоверений, свидетельств).<br>Порядок подготовки сведений, подтверждающих наличие аттестованных по требованиям безопасности информации защищаемых помещений.<br>Порядок подготовки сведений, подтверждающих наличие аттестованных по требованиям безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации.<br>Порядок подготовки сведений, подтверждающих наличие контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности.<br>Порядок подготовки сведений об имеющихся технической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг.<br>Порядок подготовки сведений, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами |

Примечание: подготовка к практическим занятиям проводится в часы, выделенные для самостоятельной работы слушателей.

### 3.1.5. Учебно-методическое и информационное обеспечение дисциплины

**Литература**


1. Воеводин, В.А. Аудит информационной безопасности автоматизированных систем: учебное пособие / В. А. Воеводин, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет «МИЭТ»; под редакцией А.А. Хорева. – Москва: МИЭТ, 2021. – 208 с. – ISBN 978-5-7256-0974-5 : - Текст : непосредственный.
2. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учеб. Пособие / Ю.И. Коваленко. – М. : Горячая линия-Телеком, 2012. – 140 с. – URL: https://e.lanbook.com/book/5163 (дата обращения: 15.03.2021). – ISBN 978-5-9912-0261-9. – Текст : непосредственный.
3. Мельников, Д. А. Информационная безопасность открытых систем: учебник / Д. А. Мельников. – Москва: Флинта: Наука, 2014. – 448 с. – URL: https://e.lanbook.com/book/48368 (дата обращения: 15.03.2021). – ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7. – Текст : электронный.
4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. – М. : Юрайт, 2018. – 325 с. – (Бакалавр и магистр. Академический курс). – URL: https://urait.ru/bcode/413158 (дата обращения: 15.03.2021). – ISBN 978-5-534-03600-8. – Текст : электронный.
5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. Пособие. Ч. 1 :Правовое обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет «МИЭТ». – М. : МИЭТ, 2013. – 184 с. – Имеется электронная версия издания. – ISBN 978-5-7256-0733-8.
6. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. Пособие. Ч. 2 Организационное обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет «МИЭТ». – М. : МИЭТ, 2013. – 172 с. – ISBN 978-5-7256-0738-3.
7. Галатенко В.А. Основы информационной безопасности : Учеб. Пособие / В.А. Галатенко. – 2-е изд. – М. : ИНТУИТ, 2016. – 266 с. – URL: https://e.lanbook.com/book/100295 (дата обращения: 16.03.2021). – ISBN 978-5-94774-821-5 .
8. Воеводин, В. А. Правовые основы аудита информационной безопасности: учебное пособие / В. А. Воеводин, П. Л. Пилюгин; Министерство образования и науки РФ, Национальный исследовательский университет «МИЭТ». – Москва : МИЭТ, 2021. – 180 с. – ISBN 978-5-7256-0961-5 .

9. Программно-аппаратные средства защиты информации: учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет «МИЭТ»; под редакцией А.А. Хорева. – Москва : МИЭТ, 2021. – 280 с. – ISBN 978-5-7256-0972-1 .

10. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – 7-е изд., испр. И доп. – М. : Горячая линия-Телеком, 2018. – 444 с. – URL: https://e.lanbook.com/book/111057 (дата обращения: 16.03.2021). – ISBN 978-5-9912-0233-6.

11. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет «МИЭТ»; под редакцией А.В. Душкина. – Москва : МИЭТ, 2021. – 208 с. – ISBN 978-5-7256-0973-8 .

12. Хорев А.А. Техническая защита информации : Учеб. Пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). – М. : НПЦ Аналитика, 2008. – 436 с. – ISBN 978-59901488-1-9 .

13. Хорев П.Б. Программно-аппаратная защита информации : Учеб. Пособие / П.Б. Хорев. – М. : Форум, 2013. – 352 с. – (Высшее образование). – ISBN 978-5-91134-353-8 .

**Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы**

1. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/10102673/ - (дата обращения 12.03.2022).

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71730198/paragraph/1:0 - (дата обращения 12.03.2022).

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/12148555/- (дата обращения 12.03.2022).

4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12148567/paragraph/24880:0 - (дата обращения 12.03.2022).

5. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12136454/paragraph/12089:0- (дата обращения 12.03.2022).

6. Федеральный закон от 7 июля 2003 г. « 126-ФЗ «О связи» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/186117/paragraph/430816:0 (дата обращения 12.03.2022).

7. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями) ; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12184522/paragraph/455:0 (дата обращения 12.03.2022).

8. Федеральный закон Российской Федерации от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12185475/paragraph/5637:0 (дата обращения 12.03.2022).

9. Гражданский кодекс Российской Федерации (ГК РФ) (части первая, вторая, третья и четвертая) (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/10164072/paragraph/521837163:0 (дата обращения 12.03.2022).

10. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (КоАП РФ) (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12125267/paragraph/1:0 (дата обращения 12.03.2022).

11. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (УК РФ) (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/10108000/paragraph/26654339:0 (дата обращения 12.03.2022).

12. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/10105548/paragraph/196115:0 (дата обращения 12.03.2022).

13. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71556224/paragraph/1:0 (дата обращения 12.03.2022).

14. Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71556224/paragraph/1:0 (дата обращения 12.03.2022).

15. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/188429/ (дата обращения 12.03.2022).

16. Постановление Правительства РФ от 21.11.2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12192119/paragraph/1:0 (дата обращения 13.03.2022).

17. Постановление Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70136258/paragraph/1:0 (дата обращения 12.03.2022).

18. Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании

деятельности по разработке и производству средств защиты конфиденциальной информации); Текст: электронный// Гарант: [сайт]. – URL: https://base.garant.ru/70146250/ (дата обращения 12.03.2022).

19. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70391358/paragraph/1:0 (дата обращения 12.03.2022).

20. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70690918/paragraph/1:0 (дата обращения 12.03.2022).

21. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70380924/paragraph/1:0 (дата обращения 12.03.2022).

22. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/401599204/paragraph/1/doclist/1959/showentries/0/highlight/приказ%20фстэк%2077%20от29.04.2021:2 (дата обращения 12.03.2022).

23. Приказ ФСТЭК России от 17 июля 2017 г. № 133 «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» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71743624/paragraph/1:0 (дата обращения 12.03.2022).

24. Приказ ФСТЭК России от 17 июля 2017 г. № 134 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями)**;** Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71689708/paragraph/1/doclist/1981/showentries/0/highlight/приказ%20министерства%20спорта%20рф%20от%2028%20февраля%202017%20г.%20n%20134:3 (дата обращения 12.03.2022).

25. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55; Текст: электронный //ФСТЭК [сайт]. – URL: https://fstec.ru/component/attachments/download/1883 (дата обращения 12.03.2022).

26. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний: Национальный стандарт РФ: Введ. 13.04.2016: М.: Стандартинформ, 2015. – 35 с.*

27. ГОСТ 22505-97. Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний: Межгосударственный стандарт: Введ. 01.01.1999: М.: Издательство стандартов, 1998. – 20 с.

28. ГОСТ 30373-95/ГОСТ Р 50414-92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний. Межгосударственный стандарт: Введ. 15.05.1996: М.: Издательство стандартов, 1996. – 17 с.

29. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Национальный стандарт РФ: Введ. 01.01.1996: М.: Стандартинформ, 2006. – 6 с.

30. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 27.12.2006: М.: Стандартинформ, 2006. – 8 с.

31. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, 2007. – 7 с.

32. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: Национальный стандарт РФ: Введ. 28.01.2014.- М.: Стандартинформ, 2014. – 18 с.

33. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества: Национальный стандарт РФ: Введ. 28.12.2005.- М.: Стандартинформ, 2006. – 27 с.

34. ГОСТ Р 53112-2008. Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний: Национальный стандарт РФ: Введ. 18.12.2008. - М.: Стандартинформ, 2009. – 24 с.

35. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: Национальный стандарт РФ: Введ. 01.10.2009: М.: Стандартинформ, 2009. - 20 с.

36. ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства: Национальный стандарт РФ: Введ. 18.12.2009: М.: Стандартинформ, 2009. - 31 с.

37. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: Национальный стандарт РФ: Введ. 15.11.2012:

М.: Стандартинформ, 2014. – 54 с.

38. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности: Национальный стандарт РФ: Введ. 08.01.2013: М.: Стандартинформ, 2014. – 161 с.

39. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности: Национальный стандарт РФ: Введ. 08.11.2013: М.: Стандартинформ, 2014. – 150 с.

40. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации: Национальный стандарт РФ: Введ. 06.04.2005. - М.: Стандартинформ, 2005. – 16 с.

41. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 29.12.2005.- М.: Стандартинформ, 2006. – 20 с.

42. СНиП 23-03-2003. Защита от шума. Введ. 30.06.2003. - М.: Госстрой России, 2004. – 34 с.

43. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij- (дата обращения 12.03.2022).

44. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/component/content/article/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot (дата обращения 12.03.2022).

45. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g4 (дата обращения 12.03.2022).

46. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/component/content/article/114-tekhnicheskaya-zashchitainformatsii/

dokumenty/spetsialnye-normativnye-dokumenty/385rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissiirossii-ot-30-marta-1992-g2 (дата обращения 12.03.2022).

47. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyuly (дата обращения 12.03.2022).

48. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.*

49. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения 12.03.2022).

50. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения 12.03.2022).

51. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114spetsialnye-normativnye-dokumenty/379bazovaya-model-ugroz-bezopasnosti-perso-nalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii2008god (дата обращения 12.03.2022).

## Периодические издания

1. Безопасность информационных технологий: научный журнал / ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ». - Москва: НИЯУ МИФИ, 1994 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8429 (дата обращения: 12.03.2022). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011-.- URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

3. Information Security/Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Текст: электронный.

4. Вопросы кибербезопасности: научный журнал. - Москва: НПО «Эшелон», 2013. – URL: http://cyberrus.com/ (дата обращения: 12.03.2022). – Текст: электронный.

5. Защита информации. Inside : информационно-методический журнал/ Издательский дом «Афина». - Санкт-Петербург: ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 12.03.2022). - Режим доступа: по подписке (2017-2022). - ISSN 2413-3582. - Текст : электронный

6. Jet Info/Инфосистемы Джет. – URL: http://www.jetinfo.ru (дата обращения: 12.03.2022). – Режим доступа: свободный.

7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 12.03.2022). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

**Перечень профессиональных баз данных, информационных справочных систем**

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 12.03.2022). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: https://e.lanbook.com (дата обращения: 12.03.2022). - Текст: электронный.

3. ФСТЭК России: сайт. М.: -.- URL: https://fstec.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

4. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 12.03.2022). - Текст: электронный.

5. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 12.03.2022). - Текст: электронный.

6. Бюро научно-технической информации «Техника для спецслужб»: сайт. – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Текст : электронный.

7. ФСБ России: сайт. М.: -.- URL: http://fsb.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

### 3.1.6. Материально-техническое обеспечение дисциплины

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| Специализированная мультимедийная аудитория | Лекции, практические занятия | Мультимедийное оборудование: компьютер, подключенный к сети Интернет и доступом в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (звуковые колонки), вебкамера с микрофоном. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). Учебная доска. |
| Помещение для самостоятельной работы слушателей (кл. 3226) | Самостоятельная работа слушателей | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). 2. Автоматизированное рабочее место студента (27 шт) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). |

### 3.1.7. Система контроля и оценивания

Оценка качества освоения дисциплины включает текущую и промежуточную аттестацию слушателей.

Текущий контроль освоенных знаний осуществляется в виде оценок за контрольные мероприятия:

– доклады (выступления) на семинаре;

– отчеты по выполнению заданий на групповых упражнениях;

– компьютерные тесты по разделам дисциплины.

Промежуточная аттестация по дисциплине осуществляется в виде зачета с оценкой.

Итоговая оценка за дисциплину выставляется по 5-ти балльной шкале на основе среднего балла за контрольные мероприятия. При выставлении итоговой оценки используется шкала, приведенная в таблице.

Таблица

**Критерии выставления итоговой оценки по дисциплине**

| Средний балл за контрольные мероприятия $N_{ср}$ | Оценка |
|---|---|
| $N_{ср} < 3$ | 2 |
| $3 \le N_{ср} < 3{,}5$ | 3 |
| $3{,}5 \le N_{ср} < 4{,}5$ | 4 |
| $N_{ср} \ge 4{,}5$ | 5 |

## 3.2. Рабочая программа учебной дисциплины «Защита информации от утечки по техническим каналам»

### 3.2.1. Цели и задачи дисциплины

**Цель дисциплины** – сформировать у слушателей профессиональные компетенции, позволяющие осуществлять деятельность по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

**Задачи дисциплины** – формирование знаний, умений и опыта деятельности в области защиты информации от утечки по техническим каналам.

### 3.2.2. Требования к результатам освоения учебной дисциплины

**Планируемые результаты освоения программы:**

Дисциплина «Защита информации от течки по техническим каналам» участвует в формировании компетенций:

ПК-1 «Способен проводить работы по установке и настройке средств технической защиты информации и защищенных технических средств обработки информации».

**В результате изучения дисциплины слушатель должен:**

**Знать**:

цели и задачи защиты информации от утечки по техническим каналам;

технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ), возможности специальных технических средств по перехвату информации, обрабатываемой СВТ;

технические каналы утечки акустической речевой информации, возможности средств акустической речевой разведки по перехвату разговоров из выделенных помещений;

принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам;

принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам;

методы и средства контроля эффективности защиты СВТ от утечки информации по техническим каналам;

методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам.

**Уметь:**

проводить анализ потенциальных технических каналов утечки информации на объектах информатизации, рассчитывать опасные зоны R2 и r1;

проводить анализ потенциальных технических каналов утечки речевой информации в выделенных помещениях, рассчитывать словесную разборчивость речи;

проводить работы по установке и настройке средств защиты СВТ от утечки информации по техническим каналам;

проводить работы по установке и настройке средств защиты речевой информации от ее утечки по техническим каналам;

проводить контроль и оценку выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН;

проводить контроль и оценку выполнения норм защищенности акустической речевой информации от утечки по техническим каналам.

**Иметь опыт практической деятельности:**

проведения работ по установке и настройке средств защиты информации от ее утечки по техническим каналам.

### 3.2.3. Учебно-тематический план дисциплины

| № | Наименование разделов | Общая трудоёмкость (часы) | Контактная работа, час | | | | Самостоятельная работа, час |
|---|---|---|---|---|---|---|---|
| | | | Всего | Лекции | Лабораторные занятия | Практические занятия | |
| 1 | Технические каналы утечки информации | 44 | 32 | 12 | 12 | 8 | 12 |
| 2 | Способы и средства защиты информации от утечки ее утечки по техническим каналам | 38 | 30 | 14 | 16 | – | 8 |
| 3 | Методы и средства контроля защищенности информации от ее утечки по техническим каналам | 32 | 24 | 8 | 8 | 8 | 8 |
| | **Всего** | **114** | **86** | **34** | **36** | **16** | **28** |

### 3.2.4. Содержание дисциплины

**Перечень лекций**

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 2 | **Вводная лекция. Цели и задачи защиты информации от утечки информации по техническим каналам.** Термины и определения в области защиты информации от утечки по техническим каналам: объект информатизации, выделенное помещение, ОТСС, ВТСС, посторонние проводники, контролируемая зона, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, технический канал утечки информации. Цели и задачи защиты информации от утечки информации по техническим каналам. |
| | 2. | 2 | **Электромагнитные технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ).** |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Классификация технических каналов утечки информации, обрабатываемой СВТ. Причины возникновения побочных электромагнитных излучений (ПЭМИ) СВТ. Принципы построения средств перехвата ПЭМИ СВТ. Опасная зона R2. Схема технического канала утечки информации, возникающего за счет ПЭМИ СВТ. |
| | 3. | 2 | **Электрические и специально создаваемые технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ)**<br>Причины возникновения электрических технических каналов утечки информации, обрабатываемой СВТ.<br>Случайные антенны. Причины возникновения наводок информативных сигналов в случайных антеннах. Опасная зон r1. Схема технического канала утечки информации, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах. Причины возникновения наводок информативных сигналов в линиях электропитания и цепях заземления СВТ. Схемы технических каналов утечки информации, возникающих за счет наводок ПЭМИ СВТ в линиях электропитания и цепях заземления СВТ.<br>Схема перехвата информации путем «высокочастотного облучения» СВТ. Основные характеристики аппаратуры «высокочастотного облучения».<br>Схема перехвата информации путем внедряемых в СВТ электронных устройств перехвата информации. Основные виды электронных устройств перехвата информации, внедряемых в СВТ. |
| | 4. | 2 | **Характеристики речи. Классификация технических каналов утечки акустической (речевой) информации.**<br>Акустические сигналы. Линейные и энергетические характеристики акустического поля. Характеристики речи (семантические, фонетические, физические). Спектр и типовые уровни речевого сигнала. Разборчивость речи. Методы оценки разборчивости речи. Общая характеристика и классификация технических каналов утечки акустической (речевой) информации. |
| | 5. | 2 | **Прямые акустические каналы утечки речевой информации.**<br>Схемы перехвата информации по прямым акустическим каналам утечки информации. Средства акустической разведки с датчиками |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | микрофонного типа: цифровые диктофоны, электронные устройства перехвата речевой информации, направленные микрофоны. |
| | 6. | 2 | **Акустовибрационные, акустооптический, акустоэлектрические и акустоэлектромагнитные каналы утечки речевой информации.** Схемы перехвата речевой информации по акустовибрационным каналам. Электронные стетоскопы. Радиостетосскопы. Схема перехвата речевой информации по акустооптическому каналу. Лазерные акустические системы разведки. Причины возникновения акустоэлектрических каналов утечки речевой информации. Акустоэлектрические преобразователи генераторного типа. Акустоэлектрические преобразователи модуляторного типа. Схема пассивного акустоэлектрического канала утечки речевой информации. Схема активного акустоэлектрического канала утечки речевой информации. Схема пассивного акустоэлектромагнитного канала утечки речевой информации. Схема активного акустоэлектромагнитного канала утечки речевой информации. |
| 2 | 7. | 2 | **Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам.** Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Пассивные способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Активные способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Защищенные ПЭВМ. |
| | 8. | 2 | **Экранирование и заземление технических средств.** Экранирование технических средств их соединительных линий. Экранирующие материалы. Экранированные помещения (экранированные камеры). Заземление технических средств. Требования к заземлению ОТСС. Схемы заземления ОТСС. Методы и средства измерения сопротивления заземления ОТСС. |
| | 9. | 2 | **Системы пространственного электромагнитного зашумления**. |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Требования к системе пространственного электромагнитного зашумления. Принципы построения широкополосных генераторов шума. Системы пространственного электромагнитного зашумления типа А (состав, основные характеристики, требования по установке). Особенности зашумления инженерных коммуникаций. |
| | 10. | 2 | **Способы и средства защиты объектов информатизации от утечки информации по цепям электропитания и заземления.** Требования к системе электропитания ОТСС. Требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания СВТ. Принципы построения, основные характеристики и требования по установке помехоподавляющих фильтров. Системы линейного электромагнитного зашумления типа Б (состав, основные характеристики, требования по установке). |
| | 11. | 2 | **Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.** Пассивные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Активные способы защиты выделенных помещений от утечки речевой информации по техническим каналам. Звуко- и виброизоляция выделенных помещений, глушители шума. Звукопоглощающие материалы. Специальные защищенные помещения. |
| | 12. | 2 | **Системы и средства виброакустической маскировки.** Требования к системе виброакустической маскировки. Принципы построения низкочастотных генераторов шума. Принципы построения акустических излучателей и виброизлучателей. Системы виброакустической маскировки типа А. Системы виброакустической маскировки типа Б. Особенности установки акустических излучателей и виброизлучателей. Специальная аппаратура для ведения конфиденциальных переговоров. |
| | 13. | 2 | **Средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам.** Пассивные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам (ограничение сигналов малой |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | амплитуды, фильтрация высокочастотных сигналов навязывания, отключение акустоэлектрических преобразователей опасных сигналов). Активные способы защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам.<br>Принципы построения и основные характеристики средств защиты ВТСС, основанных на использовании ограничителей малой амплитуды и фильтров нижних частот. Принципы построения основные характеристики средств защиты ВТСС, основанных на отключении акустоэлектрических преобразователей. Принципы построения основные характеристики средств защиты ВТСС, основанных на использовании низкочастотных генераторов шума. |
| 3 | 14. | 2 | **Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ:**<br>Показатели эффективности защиты информации, обрабатываемой СВТ, от утечки по техническим каналам. Методы контроля эффективности защиты информации, обрабатываемой СВТ.<br>Требования к средствам измерения ПЭМИН СВТ и условиям проведения измерений. |
| | 15. | 2 | **Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН:**<br>Порядок проведения аттестационных испытаний СВТ при контроли эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИ.<br>Порядок проведения аттестационных испытаний СВТ при контроле эффективности защиты СВТ от утечки<br>информации, возникающей за счет наводок информативных сигналов на токопроводящие коммуникации. |
| | 16. | 2 | **Методы и средства контроля выполнения норм защищенности речевой информации от утечки по техническим каналам:**<br>Показатели защищенности речевой информации от утечки речевой информации по техническим каналам. Методы контроля эффективности защиты ВП от утечки речевой информации по техническим каналам. |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по прямым акустическим, акустовибрационным и акустооптическому каналам. Требования к средствам измерения при контроле выполнения норм защищенности речевой информации от утечки по акустоэлектрическим каналам. |
| | 17. | 2 | **Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по техническим каналам:** Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам. Порядок проведения контроля выполнения норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам. Порядок проведения контроля ВТСС на подверженность акустоэлектрическим преобразованиям. Порядок проведения контроля ВТСС на подверженность «высокочастотному навязыванию». |

**Перечень лабораторных работ**

| № раздела дисциплины | № лабораторной работы | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 4 | **Исследование побочных электромагнитных излучений (ПЭМИ) ПЭВМ:** Исследование ПЭМИ видеосистемы монитора ПЭВМ. Исследование ПЭМИ клавиатуры ПЭВМ. Исследование ПЭМИ съемных носителей ПЭВМ. |
| | 2. | 4 | **Исследование акустических и акустовибрационых каналов утечки речевой информации:** Исследование вибрационных сигналов, возбуждаемых в ограждающих конструкциях при ведении разговоров в помещении. |

| № раздела дисциплины | № лабораторной работы | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Измерение звукоизоляции помещения (двери в помещение). |
| | 3. | 4 | **Исследование акустоэлектрических каналов утечки информации**<br>Исследование пассивного акустоэлектрического канала утечки информации<br>Исследование канала утечки информации, создаваемого методом «высокочастотного навязывания» |
| 2. | 4. | 4 | **Установка, настройка и измерение основных характеристик систем пространственного и линейного электромагнитного зашумления:**<br>Установка и настройка систем пространственного и линейного электромагнитного зашумления (типа Гном-3, ГШ-1000У, ЛГШ-503, Соната-Р2, SP-44).<br>Измерение спектров помеховых сигналов систем пространственного электромагнитного зашумления (Гном-3, ГШ-1000У, ЛГШ-503, Соната-Р2).<br>Измерение спектров помеховых сигналов, создаваемых в инженерных коммуникациях системой линейного электромагнитного зашумления (ГШ-1000У).<br>Измерение спектров помеховых сигналов, создаваемых в сети 220 В системой линейного электромагнитного зашумления (SP-44). |
| | 5. | 4 | **Установка и измерение характеристик помехоподавляющих фильтров**<br>Установка помехоподавляющих фильтров (типа ФП-8, ФСП=1Ф-10А).<br>Измерение характеристик помехоподавляющего фильтра ФП-8.<br>Измерение характеристик помехоподавляющего фильтра ФСП-1Ф-10А. |
| | 6. | 4 | **Установка, настройка и измерение характеристик систем виброакустической защиты.**<br>Установка и настройка системы виброакустической защиты (типа Соната 3Б).<br>Измерение характеристик акустического шумового сигнала, излучаемого генератором - акустическим излучателем (типа Соната 3Б). |

| № раздела дисциплины | № лабораторной работы | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Измерение характеристик вибрационных шумовых сигналов, возбуждаемых в стене, инженерной коммуникации, оконном стекле генераторами-виброизлучателями при различных режимах их работы. |
| | 7. | 4 | **Установка, настройка и измерение характеристик средств защиты телефонных аппаратов от утечки информации по акустоэлектрическим каналам.**<br>Установка средств защиты телефонных аппаратов от утечки информации по акустоэлектрическим каналам (типа Гранит-8, МП-8, МП-1А).<br>Измерение характеристик пассивных средств защиты телефонных аппаратов от утечки информации по техническим каналам (Гранит-8, МП-8).<br>Измерение характеристик активных средств защиты телефонных аппаратов от утечки информации по техническим каналам (МП-1А). |
| 3 | 8. | 4 | **Контроль защищенности СВТ от утечки информации по каналам ПЭМИН:**<br>Измерение ПЭМИ видеосистемы монитора ПЭВМ.<br>Измерение реального затухания ПЭМИ СВТ.<br>Измерение наводок ПЭМИ видеосистемы монитора ПЭВМ в цепях электропитания.<br>Измерение уровня напряженности поля помеховых сигналов, создаваемых системой электромагнитного зашумления.<br>Измерение уровня помеховых сигналов, создаваемых в инженерных коммуникациях системой электромагнитного зашумления. |
| | 9. | 4 | **Контроль защищенности речевой информации от утечки по техническим каналам**<br>Измерение уровня звукоизоляции выделенного помещения.<br>Измерение уровня вибрационных сигналов, возбуждаемых в оконном стекле и инженерной коммуникации.<br>Измерение уровня вибрационных шумов, создаваемых системой виброакустической защиты, в оконном стекле и инженерной коммуникации. |

Примечание: подготовка к лабораторным работам проводится в часы, выделенные для самостоятельной работы слушателей.

**Перечень практических занятий**

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 4 | **Практическое занятие (групповое упражнение). Оценка возможностей по перехвату ПЭМИ СВТ средствами разведки.** Расчет опасной зоны *R2.* Расчет опасной зоны *r1.* |
| | 2. | 4 | **Практическое занятие (групповое упражнение). Оценка возможностей по перехвату речевой информации средства акустической разведки.** Оценка возможности непреднамеренного прослушивания речи. Оценка возможности перехвата речевой информации направленными микрофонами. |
| 3. | 3. | 4 | **Практическое занятие (групповое упражнение). Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИН:** Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИ при использовании средств экранирования. Оценка выполнения норм защищенности СВТ от утечки информации по каналам ПЭМИ при использовании системы пространственного электромагнитного зашумления. Оценка выполнения норм защищенности СВТ от утечки информации, возникающей за счет наводок ПЭМИ в линиях электропитания и в токопроводящих коммуникациях при использовании системы линейного электромагнитного зашумления. |
| | 4. | 4 | **Оценка выполнения норм защищенности речевой информации от утечки по техническим каналам:** Оценка выполнения норм защищенности речевой информации от утечки по прямым акустическим каналам. |

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Оценка выполнения норм защищенности речевой информации от утечки по акустовибрационным и акустооптическому каналам. |

Примечание: подготовка к практическим занятиям проводится в часы, выделенные для самостоятельно работы слушателей.

### 3.2.5. Учебно-методическое и информационное обеспечение дисциплины

#### Литература


1. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 15.03.2021). - ISBN 978-5-9912-0233-6. - Текст : электронный.
2. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 . - Текст : электронный.
3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: учебн. пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.: ил.


#### Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы


1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/12148555/- (дата обращения 12.03.2022).
2. Федеральный закон Российской Федерации от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями); Текст:

электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12185475/paragraph/5637:0 (дата обращения 12.03.2022).

3. Постановление Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70136258/paragraph/1:0 (дата обращения 12.03.2022).

4. Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации); Текст: электронный// Гарант: [сайт]. – URL: https://base.garant.ru/70146250/ (дата обращения 12.03.2022).

5. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/401599204/paragraph/1/doclist/1959/showentries/0/highlight/приказ%20фстэк%2077%20от29.04.2021:2 (дата обращения 12.03.2022).

6. Приказ ФСТЭК России от 17 июля 2017 г. № 133 «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» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71743624/paragraph/1:0 (дата обращения 12.03.2022).

7. Приказ ФСТЭК России от 17 июля 2017 г. № 134 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями)**;** Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71689708/paragraph/1/doclist/1981/showentries/0/highlight/приказ%20министерства%20спорта%20рф%20от%2028%20февраля%202017%20г.%20n%20134:3 (дата обращения 12.03.2022).

8. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний: Национальный стандарт РФ: Введ. 13.04.2016: М.: Стандартинформ, 2015. – 35 с.*

9. ГОСТ 22505-97. Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний: Межгосударственный стандарт: Введ. 01.01.1999: М.: Издательство стандартов, 1998. – 20 с.

10. ГОСТ 30373-95/ГОСТ Р 50414-92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний. Межгосударственный стандарт: Введ. 15.05.1996: М.: Издательство стандартов, 1996. – 17 с.

11. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от

несанкционированного доступа к информации. Общие технические требования: Национальный стандарт РФ: Введ. 01.01.1996: М.: Стандартинформ, 2006. – 6 с.

12. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 27.12.2006: М.: Стандартинформ, 2006. – 8 с.

13. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, 2007. – 7 с.

14. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: Национальный стандарт РФ: Введ. 28.01.2014.- М.: Стандартинформ, 2014. – 18 с.

15. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества: Национальный стандарт РФ: Введ. 28.12.2005.- М.: Стандартинформ, 2006. – 27 с.

16. ГОСТ Р 53112-2008. Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний: Национальный стандарт РФ: Введ. 18.12.2008. - М.: Стандартинформ, 2009. – 24 с.

17. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: Национальный стандарт РФ: Введ. 01.10.2009: М.: Стандартинформ, 2009. - 20 с.

18. ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства: Национальный стандарт РФ: Введ. 18.12.2009: М.: Стандартинформ, 2009. - 31 с.

19. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации: Национальный стандарт РФ: Введ. 06.04.2005. - М.: Стандартинформ, 2005. – 16 с.

20. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 29.12.2005.- М.: Стандартинформ, 2006. – 20 с.

21. СНиП 23-03-2003. Защита от шума. Введ. 30.06.2003. - М.: Госстрой России, 2004. – 34 с.

22. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.*

23. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения 12.03.2022).

24. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения 12.03.2022).

25. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.*

26. Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.*

27. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.*

28. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.*

**Периодические издания**

1. Безопасность информационных технологий: научный журнал / ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ». - Москва: НИЯУ МИФИ, 1994 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8429 (дата обращения: 12.03.2022). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011-.- URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

3. Information Security/Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Текст: электронный.

4. Вопросы кибербезопасности: научный журнал. - Москва: НПО «Эшелон», 2013. – URL: http://cyberrus.com/ (дата обращения: 12.03.2022). – Текст: электронный.

5. Защита информации. Inside : информационно-методический журнал/ Издательский дом «Афина». - Санкт-Петербург: ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 12.03.2022). - Режим доступа: по подписке (2017-2022). - ISSN 2413-3582. - Текст : электронный

6. Jet Info/Инфосистемы Джет. – URL: http://www.jetinfo.ru (дата обращения: 12.03.2022). – Режим доступа: свободный.

7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 12.03.2022). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

**Перечень профессиональных баз данных, информационных справочных систем**

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 12.03.2022). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: https://e.lanbook.com (дата обращения: 12.03.2022). - Текст: электронный.
3. ФСТЭК России: сайт. М.: -.- URL: https://fstec.ru/ (дата обращения: 12.03.2022). – Текст: электронный.
4. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 12.03.2022). - Текст: электронный.
5. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 12.03.2022). - Текст: электронный.
6. Бюро научно-технической информации «Техника для спецслужб»: сайт. – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Текст : электронный.
7. ФСБ России: сайт. М.: -.- URL: http://fsb.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

### 3.2.6. Материально-техническое обеспечение дисциплины

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| Специализированная мультимедийная аудитория | Лекции, практические занятия | Мультимедийное оборудование: компьютер, подключенный к сети Интернет и доступом в электронно-образовательную среду МИЭТ; |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| | | телевизор/проектор; акустическое оборудование (звуковые колонки), вебкамера с микрофоном. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). Учебная доска. |
| Учебная аудитории № 3225Б: Лаборатория «Технической защиты информации» | Лабораторные работы | 1) Программно-технический комплекс (лабораторная установка) для исследования побочных электромагнитных излучений (ПЭМИ) СВТ (ЛУ 01)<br>2) Программно-технический комплекс (лабораторная установка) для исследования реального затухания ПЭМИ СВТ и их наводок (ЛУ 02).<br>3) Программно-технический комплекс (лабораторная установка) для исследования систем пространственного и линейного электромагнитного зашумления (ЛУ 03).<br>4) Программно-технический комплекс (лабораторная установка) для исследования характеристик помехоподавляющих фильтров (ЛУ 04).<br>5) Программно-технический комплекс (лабораторная установка) для исследования прямых акустических, акусто-вибрационных каналов утечки информации и систем виброакустической маскировки (ЛУ 05).<br>6) Программно-технический комплекс (лабораторная установка) для исследования акустоэлектрических каналов утечки информации и средств защиты вспомогательных технических средств (ВТСС) (ЛУ 06).<br>Автоматизированное рабочее место |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| | | преподавателя (АРМ-П). |
| Помещение для самостоятельной работы слушателей (кл. 3226) | Самостоятельная работа слушателей | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). 2. Автоматизированное рабочее место студента (27 шт.) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). (27 шт.). |

### 3.2.7. Система контроля и оценивания

Оценка качества освоения дисциплины включает текущую и промежуточную аттестацию слушателей.

Текущий контроль освоенных знаний осуществляется в виде оценок за контрольные мероприятия:

– отчеты по выполнению заданий по лабораторным работам;

– отчеты по выполнению заданий на групповых упражнениях;

– компьютерные тесты по разделам дисциплины.

Промежуточная аттестация по дисциплине осуществляется в виде зачета с оценкой.

Итоговая оценка за дисциплину выставляется по 5-ти балльной шкале на основе среднего балла за контрольные мероприятия. При выставлении итоговой оценки используется шкала, приведенная в таблице.

Таблица

**Критерии выставления итоговой оценки по дисциплине**

| Средний балл за контрольные мероприятия $N_{ср}$ | Оценка |
|---|---|
| $N_{ср} < 3$ | 2 |
| $3 \le N_{ср} < 3{,}5$ | 3 |

| | |
|---|---|
| $3{,}5 \le N_{ср} < 4{,}5$ | 4 |
| $N_{ср} \ge 4{,}5$ | 5 |

## 3.3. Рабочая программа учебной дисциплины «Защита информации от несанкционированного доступа»

### 3.3.1. Цели и задачи дисциплины

**Цель дисциплины** – сформировать у слушателей профессиональные компетенции, позволяющие осуществлять деятельность по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

**Задачи дисциплины** – формирование знаний, умений и опыта деятельности в области защиты информации от несанкционированного доступа.

### 3.3.2. Требования к результатам освоения учебной дисциплины

**Планируемые результаты освоения программы:**

Дисциплина «Защита информации от несанкционированного доступа» участвует в формировании компетенций:

ПК-1 «Способен проводить работы по установке и настройке средств технической защиты информации и защищенных технических средств обработки информации».

**В результате изучения дисциплины слушатель должен:**

**Знать**:

угрозы несанкционированного доступа к информации при ее обработке в автоматизированных системах (АС);

модели нарушителя;

технологии идентификации и аутентификации;

модели управления доступом;

технологии управления доступом к информации, использующие дискреционный принцип;

технологии управления доступом к информации, использующие мандатный принцип;

технологии управления доступом к информации, использующие ролевой принцип;

технологии управления доступом для обеспечения целостности информации;

технологии контроля доступа в вычислительных сетях, технологии обеспечения изоляции, изоляция в сети, защищенные сетевые протоколы;

основные требования по защите автоматизированных систем от несанкционированного доступа к информации;

средства аутентификации и доверенной загрузки;

средства (системы) защиты информации от несанкционированного доступа;

антивирусные программы;

средства сетевой безопасности, средства создания виртуальных защищенных сетей;

средства контроля защищенности информации от несанкционированного доступа;

сканеры безопасности.

**Уметь:**

проводить настройку средств безопасности ОС Windows;

проводить установку и настройку средств антивирусной защиты информации;

проводить установку и настройку программных и программно-аппаратных средств защиты информации от несанкционированного доступа к информации;

проводить установку и настройку средств межсетевого экранирования;

проводить контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием средств контроля защищенности информации;

проводить контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием сканеров безопасности.

**Иметь опыт практической деятельности:**

проведения работ по установке и настройке средств защиты АС информации от несанкционированного доступа к информации.

### 3.3.3. Учебно-тематический план дисциплины

| № | Наименование разделов и тем | Общая трудоёмкость (часы) | Контактная работа, час | | | | Самостоятельная работа, час |
|---|---|---|---|---|---|---|---|
| | | | Всего | Лекции | Лабораторные занятия | Практические занятия | |
| 1. | Угрозы безопасности информации, обрабатываемой в автоматизированных системах и вычислительных сетях | 14 | 10 | 6 | 4 | – | 4 |
| 2. | Способы и технологии защиты информации от несанкционированного доступа | 42 | 34 | 18 | 16 | – | 8 |
| 3. | Системы и средства защиты информации от несанкционированного доступа | 52 | 40 | 16 | 24 | – | 12 |
| | **Всего** | **108** | **84** | **40** | **44** | – | **24** |

### 3.3.4. Содержание дисциплины

**Перечень лекций**

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 2 | **Классификация угроз безопасности информации при ее обработке в автоматизированных системах (АС).**<br>Классификация угроз несанкционированного доступа к информации в АС.<br>Общая характеристика источников угроз несанкционированного доступа в АС. Общая характеристика уязвимостей АС. Угрозы программно-математических воздействий.<br>Модели нарушителя. |
| | 2. | 2 | **Сетевые атаки**<br>Субъекты и объекты компьютерных атак в сетях, виды сетевых атак.<br>Пассивные сетевые атаки: атаки, не нарушающие функционирование сети. Анонимное сканирование. Активные сетевые атаки: атаки на слабости протоколов. Имперсонация. Методы внедрения ложного сервера. MITM атаки. Методы десинхронизации TCP соединений. DOS атаки. |
| | 3. | 2 | **Угрозы программно-математических воздействий**<br>Вредоносные программы и их классификация.<br>Программные закладки. Программные вирусы. Сетевые черви.<br>Недекларированные возможности программного обеспечения.<br>Скрытые каналы утечки информации. |
| 2. | 4. | 2 | **Классификация способов защиты информации от несанкционированного доступа**<br>Классификация способов защиты информации от несанкционированного доступа: управление доступом; регистрация и учет; обеспечение целостности; контроль отсутствия недекларированных возможностей; антивирусная защита; криптографическая защита информации; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений; предотвращение утечек и т.д. |
| | 5. | 2 | **Технологии идентификации и аутентификации**<br>Аутентификация, авторизация и идентификация (определения). Технологии аутентификации: одноразовые пароли, многоразовые |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | пароли, базы учетных записей, многофакторная аутентификация. Технологии аутентификации пользователей по специальным устройствам. Технологии аутентификации пользователей по биометрическим характеристикам человека. Технологии идентификации и аутентификации используемых компонентов обработки информации (аппаратных и программных средств). Особенности аутентификации в вычислительных сетях. |
| | 6. | 2 | **Модели управления доступом**<br>Модель системы защиты с полным перекрытием, субъектно-объектная модель системы защиты, понятие изолированной системы, особенности моделирования механизмов безопасности операционных систем и баз данных, основные виды моделей политик управления доступом – ограниченность моделей и проблемы изменения прав доступа. |
| | 7. | 2 | **Технологии управления доступом к информации, использующие дискреционный принцип**<br>Технологии управления доступом к АРМ и серверам. Технологии управления учетными записями. Дискреционный принцип доступа. Модели Грехема-Денинига, Хартсона, HRU, T-G. Реализации этих моделей в информационных системах. Сравнение результатов моделирования. |
| | 8. | 2 | **Технологии управления доступом к информации, использующие мандатный принцип**<br>Принципы военной безопасности MLS. Понятие решетки безопасности. Модель Деннинга. Технологии управления доступом на основе мандатного принципа. Модели Белла-ЛаПадулы (простая, RW, классическая и пр.). Реализации этих моделей в информационных системах. |
| | 9. | 2 | **Технологии управления доступом к информации, использующие ролевой принцип**<br>Принципы ролевого подхода. Примеры и типы ролевых моделей. Индивидуально-групповое управление доступом. Реализации ролевых моделей в информационных системах. |
| | 10. | 2 | **Технологии управления доступом для обеспечения целостности информации** |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Основные требования к подсистеме обеспечения целостности информации. Подсистема резервного копирования: основные требования к подсистеме резервного копирования; типы резервного копирования; типы резервных носителей; хранение и использование резервных копий; архитектура подсистемы резервного копирования. Подсистема распределения обновлений: основные требования к подсистеме распределения обновлений; возможные варианты построения системы; архитектура подсистемы распределения обновлений. Модель Биба. |
| | 11. | 2 | **Технологии контроля доступа в вычислительных сетях**<br>Задачи фильтрации сетевого трафика. Межсетевые экраны. Фильтрация пакетов. Коммутация каналов. Анализ приложений. Анализ состояний. Прокси сервер. Понятие DMZ |
| | 12. | 2 | **Технологии обеспечения изоляции, изоляция в сети, защищенные сетевые протоколы**<br>Основные требования к обеспечению изоляции. Изоляция в операционных системах, в СУБД, в сетях. Реализации технологии изоляции.<br>Протоколы IPv6, IPsec, SSL, TLS, PPTP. Построение VPN |
| 3. | 13. | 2 | **Основные требования по защите автоматизированных систем от несанкционированного доступа к информации**<br>Состав системы защиты автоматизированной системы (АС) от несанкционированного доступа к информации (НСД).<br>Классификация АС. Требования по защите информации от НСД для АС различных классов.<br>Показатели защищенности СВТ от НСД. Требования к показателям защищенности СВТ различных классов.<br>Классификация межсетевых экранов (МЭ).<br>Требования к различным классам защищенности МЭ. |
| | 14. | 2 | **Средства аутентификации и доверенной загрузки**<br>Типы средств аутентификации. Обзор современных средств аутентификации.<br>Типы средств доверенной загрузки. Обзор современных программно-аппаратных средств доверенной загрузки. |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | 15. | 2 | **Средства (системы) защиты информации от несанкционированного доступа**<br>Типовой состав и назначение системы защиты информации (СЗИ) от НСД.<br>Задачи, решаемые СЗИ от НСД.<br>Обзор современных СЗИ от НСД. |
| | 16. | 2 | **Средства защиты информации от вредоносного программного обеспечения**<br>Сертифицированные средства антивирусной защиты.<br>Средства антивирусной защиты иностранного производства. |
| | 17. | 2 | **Средства сетевой безопасности**<br>Межсетевые экраны.<br>Средства обнаружения вторжений. |
| | 18. | 2 | **Средства создания виртуальных защищенных сетей**<br>Основные принципы организации виртуальных частных сетей.<br>Типовые средства создания виртуальных частных сетей. |
| | 19. | 2 | **Средства контроля защищенности информации от несанкционированного доступа**<br>Средство фиксации и контроля исходного состояния.<br>Средство контроля защищенности от несанкционированного доступа.<br>Средства поиска и гарантированного уничтожения информации. |
| | 20. | 2 | **Сканеры безопасности**<br>Основные принципы работы сканеров безопасности.<br>Обзор современных сканеров безопасности. |

**Перечень лабораторных работ**

| № раздела дисциплины | № лабораторной работы | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 4 | **Исследование сетевых атак** |

| № раздела дисциплины | № лабораторной работы | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 2. | 2. | 4 | **Технологии управления доступом. Управление потоками информации.** |
| | 3. | 4 | **Технологии разграничения доступа. Реализация матрицы доступа и проверка введенных ограничений по доступу в операционной системе.** |
| | 4. | 4 | **Технологии проверки целостности данных и резервирование. Технологии восстановления системного и прикладного программного обеспечения после сбоев и отказов оборудования и программно-математического воздействия.** |
| | 5. | 4 | **Технологии межсетевого экранирования.** |
| 3. | 6. | 4 | **Настройка средств системного администрирования операционными системами** (на примере операционной системы Windows). |
| | 7. | 4 | **Установка и настройка средств защиты информации от несанкционированного доступа** (на примере СЗИ от НСД «DallasLock»). |
| | 8. | 4 | **Установка и настройка средств антивирусной защиты информации** (на примере Dr.Web Security Space, Kaspersky Anti-Virus). |
| | 9. | 4 | **Установка и настройка средств сетевой безопасности** (на примере СЗИ от НСД «Застава»). |
| | 10. | 4 | **Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа** (с использованием средств контроля защищенности типа «Ревизор 1», «Ревизор 2», «TERRIER», «ФИКС»). |
| | 11. | 4 | **Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа** (с использованием сканеров безопасности типа «Сканер-ВС», «Ревизор сети»). |

Примечание: подготовка к лабораторным работам проводится в часы, выделенные для самостоятельной работы слушателей.

**Перечень практических занятий**

*Не предусмотрены*

### 3.3.5. Учебно-методическое и информационное обеспечение дисциплины

#### Литература


1. Мельников, Д.А. Информационная безопасность открытых систем : учебник /Д.А. Мельников. - Москва: Флинта: Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 15.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7.
2. Программно-аппаратные средства защиты информации: учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1.
3. Программно-аппаратные средства защиты информации: учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 .
4. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8 .


#### Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы


1. Федеральный закон от 7 июля 2003 г. « 126-ФЗ «О связи» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/186117/paragraph/430816:0 (дата обращения 12.03.2022).
2. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями) ; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12184522/paragraph/455:0 (дата обращения 12.03.2022).
3. Федеральный закон Российской Федерации от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12185475/paragraph/5637:0 (дата обращения 12.03.2022).
4. Постановление Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70136258/paragraph/1:0 (дата обращения 12.03.2022).
5. Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании

деятельности по разработке и производству средств защиты конфиденциальной информации); Текст: электронный// Гарант: [сайт]. – URL: https://base.garant.ru/70146250/ (дата обращения 12.03.2022).

6. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70391358/paragraph/1:0 (дата обращения 12.03.2022).

7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70690918/paragraph/1:0 (дата обращения 12.03.2022).

8. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70380924/paragraph/1:0 (дата обращения 12.03.2022).

9. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/401599204/paragraph/1/doclist/1959/showentries/0/highlight/приказ%20фстэк%2077%20от29.04.2021:2 (дата обращения 12.03.2022).

10. Приказ ФСТЭК России от 17 июля 2017 г. № 133 «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» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71743624/paragraph/1:0 (дата обращения 12.03.2022).

11. Приказ ФСТЭК России от 17 июля 2017 г. № 134 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями)**;** Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71689708/paragraph/1/doclist/1981/showentries/0/highlight/приказ%20министерства%20спорта%20рф%20от%2028%20февраля%202017%20г.%20n%20134:3 (дата обращения 12.03.2022).

12. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний: Национальный стандарт РФ: Введ. 13.04.2016: М.: Стандартинформ, 2015. – 35 с.*

13. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Национальный стандарт РФ: Введ. 01.01.1996: М.: Стандартинформ, 2006. – 6 с.

14. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 27.12.2006: М.: Стандартинформ, 2006. – 8 с.

15. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, 2007. – 7 с.

16. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: Национальный стандарт РФ: Введ. 28.01.2014.- М.: Стандартинформ, 2014. – 18 с.

17. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества: Национальный стандарт РФ: Введ. 28.12.2005.- М.: Стандартинформ, 2006. – 27 с.

18. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: Национальный стандарт РФ: Введ. 01.10.2009: М.: Стандартинформ, 2009. - 20 с.

19. ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства: Национальный стандарт РФ: Введ. 18.12.2009: М.: Стандартинформ, 2009. - 31 с.

20. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: Национальный стандарт РФ: Введ. 15.11.2012: М.: Стандартинформ, 2014. – 54 с.

21. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности: Национальный стандарт РФ: Введ. 08.01.2013: М.: Стандартинформ, 2014. – 161 с.

22. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности: Национальный стандарт РФ: Введ. 08.11.2013: М.: Стандартинформ, 2014. – 150 с.

23. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации: Национальный стандарт РФ: Введ. 06.04.2005. - М.: Стандартинформ, 2005. – 16 с.

24. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 29.12.2005.- М.: Стандартинформ, 2006. – 20 с.

25. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij- (дата обращения 12.03.2022).

26. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/component/content/article/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot (дата обращения 12.03.2022).

27. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g4 (дата обращения 12.03.2022).

28. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/component/content/article/114-tekhnicheskaya-zashchitainformatsii/dokumenty/spetsialnye-normativnye-dokumenty/385rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissiirossii-ot-30-marta-1992-g2 (дата обращения 12.03.2022).

29. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyuly (дата обращения 12.03.2022).

30. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.*

31. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения 12.03.2022).

32. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения 12.03.2022).

33. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114spetsialnye-normativnye-dokumenty/379bazovaya-model-ugroz-bezopasnosti-perso-nalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii2008god (дата обращения 12.03.2022).

34. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9.*

35. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638.*

36. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28.*

37. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 №119.*

38. Требования к средствам контроля машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.*

**Периодические издания**

1. Безопасность информационных технологий: научный журнал / ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ». - Москва: НИЯУ МИФИ, 1994 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8429 (дата обращения: 12.03.2022). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011-.- URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

3. Information Security/Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Текст: электронный.

4. Вопросы кибербезопасности: научный журнал. - Москва: НПО «Эшелон», 2013. – URL: http://cyberrus.com/ (дата обращения: 12.03.2022). – Текст: электронный.

5. Защита информации. Inside : информационно-методический журнал/ Издательский дом «Афина». - Санкт-Петербург: ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 12.03.2022). - Режим доступа: по подписке (2017-2022). - ISSN 2413-3582. - Текст : электронный

6. Jet Info/Инфосистемы Джет. – URL: http://www.jetinfo.ru (дата обращения: 12.03.2022). – Режим доступа: свободный.

7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 12.03.2022). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

**Перечень профессиональных баз данных, информационных справочных систем**

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 12.03.2022). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: https://e.lanbook.com (дата обращения: 12.03.2022). - Текст: электронный.
3. ФСТЭК России: сайт. М.: -.- URL: https://fstec.ru/ (дата обращения: 12.03.2022). – Текст: электронный.
4. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 12.03.2022). - Текст: электронный.
5. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 12.03.2022). - Текст: электронный.
6. Бюро научно-технической информации «Техника для спецслужб»: сайт. – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Текст : электронный.
7. ФСБ России: сайт. М.: -.- URL: http://fsb.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

### 3.3.6. Материально-техническое обеспечение дисциплины

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| Специализированная мультимедийная аудитория | Лекции, практические занятия | Мультимедийное оборудование: компьютер, подключенный к сети Интернет и доступом в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (звуковые колонки), вебкамера с микрофоном. |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| | | Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). Учебная доска. |
| Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью» | Лабораторные работы | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>2. Автоматизированное рабочее место студента (27 шт.) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>Средства защиты информации (27 компл.):<br>– СЗИ от НСД «DallasLock»;<br>– ПАК "Соболь»;<br>– СЗИ от НСД «Застава»;<br>– антивирус Kaspersky EnterpriseSpace Security Russian;<br>– антивирус Dr.Web Desktop Security Suite;<br>– средство создания модели разграничения доступа «Ревизор 1 XP»;<br>– программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»;<br>– программа фиксации и контроля исходного состояния программного комплекса "ФИКС»; |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| | | – программа поиска и гарантированного уничтожения информации на дисках «TERRIER»;<br>– сканер безопасности «Сканер-ВС»;<br>– сканер безопасности «Ревизор сети». |
| Помещение для самостоятельной работы слушателей (кл. 3226) | Самостоятельная работа слушателей | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>2. Автоматизированное рабочее место студента (27 шт) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). |

### 3.3.7. Система контроля и оценивания

Оценка качества освоения дисциплины включает текущую и промежуточную аттестацию слушателей.

Текущий контроль освоенных знаний осуществляется в виде оценок за контрольные мероприятия:

– отчеты по выполнению заданий по лабораторным работам;

– компьютерные тесты по разделам дисциплины.

Промежуточная аттестация по дисциплине осуществляется в виде зачета с оценкой.

Итоговая оценка за дисциплину выставляется по 5-ти балльной шкале на основе среднего балла за контрольные мероприятия. При выставлении итоговой оценки используется шкала, приведенная в таблице.

Таблица

**Критерии выставления итоговой оценки по дисциплине**

| Средний балл за контрольные мероприятия $N_{cp}$ | Оценка |
|---|---|

| | |
|---|---|
| $N_{ср} < 3$ | 2 |
| $3 \le N_{ср} < 3{,}5$ | 3 |
| $3{,}5 \le N_{ср} < 4{,}5$ | 4 |
| $N_{ср} \ge 4{,}5$ | 5 |

## 3.4. Рабочая программа учебной дисциплины «Организация защиты информации»

### 3.4.1. Цели и задачи дисциплины

**Цель дисциплины** – сформировать у слушателей профессиональные компетенции, позволяющие осуществлять деятельность по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

**Задачи дисциплины** – формирование знаний, умений и опыта деятельности в области организации защиты информации.

### 3.4.2. Требования к результатам освоения учебной дисциплины

**Планируемые результаты освоения программы:**

Дисциплина «Организация защиты информации» участвует в формировании компетенций:

ПК-3. «Способен проводить работы техническому обслуживанию средств защиты информации и защищенных технических средств обработки информации».

ПК-4. «Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах».

**В результате изучения дисциплины слушатель должен:**

**Знать**:

организацию защиты информации на объекте информатизации;

состав системы защиты информации (СЗИ) объекта информатизации (ОИ).

основные требования к СЗИ ОИ.

содержание аналитического обоснования необходимости создания СЗИ ОИ;

порядок создания СЗИ ОИ;

организационно-распорядительные документы по защите информации на ОИ;

организацию аттестации ОИ;

основы организации эксплуатации средств (систем) защиты информации;

порядок ввода и вывода средств защиты информации в эксплуатацию;

меры безопасности при эксплуатации средств защиты информации;

состав и содержание эксплуатационной документации на СЗИ.

организацию технического обслуживания СЗИ;

организацию ремонта средств защиты информации.

**Уметь:**

проводить предварительное специальное обследование ОИ;

разрабатывать модели угроз безопасности информации ОИ;
разрабатывать концепции информационной безопасности ОИ;
разрабатывать техническое задания на создание СЗИ ОИ;
разрабатывать технический паспорт на ОИ;
разрабатывать организационно- распорядительные документы по защите АС от НСД:
разрабатывать документы по приему, вводу в эксплуатацию и списанию СЗИ;
разрабатывать документы по техническому обслуживанию СЗИ;
проводить техническое обслуживание СЗИ.

**Иметь опыт практической деятельности:**

по разработке организационно-распорядительных документов по защите информации в автоматизированных системах;

проведения работ техническому обслуживанию средств защиты информации и защищенных технических средств обработки информации.

### 3.4.3. Учебно-тематический план дисциплины

| № | Наименование разделов и тем | Общая трудоёмкость (часы) | Контактная работа, час | | | | Самостоятельная работа, час |
|---|---|---|---|---|---|---|---|
| | | | Всего | Лекции | Лабораторные занятия | Практические занятия | |
| 1. | Создание и внедрение системы защиты информации на объекте информатизации | 58 | 42 | 10 | - | 32 | 16 |
| 2. | Эксплуатация средств защиты информации и защищенных технических средств обработки информации | 40 | 30 | 18 | - | 12 | 10 |
| | **Всего** | 98 | 72 | 28 | - | 44 | 26 |

### 3.4.4. Содержание дисциплины

**Перечень лекций**

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 2 | **Организация защиты информации на объекте информатизации.** Порядок организации защиты информации на объекте информатизации. Акт классификации автоматизированной системы (АС). Категорирование объекта информатизации (ОИ). Состав системы защиты информации (СЗИ) объекта информатизации (ОИ). Основные требования к СЗИ ОИ. |
| | 2. | 2 | **Аналитическое обоснование необходимости создания системы защиты информации объекта информатизации** Предпроектное специальное обследование ОИ. Разработка модели угроз безопасности информации. Обоснование состава СЗИ ОИ. |
| | 3. | 2 | **Порядок создания системы защиты информации объекта информатизации** Стадии и этапы создания СЗИ ОИ. Разработка концепции СЗИ ОИ. Техническое задание. Эскизный проект. Технический проект. Рабочая документация. Ввод в действие СЗИ ОИ. |
| | 4. | 2 | **Организационно-распорядительные документы по защите информации** Организационно-распорядительные документы по защите информации, регламентирующие защиту информации в ходе эксплуатации ОИ (план мероприятий по защите информации на ОИ, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации). |
| | 5. | 2 | **Организация аттестации объекта информатизации:** Порядок организации аттестации ОИ по требованиям безопасности информации. Подготовка к проведению аттестации ОИ. Программа и методика аттестационных испытаний ОИ. Порядок проведения аттестации ОИ. |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 2. | 6. | 2 | **Основы организации эксплуатации средств (систем) защиты информации**<br>Термины и определения в области эксплуатации средств (систем) защиты информации (СЗИ). Классификация СЗИ (технические, программные, программно-технические). Основные этапы эксплуатации СЗИ, их краткая характеристика. |
| | 7. | 2 | **Ввод и вывод средств защиты информации в эксплуатацию**<br>Порядок приема, выдачи и закрепления СЗИ. Порядок ввода СЗИ в эксплуатацию. Порядок вывода из эксплуатации СЗИ. Организация списания и утилизации СЗИ. |
| | 8. | 2 | **Меры безопасности при эксплуатации средств защиты информации**<br>Общие требования по обеспечению безопасности при эксплуатации СЗИ.<br>Меры безопасности при эксплуатации СЗИ.<br>Порядок допуска личного состава к самостоятельной работе со СЗИ.<br>Виды, порядок и сроки инструктажей личного состава по технике безопасности. |
| | 9. | 2 | **Основы технического обслуживания средств защиты информации**<br>Роль и место системы технического обслуживания и ремонта в системе эксплуатации СЗИ.<br>Состав и содержание эксплуатационной документации на СЗИ. |
| | 10. | 2 | **Организация технического обслуживания средств защиты информации**<br>Задачи и виды технического обслуживания СЗИ.<br>Характеристика видов технического обслуживания СЗИ.<br>Контроль и проверка состояния СЗИ.<br>Организация и проведение технического обслуживания СЗИ.<br>Организация обновления программного обеспечения СЗИ. |
| | 11. | 2 | **Основы метрологического обеспечения средств защиты информации**<br>Общие сведения о метрологии и метрологическом обеспечении.<br>Виды и методы измерений. Погрешности измерений. |

| № раздела и темы дисциплины | № лекции | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Виды средств измерений. Метрологические характеристики средств измерений. Классы точности средств измерений.<br>Виды и периодичность поверок средств измерений.<br>Организация поверок средств измерений.<br>Калибровка средств измерений. |
| | 12. | 2 | **Организация рекламационной работы и ремонта средств защиты информации**<br>Организация рекламационной работы.<br>Организация ремонта СЗИ и СКЭЗИ. |
| | 13. | 2 | **Техническое обслуживание технических средств защиты информации**<br>Техническое обслуживание систем пространственного и линейного электромагнитного зашумления.<br>Техническое обслуживание систем виброакустической защиты |
| | 14. | 2 | **Контроль, диагностирование и восстановление программного обеспечения**<br>Методы диагностирования программного обеспечения и СВТ. Средства диагностирования программного обеспечения и СВТ.<br>Средства восстановления программного обеспечения. Организация восстановления программного обеспечения при сбоях. |

**Практические занятия**

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 1. | 1. | 4 | **Практическое занятие (групповое упражнение). Разработка проекта перечня сведений конфиденциального характера.**<br>Порядок разработки перечня сведений конфиденциального характера.<br>Оценка потенциального ущерба разглашения сведений конфиденциального характера.<br>Категорирование сведений конфиденциального характера. |

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Классификация сведений конфиденциального характера. |
| | 2. | 4 | **Практическое занятие (групповое упражнение). Разработка «Модели угроз безопасности информации»**<br>Предварительное специальное обследование объекта информатизации.<br>Разработка «Модели угроз безопасности информации» |
| | 3. | 4 | **Практическое занятие (групповое упражнение). Разработка «Концепции информационной безопасности объекта информатизации»** |
| | 4. | 4 | **Практическое занятие (групповое упражнение). Разработка технического задания на создание системы защиты информации объекта информатизации**. |
| | 5. | 4 | **Практическое занятие (групповое упражнение). Разработка технического паспорта на объект информатизации** |
| | 6. | 4 | **Групповое упражнение. Разработка организационно-распорядительных документов по защите автоматизированной системы от НСД:**<br>Разработка акта классификации автоматизированной системы (АС).<br>Описание технологического процесса обработки информации в АС.<br>Разработка перечня защищаемых информационных ресурсов АС.<br>Разработка перечня объектов и субъектов доступа.<br>Описание реализованных правил разграничения доступа.<br>Разработка инструкции администратора категорированной АС по обеспечению безопасности информации.<br>Разработка инструкции пользователя категорированной АС по обеспечению информационной безопасности. |
| | 7. | 4 | **Практическое занятие (групповое упражнение). Разработка организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**<br>Классификация информационной системы персональных данных.<br>Разработка положения по обработке и защите персональных данных в организации. |
| | 8. | 4 | **Практическое занятие (групповое упражнение). Разработка организационно-распорядительных документов по защите АСУ ТП** |

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Классификация АСУ ТП.<br>Разработка перечня ОТСС и информационных ресурсов, подлежащих защите.<br>Разработка перечня лиц, допущенных до обработки информации ограниченного доступа.<br>Разработка приказа о назначении лица, ответственного за защиту информации.<br>Разработка инструкции администратору по безопасности АСУ ТП.<br>Разработка инструкции оператору АСУ ТП. |
| 2. | 9. | 4 | **Практическое занятие (групповое упражнение). Прием, ввод в эксплуатацию и списание средств защиты информации.**<br>Разработка документов по приему, выдаче и закреплении СЗИ**.**<br>Разработка документов по ввод СЗИ в эксплуатацию.<br>Разработка документов по выводу из эксплуатации и списании СЗИ.<br>Разработка инструкций по обеспечению безопасности при эксплуатации СЗИ. |
| | 10. | 4 | **Практическое занятие (групповое упражнение). Техническое обслуживания технических средств защиты информации.**<br>Разработка инструкций по проведению технического обслуживания систем пространственного и линейного электромагнитного зашумления.<br>Проведение технического обслуживания системы пространственного и линейного электромагнитного зашумления.<br>Разработка инструкций по проведению технического обслуживания систем виброакустической защиты.<br>Проведение технического обслуживания системы виброакустической защиты. |
| | 11. | 4 | **Практическое занятие (групповое упражнение). Техническое обслуживания программно-технических средств защиты информации.**<br>Разработка инструкций по обновлению программного обеспечения СЗИ.<br>Разработка инструкций по проведению диагностики программного обеспечения и СВТ.<br>Разработка инструкций по восстановлению программного обеспечения при сбоях. |

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | | | Разработка инструкций по устранению неисправностей СВТ. Проведение технического обслуживания программно-технического средства защиты информации. |

Примечание: подготовка к практическим занятиям проводится в часы, выделенные для самостоятельной работы слушателей.

**Лабораторные работы**

*Не предусмотрены*

**3.4.5. Учебно-методическое и информационное обеспечение дисциплины**

**Литература**


1. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 16.03.2021). - ISBN 978-5-9912-0233-6.
2. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .
3. Извозчикова, В.В. Эксплуатация и диагностирование технических и программных средств информационных систем : учебное пособие / В. В. Извозчикова. - Оренбург : ОГУ, 2017. - 137 с. . – URL: http://elib.osu.ru/handle/123456789/13754 (дата обращения: 16.03.2021). – ISBN 978-5-7410-1746-3.
4. Гвоздева, Т. В. Проектирование информационных систем. Стандартизация: учеб. пособие / Т. В. Гвоздева, Б. А. Баллод. - 2-е изд., стер. - Санкт-Петербург: Лань, 2021. - 252 с. - URL: https://e.lanbook.com/book/169810 (дата обращения: 15.03.2021). - ISBN 978-5-8114-7963-4.
5. Коваленко В.В. Проектирование информационных систем: учеб. пособие. - М. : Форум, 2012. - 320 с. - (Высшее образование). - ISBN 978-5-91134-549-5.
6. Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва : Флинта : Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 16.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7.
7. Программно-аппаратные средства защиты информации: учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ,

Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1.

8. Программно-аппаратные средства защиты информации: учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 .

9. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 16.03.2021). - ISBN 978-5-9912-0233-6.

10. Управление безопасностью критических информационных инфраструктур: учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8.

11. Хорев, А.А. Техническая защита информации: учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А. А. Хорев. - М. : НПЦ "Аналитика", 2008. - 436 с. - 3000 экз. - ISBN 978-59901488-1-9.

**Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы**

1. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/10102673/ - (дата обращения 12.03.2022).

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71730198/paragraph/1:0 - (дата обращения 12.03.2022).

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/12148555/- (дата обращения 12.03.2022).

4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12148567/paragraph/24880:0 - (дата обращения 12.03.2022).

5. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12136454/paragraph/12089:0- (дата обращения 12.03.2022).

6. Федеральный закон от 7 июля 2003 г. « 126-ФЗ «О связи» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/186117/paragraph/430816:0 (дата обращения 12.03.2022).

7. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями) ; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12184522/paragraph/455:0 (дата обращения 12.03.2022).

8. Федеральный закон Российской Федерации от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12185475/paragraph/5637:0 (дата обращения 12.03.2022).

9. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/10105548/paragraph/196115:0 (дата обращения 12.03.2022).

10. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71556224/paragraph/1:0 (дата обращения 12.03.2022).

11. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/188429/ (дата обращения 12.03.2022).

12. Постановление Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70136258/paragraph/1:0 (дата обращения 12.03.2022).

13. Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации); Текст: электронный// Гарант: [сайт]. – URL: https://base.garant.ru/70146250/ (дата обращения 12.03.2022).

14. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70391358/paragraph/1:0 (дата обращения 12.03.2022).

15. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70690918/paragraph/1:0 (дата обращения 12.03.2022).

16. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных

данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/70380924/paragraph/1:0 (дата обращения 12.03.2022).

17. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/401599204/paragraph/1/doclist/1959/showentries/0/highlight/приказ%20фстэк%2077%20от29.04.2021:2 (дата обращения 12.03.2022).

18. Приказ ФСТЭК России от 17 июля 2017 г. № 133 «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» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71743624/paragraph/1:0 (дата обращения 12.03.2022).

19. Приказ ФСТЭК России от 17 июля 2017 г. № 134 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации» (с изменениями и дополнениями)**;** Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71689708/paragraph/1/doclist/1981/showentries/0/highlight/приказ%20министерства%20спорта%20рф%20от%2028%20февраля%202017%20г.%20n%20134:3 (дата обращения 12.03.2022).

20. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний: Национальный стандарт РФ: Введ. 13.04.2016: М.: Стандартинформ, 2015. – 35 с.*

21. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Национальный стандарт РФ: Введ. 01.01.1996: М.: Стандартинформ, 2006. – 6 с.

22. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 27.12.2006: М.: Стандартинформ, 2006. – 8 с.

23. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, 2007. – 7 с.

24. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: Национальный стандарт РФ: Введ. 28.01.2014.- М.: Стандартинформ, 2014. – 18 с.

25. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества: Национальный стандарт РФ: Введ. 28.12.2005.- М.: Стандартинформ, 2006. – 27 с.

26. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: Национальный стандарт РФ:

Введ. 01.10.2009: М.: Стандартинформ, 2009. - 20 с.

27. ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства: Национальный стандарт РФ: Введ. 18.12.2009: М.: Стандартинформ, 2009. - 31 с.

28. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации: Национальный стандарт РФ: Введ. 06.04.2005. - М.: Стандартинформ, 2005. – 16 с.

29. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 29.12.2005.- М.: Стандартинформ, 2006. – 20 с.

30. СНиП 23-03-2003. Защита от шума. Введ. 30.06.2003. - М.: Госстрой России, 2004. – 34 с.

31. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij- (дата обращения 12.03.2022).

32. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/component/content/article/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot (дата обращения 12.03.2022).

33. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g4 (дата обращения 12.03.2022).

34. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/component/content/article/114-tekhnicheskaya-zashchitainformatsii/ dokumenty/spetsialnye-normativnye-dokumenty/385rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissiirossii-ot-30-marta-1992-g2 (дата обращения 12.03.2022).

35. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России

от 25 июля 1997 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyuly (дата обращения 12.03.2022).

36. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.*

37. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения 12.03.2022).

38. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения 12.03.2022).

39. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114spetsialnye-normativnye-dokumenty/379bazovaya-model-ugroz-bezopasnosti-perso-nalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii2008god (дата обращения 12.03.2022).

40. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9.*

41. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638.*

42. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28.*

43. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 №119.*

44. Требования к средствам контроля машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.*

**Периодические издания**

1. Безопасность информационных технологий: научный журнал / ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ». - Москва: НИЯУ МИФИ, 1994 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8429 (дата обращения:

12.03.2022). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011-.- URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

3. Information Security/Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Текст: электронный.

4. Вопросы кибербезопасности: научный журнал. - Москва: НПО «Эшелон», 2013. – URL: http://cyberrus.com/ (дата обращения: 12.03.2022). – Текст: электронный.

5. Защита информации. Inside : информационно-методический журнал/ Издательский дом «Афина». - Санкт-Петербург: ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 12.03.2022). - Режим доступа: по подписке (2017-2022). - ISSN 2413-3582. - Текст : электронный

6. Jet Info/Инфосистемы Джет. – URL: http://www.jetinfo.ru (дата обращения: 12.03.2022). – Режим доступа: свободный.

7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 12.03.2022). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

**Перечень профессиональных баз данных, информационных справочных систем**

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 12.03.2022). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: https://e.lanbook.com (дата обращения: 12.03.2022). - Текст: электронный.

3. ФСТЭК России: сайт. М.: -.- URL: https://fstec.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

4. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 12.03.2022). - Текст: электронный.

5. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 12.03.2022). - Текст: электронный.

6. Бюро научно-технической информации «Техника для спецслужб»: сайт. – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Текст : электронный.

7. ФСБ России: сайт. М.: -.- URL: http://fsb.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

8. ТК-26: сайт. М.: -.- URL: https://tc26.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

### 3.4.6. Материально-техническое обеспечение дисциплины

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| Специализированная мультимедийная аудитория | Лекции, практические занятия | Мультимедийное оборудование: компьютер, подключенный к сети Интернет и доступом в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (звуковые колонки), вебкамера с микрофоном.<br>Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>Учебная доска. |
| Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью» | Практические занятия (групповые упражнения) | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС.<br>Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>2. Автоматизированное рабочее место студента (27 шт.) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС.<br>Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>Средства защиты информации (27 компл.):<br>– СЗИ от НСД «DallasLock»;<br>– ПАК "Соболь»;<br>– СЗИ от НСД «Застава»;<br>– антивирус Kaspersky EnterpriseSpace Security Russian;<br>– антивирус Dr.Web Desktop Security Suite; |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| | | – средство создания модели разграничения доступа «Ревизор 1 XP»;<br>– программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»;<br>– программа фиксации и контроля исходного состояния программного комплекса "ФИКС»;<br>– программа поиска и гарантированного уничтожения информации на дисках «TERRIER»;<br>– сканер безопасности «Сканер-ВС»;<br>– сканер безопасности «Ревизор сети». |
| Помещение для самостоятельной работы слушателей (кл. 3226) | Самостоятельная работа слушателей | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>2. Автоматизированное рабочее место студента (27 шт) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). |

### 3.4.7. Система контроля и оценивания

Оценка качества освоения дисциплины включает текущую и промежуточную аттестацию слушателей.

Текущий контроль освоенных знаний осуществляется в виде оценок за контрольные мероприятия:

– отчеты по выполнению заданий на практических занятиях;

– компьютерные тесты по разделам дисциплины.

Промежуточная аттестация по дисциплине осуществляется в виде зачета с оценкой.

Итоговая оценка за дисциплину выставляется по 5-ти балльной шкале на основе среднего балла за контрольные мероприятия. При выставлении итоговой оценки используется шкала, приведенная в таблице.

Таблица

**Критерии выставления итоговой оценки по дисциплине**

| Средний балл за контрольные мероприятия $N_{ср}$ | Оценка |
|---|---|
| $N_{ср} < 3$ | 2 |
| $3 \le N_{ср} < 3{,}5$ | 3 |
| $3{,}5 \le N_{ср} < 4{,}5$ | 4 |
| $N_{ср} \ge 4{,}5$ | 5 |

## МОДУЛЬ 2 «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

### 3.5. Рабочая программа учебной дисциплины «Методы и средства криптографической защиты информации»

#### 3.5.1. Цели и задачи дисциплины

**Цель дисциплины** – сформировать у слушателей профессиональные компетенции, позволяющие осуществлять деятельность по криптографической защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

**Задачи дисциплины** – формирование знаний, умений и опыта деятельности в области криптографической защиты информации.

#### 3.5.2. Требования к результатам освоения учебной дисциплины

**Планируемые результаты освоения программы:**

Дисциплина «Методы и средства криптографической защиты информации» участвует в формировании компетенций:

ПК-2 «Способен проводить работы по установке и настройке средств криптографической защиты информации в автоматизированных системах».

ПК-4 «Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах».

**В результате изучения дисциплины слушатель должен:**

**Знать**:

основные термины и определения в области криптографии;

задачи защиты информации, решаемые криптографическими методами;

виды криптографических преобразований. Основные методы шифрования;

классификацию шифров;

поточные системы шифрования;

блочные системы шифрования;

криптосистемы с открытым ключом;

электронную подпись. Стандартные алгоритмы электронной подписи;

инфраструктуру открытых ключей (PKI);

криптографические протоколы аутентификации;

криптографические протоколы передачи данных;

протоколы распределения ключей;

классификацию средств криптографической защиты информации (СКЗИ);

структуру СКЗИ, требования к СКЗИ;

современные программные и программно-аппаратные СКЗИ;

СКЗИ сетевого взаимодействия;

законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минкомсвязи России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием криптографических средств;

национальные и международные стандарты в области криптографической защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

организацию лицензирования деятельности по разработке и использованию СКЗИ;

организацию сертификации СКЗИ;

организацию защиты информации с использованием СКЗИ;

состав организационно-распорядительных документов по защите информации с использованием СКЗИ;

организацию технического обслуживания СКЗИ.

**Уметь:**

устанавливать, настраивать и использовать СКЗИ;

разрабатывать организационно-распорядительные документы по защите информации с использованием СКЗИ.

**Иметь опыт практической деятельности:**

по разработке организационно-распорядительных документов по защите информации в АС с использованием СКЗИ.

по установке, настройке и использованию СКЗИ.

### 3.5.3. Учебно-тематический план дисциплины

| № | Наименование разделов и тем | Общая трудоёмкость (часы) | Контактная работа, час | | | | Самостоятельная работа, час |
|---|---|---|---|---|---|---|---|
| | | | Всего | Лекции | Лабораторные занятия | Практические занятия | |
| 1 | Основные понятия криптографии | 6 | 4 | 4 | - | - | 2 |
| 2 | Симметричные системы шифрования | 32 | 24 | 8 | 12 | 4 | 8 |
| 3 | Асимметричные системы шифрования | 32 | 24 | 12 | 8 | 4 | 8 |
| 4 | Криптографические протоколы | 12 | 10 | 6 | - | 4 | **2** |
| 5 | Средства криптографической защиты информации | 56 | 40 | 12 | 28 | - | 16 |
| 6 | Правовые и организационные основы криптографической защиты информации. | 42 | 30 | 10 | - | 20 | 12 |
| | Всего | **180** | **132** | **52** | **48** | **32** | **48** |

### 3.5.4. Содержание дисциплины

**Перечень лекций**

| Номер раздела дисциплины | Номер лекции | Объем занятий, часы | Краткое содержание |
|---|---|---|---|
| 1 | 1. | 4 | **Основные понятия криптографии**<br>Основные термины и определения в области криптографии.<br>Задачи защиты информации, решаемые криптографическими методами.<br>Виды криптографических преобразований. Основные методы шифрования.<br>Классификация средств криптографической защиты информации (СКЗИ) |
| 2 | 2. | 2 | **Классификация шифров:**<br>Классификация шифров по различным признакам. Формальные модели шифров. Математические модели открытого текста.<br>Шифры перестановки. Шифры замены. Шифры гаммирования. |
| | 3. | 2 | **Поточные системы шифрования:**<br>Регистры сдвига с обратной связью. Скремблеры. Методы рандомизации сообщений. Поточные шифрсистемы. |
| | 4. | 4 | **Блочные системы шифрования:**<br>Принципы построения блочных шифров.<br>Алгоритмы шифрования DES и AES.<br>Алгоритмы шифрования ГОСТ 28147-89, ГОСТ Р 34.12-2015. |
| 3 | 5. | 4 | **Криптосистемы с открытым ключем:**<br>Асимметричные системы шифрования.<br>Открытое распределение ключей. Схема Диффи-Хеллмана.<br>Криптосистема RSA. Криптоанализ шифра RSA.<br>Система шифрования El Gamal.<br>Система шифрования Эль Гамаля<br>Криптография на эллиптических кривых. |
| | 6. | 4 | **Электронная подпись:**<br>Механизм действия электронной подписи<br>Функции хэширования. Хэш-функции SHA-1, SHA-2, SHA-3 и ГОСТ Р 34.11-2012.<br>Стандартные алгоритмы электронной подписи: алгоритмы электронной подписи DSA, ECDSA, ГОСТ Р 34.10-2012. Основные виды электронной подписи, средства электронной подписи, сертификат ключа проверки электронной подписи. |
| | 7. | 4 | **Инфраструктура открытых ключей (PKI)**<br>Основные понятия, термины и определения в области PKI. |

| Номер раздела дисциплины | Номер лекции | Объем занятий, часы | Краткое содержание |
|---|---|---|---|
| | | | Управление сертификатами и ключами.<br>Архитектура, основные компоненты PKI, их функции и взаимодействие.<br>Основные стандарты в области PKI: стандарты серии X (X.509); стандарты криптографии с открытым ключом PKCS. |
| 4 | 8. | 2 | **Протоколы аутентификации.**<br>Понятие криптографического протокола.<br>Основные протоколы аутентификации. Сравнение протоколов аутентификации.<br>Безопасное сетевое взаимодействие. Аутентификационный сервис Kerberos.<br>Протокол удаленного безопасного входа SSH. |
| | 9. | 2 | **Протоколы передачи данных.**<br>Обмен защищёнными данными.<br>Безопасность сетевого трафика. Протоколы сетевого уровня.<br>Безопасность на транспортном уровне. Протоколы транспортного уровня. Протокол TLS/SSL.<br>Безопасность на прикладном уровне. Стандарт защиты электронной почты S/MIME. |
| | 10. | 2 | **Протоколы распределения ключей.**<br>Протоколы передачи ключей на симметричных криптосхемах (протокол Kerberos). Протоколы передачи ключей на асимметричных криптосхемах (протокол X.509). Протоколы обмена ключами (IKE). Протокол SESPAKE выработки общего ключа с аутентификацией на основе пароля. |
| 5 | 11. | 4 | **Средства криптографической защиты информации:**<br>Классификация средств криптографической защиты информации (СКЗИ).<br>Структура СКЗИ.<br>Требования к средствам криптографической защиты информации.<br>Программные СКЗИ. Особенности и примеры.<br>Аппаратные и аппаратно-программные СКЗИ. Особенности и примеры. Критерии выбора СКЗИ.<br>Основные принципы построения СКЗИ. Принципы построения аппаратных СКЗИ. Принципы построения программных и программно-аппаратных СКЗИ. |

| Номер раздела дисциплины | Номер лекции | Объем занятий, часы | Краткое содержание |
|---|---|---|---|
| | | | Основные подходы к обеспечению надежности СКЗИ. |
| | 12. | 4 | **Средства криптографической защиты информации на персональном компьютере:** Задачи обеспечения информационной безопасности с использованием СКЗИ на персональном компьютере. Криптографическая защита жестких дисков и съемных носителей. Создание секретных дисков. Встроенные в операционную систему средства шифрования. Шифрование архиваторов. СКЗИ свободного доступа. Программные средства шифрования. Программно-аппаратные средства шифрования. |
| | 13. | 4 | **Средства криптографической защиты информации сетевого взаимодействия:** Криптографические средства создания защищенных виртуальных сетей (VPN). Технология построения криптозащищенных туннелей. Криптографическая защита удаленного доступа к локальной сети. СКЗИ для передачи данных в локальных сетях. Распределение криптографических ключей. Протоколы управления ключами в Интернет. Согласование глобальных параметров криптозащищенного канала передачи данных. Сетевые протоколы криптографической защиты. Криптографические средства аутентификации. СКЗИ с механизмом цифровой подписи. |
| 6 | 14. | 2 | **Правовые основы криптографической защиты информации** Законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минкомсвязи России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств. Основные положения Инструкции, утвержденной приказом ФАПСИ от 13.06.2001 № 152, об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Требования по эксплуатации шифровальных (криптографических) средств защиты информации в соответствии с Положением ПКЗ- |

| Номер раздела дисциплины | Номер лекции | Объем занятий, часы | Краткое содержание |
|---|---|---|---|
| | | | 2005, утвержденным приказом ФСБ России от 09.02.2005 № 66 (с изменениями и дополнениями). |
| | 15. | 2 | **Правовые основы применения электронной подписи.**<br>Правовые основы применения электронной подписи (ЭП). Понятие удостоверяющего центра (УЦ). Статус и функции УЦ.<br>Аккредитация УЦ. Уполномоченный орган в сфере электронной подписи в Российской Федерации.<br>Требования приказов ФСБ России от 27.12.2011 № 795 и № 796 соответственно к форме квалифицированного сертификата ключа проверки ЭП, к средствам ЭП и к средствам УЦ. |
| | 16. | 2 | **Система стандартизации в области криптографической защиты информации**<br>Система стандартизации в области криптографической защиты информации. Деятельность Технического комитета по стандартизации «Криптографическая защита информации» ТК 26.<br>Национальные и международные стандарты в области криптографической защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну. |
| | 17. | 2 | **Государственное регулирование в области криптографической защиты информации.**<br>Лицензирование деятельности по разработке и использованию СКЗИ.<br>Сертификация СКЗИ.<br>Государственный контроль и надзор в области криптографической защиты информации.<br>Таможенные ограничения на ввоз и вывоз СКЗИ. |
| | 18. | 2 | **Организация защиты информации с использованием средств криптографической защиты.**<br>Организационно-распорядительные документы по защите информации с использованием СКЗИ.<br>Организация работы с ключевой информацией.<br>Организация технического обслуживания СКЗИ.<br>Нештатные ситуации при эксплуатации СКЗИ. |

**Перечень лабораторных работ**

| № раздела дисциплины | № лабораторной работы | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 2 | 1. | 4 | Исследование симметричных криптографических алгоритмов замены. |
| | 2. | 4 | Исследование симметричных криптографических алгоритмов перестановки. |
| | 3. | 4 | Исследование криптографических стандартов симметричного шифрования ГОСТ28147-89, DES, 3DES и AES |
| 3 | 4. | 4 | Анализ асимметричных криптографических алгоритмов. Применение факторизации целых чисел для анализа RSA |
| | 5. | 4 | Практическое применение механизма электронной цифровой подписи по ГОСТ Р 34.10-2012 |
| 5 | 6. | 4 | Настройка и применение средств криптографической средств защиты информации, встроенных в операционную систему Microsoft Windows |
| | 7. | 4 | Установка, настройка и применение средств криптографической защиты информации на жестких дисках и съемных носителях (на примере программного средства TrueCrypt) |
| | 8. | 4 | Установка, настройка и применение средств криптографической защиты (на примере программного средства PGP) |
| | 9. | 4 | Установка, настройка и применение средств криптографической защиты (на примере программного средства Crypton Disk) |
| | 10. | 4 | Установка, настройка и применение средств криптографической защиты (на примере программного средства Crypton IPMobile) |
| | 11. | 4 | Установка, настройка и применение средств криптографической защиты (на примере программного средства Crypton ArcMail) |
| | 12. | 4 | Настройка защищенных виртуальных сетей (VPN). |

Примечание: подготовка к лабораторным работам проводится в часы, выделенные для самостоятельной работы слушателей.

**Перечень практических занятий**

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| 2 | 1. | 4 | **Практическое занятие (семинар). Симметричные шифры**<br>Классификация шифров.<br>Поточные системы шифрования.<br>Блочные системы шифрования. |
| 3 | 2. | 4 | **Практическое занятие (семинар). Ассиметричные шифры**<br>Криптосистемы с открытыми ключами.<br>Электронная подпись. |
| 4 | 3. | 4 | **Практическое занятие (семинар). Криптографические протоколы**<br>Протоколы аутентификации.<br>Протоколы передачи данных.<br>Протоколы распределения ключей. |
| 6 | 4. | 4 | **Практическое занятие (семинар). Правовые основы криптографической защиты информации**<br>Законодательство Российской Федерации, нормативные правовые акты и нормативные методические документы ФСБ России, Минкомсвязи России по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну с использованием криптографических средств.<br>Правовые основы применения электронной подписи. |
| | 5. | 4 | **Практическое занятие (семинар). Национальные и международные стандарты в области криптографической защиты информации.**<br>Национальные стандарты в области криптографической защиты информации.<br>Международные стандарты в области криптографической защиты информации. |

| № модуля дисциплины | № практического занятия | Объем занятий (часы) | Краткое содержание |
|---|---|---|---|
| | 6. | 4 | **Практическое занятие (семинар). Лицензирование деятельности по разработке и использованию СКЗИ.**<br>Виды шифровальных (криптографических) средств (средств криптографической защиты информации).<br>Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность.<br>Лицензионные требования при осуществлении лицензируемой деятельности.<br>Порядок получения лицензии по разработке и использованию СКЗИ.. |
| | 7. | 4 | **Практическое занятие (семинар). Организация защиты информации с использованием средств криптографической защиты.**<br>Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.<br>Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей.<br>Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.<br>Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации. |
| | 8. | 4 | **Практическое занятие (групповое упражнение). Разработка организационно-распорядительных документов по защите информации с использованием СКЗИ.** |

Примечание: подготовка к практическим занятиям проводится в часы, выделенные для самостоятельной работы слушателей.

### 3.5.5. Учебно-методическое и информационное обеспечение дисциплины

**Литература**


1. Бутакова Н.Г. Криптографические методы и средства защиты информации : Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ «Интермедия», 2019. - 384 с. - ISBN ISBN 978-5-4383-0135-6.
2. Запечников, С. В. Криптографические методы защиты информации : учеб. пособие для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М. : Издательство Юрайт, 2018. — 309 с. — ISBN 978-5-534-02574-3.
3. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. —ISBN 978-5-534-12474-3.
4. Пролубников, А. В. Криптографические средства защиты информации в сетях: учебно-методическое пособие / А. В. Пролубников. – 2-е изд., испр. – Омск : Изд-во Ом. гос. ун-та, 2015. – 190 с. - ISBN 978-5-7779-1899-4.
5. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. 2-е издание, стереотип. – М.: «Горячая линия – Телеком», 2014. – 229 с. - ISBN 978-5-9912-0286-2.
6. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — ISBN 978-5-9916-7088-3.
7. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — ISBN 978-5-9916-7090-6.


**Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы**


1. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/10102673/ - (дата обращения 12.03.2022).
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71730198/paragraph/1:0 - (дата обращения 12.03.2022).

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/12148555/- (дата обращения 12.03.2022).

4. Федеральный закон от 7 июля 2003 г. « 126-ФЗ «О связи» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/186117/paragraph/430816:0 (дата обращения 12.03.2022).

5. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями) ; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12184522/paragraph/455:0 (дата обращения 12.03.2022).

6. Федеральный закон Российской Федерации от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12185475/paragraph/5637:0 (дата обращения 12.03.2022).

7. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/10105548/paragraph/196115:0 (дата обращения 12.03.2022).

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»; Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/71556224/paragraph/1:0 (дата обращения 12.03.2022).

9. Указ Президента РФ от 3 апреля 1995 г. N 334 "О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации" (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/10104146/paragraph/8861:0 (дата обращения 13.03.2022).

10. Постановление Правительства РФ от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/102670/paragraph/9532:0 (дата обращения 13.03.2022).

11. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/188429/ (дата обращения 12.03.2022).

12. Постановление Правительства РФ от 21.11.2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12192119/paragraph/1:0 (дата обращения 13.03.2022).

13. Постановление Правительства РФ от 21.11.2011 г. № 957 «Об организации лицензирования отдельных видов деятельности» (с изменениями и дополнениями); Текст:

электронный //Гарант: [сайт]. – URL: http://ivo.garant.ru/#/document/12192119/paragraph/1:0 (дата обращения 13.03.2022).

14. Постановление Правительства РФ от 9 февраля 2012 г. № 111 "Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи" (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/70138262/ (дата обращения 13.03.2022).

15. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических)средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/70164728/ (дата обращения 13.03.2022).

16. Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»; Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/183628/ (дата обращения 13.03.2022).

17. Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/187947/ (дата обращения 13.03.2022).

18. Приказ ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи" (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/70133464/ (дата обращения 13.03.2022).

19. Приказ ФСБ РФ от 27 декабря 2011 г. N 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра" (с изменениями и дополнениями); Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/70139150/ (дата обращения 13.03.2022).

20. Приказ ФСБ России от 29 декабря 2020 г. N 641 "Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по лицензированию

деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"; Текст: электронный //Гарант: [сайт]. – URL: https://base.garant.ru/400235569/#block_2 (дата обращения 13.03.2022).

21. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Национальный стандарт РФ: Введ. 01.01.1996: М.: Стандартинформ, 2006. – 6 с.

22. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: Национальный стандарт РФ: Введ. 27.12.2006: М.: Стандартинформ, 2006. – 8 с.

23. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: Национальный стандарт РФ: Введ. 28.01.2014.- М.: Стандартинформ, 2014. – 18 с.

24. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: Национальный стандарт РФ: Введ. 15.11.2012: М.: Стандартинформ, 2014. – 54 с.

25. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности: Национальный стандарт РФ: Введ. 08.01.2013: М.: Стандартинформ, 2014. – 161 с.

26. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности: Национальный стандарт РФ: Введ. 08.11.2013: М.: Стандартинформ, 2014. – 150 с.

27. ГОСТ Р ИСО/МЭК 27001-2006. Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования: Национальный стандарт РФ: Введ. 27.12.2006.- М.: Стандартинформ, 2008. – 31 с.

28. ГОСТ Р ИСО/МЭК 27002-2012. Информационные технологии. Практические правила управления информационной безопасностью: Национальный стандарт РФ: Введ. 24.09.2012.- М.: Стандартинформ, 2014. – 104 с.

29. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи: Национальный стандарт РФ: Введ. 07.08.2012.- М.: Стандартинформ, 2013. – 22 с.

30. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита

информации. Функция хэширования: Национальный стандарт РФ: Введ. 07.08.2012.- М.: Стандартинформ, 2013. – 24 с.

31. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры: Национальный стандарт РФ: Введ. 19.06.2015.- М.: Стандартинформ, 2016. – 15 с.

32. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров: Национальный стандарт РФ: Введ. 19.06.2015.- М.: Стандартинформ, 2016. – 42 с.

33. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации: Национальный стандарт РФ: Введ. 06.04.2005. - М.: Стандартинформ, 2005. – 16 с.

34. Рекомендации по стандартизации Росстандарта Р 50.1.115-2016. «Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля: Введ. 28.11.2016.- М.: Стандартинформ, 2016. – 28 с.

35. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij- (дата обращения 12.03.2022).

36. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/component/content/article/114-tekhnicheskaya-zashchitainformatsii/ dokumenty/spetsialnye-normativnye-dokumenty/385rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissiirossii-ot-30-marta-1992-g2 (дата обращения 12.03.2022).

37. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.; Текст: электронный //ФСТЭК: [сайт]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyuly (дата обращения 12.03.2022).

38. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9.*

39. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638.*

40. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28.*

41. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 №119.*

42. Требования к средствам контроля машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.*

**Периодические издания**

1. Безопасность информационных технологий: научный журнал / ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ». - Москва: НИЯУ МИФИ, 1994 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8429 (дата обращения: 12.03.2022). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011-.- URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

3. Information Security/Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Текст: электронный.

4. Вопросы кибербезопасности: научный журнал. - Москва: НПО «Эшелон», 2013. – URL: http://cyberrus.com/ (дата обращения: 12.03.2022). – Текст: электронный.

5. Защита информации. Inside : информационно-методический журнал/ Издательский дом «Афина». - Санкт-Петербург: ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 12.03.2022). - Режим доступа: по подписке (2017-2022). - ISSN 2413-3582. - Текст : электронный

6. Jet Info/Инфосистемы Джет. – URL: http://www.jetinfo.ru (дата обращения: 12.03.2022). – Режим доступа: свободный.

7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 12.03.2022). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

**Перечень профессиональных баз данных, информационных справочных систем**

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 12.03.2022). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: https://e.lanbook.com (дата обращения: 12.03.2022). - Текст: электронный.

3. ФСТЭК России: сайт. М.: -.- URL: https://fstec.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

4. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 12.03.2022). - Текст: электронный.

5. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 12.03.2022). - Текст: электронный.

6. Бюро научно-технической информации «Техника для спецслужб»: сайт. – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Текст : электронный.

7. ФСБ России: сайт. М.: -.- URL: http://fsb.ru/ (дата обращения: 12.03.2022). – Текст: электронный.

### 3.5.6. Материально-техническое обеспечение дисциплины

| **Наименование специализированных аудиторий, кабинетов, лабораторий** | **Вид занятия** | **Наименование оборудования, программного обеспечения** |
|---|---|---|
| Специализированная мультимедийная аудитория | Лекции, практические занятия (семинары) | Мультимедийное оборудование: компьютер, подключенный к сети Интернет и доступом в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (звуковые колонки), вебкамера с микрофоном.<br>Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>Учебная доска. |
| Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью» | Практические занятия (групповые упражнения), лабораторные работы | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС.<br>Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>2. Автоматизированное рабочее место студента (27 шт.) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС.<br>Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>Средства защиты информации от НСД (27 компл.):<br>– СЗИ от НСД «DallasLock»;<br>– ПАК "Соболь»;<br>– СЗИ от НСД «Застава»; |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| | | – антивирус Kaspersky EnterpriseSpace Security Russian;<br>– антивирус Dr.Web Desktop Security Suite;<br>– средство создания модели разграничения доступа «Ревизор 1 XP»;<br>– программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»;<br>– программа фиксации и контроля исходного состояния программного комплекса "ФИКС»;<br>– программа поиска и гарантированного уничтожения информации на дисках «TERRIER»;<br>– сканер безопасности «Сканер-ВС»;<br>– сканер безопасности «Ревизор сети».<br>Средства криптографической защиты информации (27 шт):<br>– СКЗИ VipNet Custom;<br>– СКЗИ «КриптоПро CSP»;<br>– СКЗИ TrueCry;,<br>– СКЗИ Crypton Disk;<br>– СКЗИ Crypton IPMobile;<br>– СКЗИ Crypton ArcMail. |
| Помещение для самостоятельной работы слушателей (кл. 3226) | Самостоятельная работа слушателей | 1. Автоматизированное рабочее место преподавателя на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс).<br>2. Автоматизированное рабочее место студента (27 шт) на базе ПЭВМ, с подключением к сети Интернет и обеспечением доступа в ОРИОКС. |

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| | | Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Яндекс). |

### 3.5.7. Система контроля и оценивания

Оценка качества освоения дисциплины включает текущую и промежуточную аттестацию слушателей.

Текущий контроль освоенных знаний осуществляется в виде оценок за:

- отчетные документы по групповым упражнениям и лабораторным работам;
- компьютерные тесты.

Промежуточная аттестация по дисциплине осуществляется в виде зачета с оценкой.

Итоговая оценка за дисциплину выставляется по 5-ти балльной шкале на основе среднего балла за контрольные мероприятия. При выставлении итоговой оценки используется шкала, приведенная в таблице.

Таблица

**Критерии выставления итоговой оценки по дисциплине**

| Средний балл за контрольные мероприятия $N_{ср}$ | Оценка |
|---|---|
| $N_{ср} < 3$ | 2 |
| $3 \le N_{ср} < 3{,}5$ | 3 |
| $3{,}5 \le N_{ср} < 4{,}5$ | 4 |
| $N_{ср} \ge 4{,}5$ | 5 |

## 4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Описание учебно-методического и материально-технического обеспечения программы переподготовки приведено в рабочих программах учебных модулей.

## 5. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы включает промежуточную и итоговую аттестацию слушателей.

Промежуточная аттестация слушателей проводится по каждой дисциплине в виде зачета с оценкой.

Итоговая оценка за дисциплину выставляется по 5-ти балльной шкале на основе среднего балла за контрольные мероприятия (отчеты по выполнению заданий по лабораторным работам, практическим занятиям, доклады на семинарах, компьютерные тесты по разделам дисциплины и т.д.), выполняемые в слушателями в ходе изучения дисциплины.

Итоговая аттестация включает междисциплинарный экзамен.

Междисциплинарный экзамен проводится в два этапа: теоретический и практический.

**Теоретический этап** проводится с целью оценки уровня знаний, необходимых для формирования профессиональных компетенций в виде компьютерного тестирования.

Максимальное время выполнения компьютерного теста: 60 мин.

Материально-технические ресурсы для обеспечения теоретического этапа профессионального экзамена:

помещение, площадью не менее 20 кв.м., оборудованное персональными компьютерами из расчета 1 компьютер на 1 слушателя с характеристиками не хуже: системный блок: процессор – Intel Core i5, количество ядер процессора 4, тактовая частота ядра – 3,4 ГГц, видеокарта – встроенная, графический процессор видеокарты – Intel, оперативная память – 8 ГГц, тип оперативной памяти - DDR4, объем жесткого диска SSD – 256 ГГб, интерфейсы – вход VGA, DisplayPort, HDMI, USB 3.0, сетевые интерфейсы - предустановленный модуль Wi-Fi (стандарт Wi-Fi 802.11 a/ac/b/g/n/ax), проводная сеть (LAN) - 10/100/1000 мбит/сек.;операционная система Microsoft Windows 10 Pro x64 Rus 1pk DSP OEI DVD; монитор 23,8" ( IPS; 16:9; 250 cd/m2; 1000:1; 5ms; 1920x1080; 178/178; 2xHDMI; Tilt; Spk 2x5W, без мерцания; комплект (клавиатура+мышь; Microsoft Office 2013, Adobe Acrobat reader), подключенными к сети Интернет, письменными столами, стульями.

Компьютерный тест формируется из случайно подбираемых вопросов (заданий) из тестов по разделам дисциплин. Вариант теста содержит 50 вопросов (заданий), по 10 заданий (вопросов) по каждой дисциплине.

Примеры вопросов (заданий) для теоретического этапа профессионального экзамена:

Вопрос (задание № 1) по знанию требований нормативных правовых актов, методических документов, национальных стандартов в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации.

Выберите правильные варианты ответа на вопрос:

В соответствие с «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.» обработка информации, составляющей государственную тайну, разрешена для АС класса защищенности:

А) 3А, 2А.

Б) 3Б, 2Б.

В) 1А, 1Б, 1В.

Г) 1 Г, 1Д.

Д) 3А, 2А, 1А.

Вопрос (задание № 6) по знанию технических каналов утечки информации, возникающих при обработке информации СВТ.

Выберите правильный вариант ответа на вопрос:

Укажите (определите) правильное соотношение:

А) $R2 \geq r1$.

Б) $R2 = r1$.

В) $R2 > r1$.

Г) $R2 \leq r1$.

Д) $R2 < r1$.

За правильный ответ начисляется 1 балл, за неправильный ответ – 0 баллов. Баллы, полученные за ответы на вопросы, суммируются. Максимальное количество баллов – 50.

Оценка за теоретический этап выставляется по 5-ти балльной шкале. При выставлении оценки используется шкала, приведенная в таблице 5.1.

Таблица 5.1

**Критерии выставления оценки за теоретический этап**

| Количество (%) правильных ответов | Оценка |
|---|---|
| $N < 25$ (50%) | 2 |
| 25 (50%) $\leq N <$ 35 (70%) | 3 |
| 35 (70%) $\leq N <$ 45 (90%) | 4 |
| $N \geq 45$ (90%) | 5 |

Если слушатель по теоретическому этапу получил оценку 2, он до практического этапа не допускается, и ему за экзамен выставляется оценка 2.

**Практический этап экзамена** проводится с целью оценки уровня умений, необходимых для формирования профессиональных компетенций, и включает два практико-ориентированных задания. Первое задание – по модулю 1, и второе задание – по модулю 2.

Задания формируются на основе заданий на выполнение лабораторных работ и практических занятий (групповых упражнений) по дисциплинам модулей.

Максимальное время выполнения каждого задания: 120 мин.

Материально-технические ресурсы для обеспечения практического этапа профессионального экзамена: помещение, площадью не менее 20 кв.м., оборудованное:

– письменными столами, стульями;

– автоматизированными системами (АС) на базе персональных компьютеров, с характеристиками не хуже: системный блок: процессор – Intel Core i5, количество ядер процессора 4, тактовая частота ядра – 3,4 ГГц, видеокарта – встроенная, графический процессор видеокарты – Intel, оперативная память – 8 ГГц, тип оперативной памяти - DDR4, объем жесткого диска SSD – 256 ГГб, интерфейсы – вход VGA, DisplayPort, HDMI, USB 3.0, сетевые интерфейсы - предустановленный модуль Wi-Fi (стандарт Wi-Fi 802.11 a/ac/b/g/n/ax), проводная сеть (LAN) - 10/100/1000 мбит/сек.;операционная система Microsoft Windows 10 Pro

x64 Rus 1pk DSP OEI DVD; монитор 23,8" ( IPS; 16:9; 250 cd/m2; 1000:1; 5ms; 1920x1080; 178/178; 2xHDMI; Tilt; Spk 2x5W, без мерцания; комплект (клавиатура+мышь; Microsoft Office 2013, Adobe Acrobat reader), подключенными к сети Интернет;

– программно-аппаратными комплексами защиты АС от несанкционированного доступа к информации (типа Secret Net Studio);

– средствами криптографической защиты информации (типа TrueCryp, Crypton Disk, Crypton IPMobile, Crypton ArcMail и др.);

– системами активной защиты от утечки информации по каналам побочных электромагнитных излучений и наводок (типа ЛГШ-503, Салют-3000Б, Соната-РС3 и др.);

– измерительным комплексом в составе анализатора спектра (типа FSL-3) и измерительной электрической антенны (типа НБА-02);

– средствами контроля защищенности информации (типа Ревизор 1 XP, Ревизор 2 XP, TERRIER (версия 3.0), ФИКС (версия 2.0.2), Ревизор Сети (версия 3.0) и др.).

Пример задания для практического этапа профессионального экзамена:

Задание № 1 по модулю 1. Установить защищенное техническое средство обработки информации в соответствие с инструкцией по эксплуатации. Настроить программно-аппаратный комплекс защиты от несанкционированного доступа к информации в соответствие с классом защищенности 1Г:

- Установить системный блок ПЭВМ и подключить его к линии электропитания. Установить монитор, подключить его к системному блоку и линии электропитания. Подключить к системному блоку клавиатуру и мышь.
- Установить систему активной защиты ПЭВМ от утечки информации по каналам побочных электромагнитных излучений и наводок, подключить ее к линии электропитания.
- Установить на ПЭВМ программно-аппаратный комплекс защиты от несанкционированного доступа к информации.
- Настроить программно-аппаратный комплекс защиты от несанкционированного доступа к информации в соответствие с классом защищенности 1Г.
- Настроить правила дискреционного доступа с соответствие с матрицей доступа.

Оценка за выполнение практического задания проводится по 5-ти балльной шкале. При выставлении оценки используется следующие критерии:

- Место установки ПЭВМ выбрано с учетом исключения наблюдения экрана монитора посторонними лицами. Подключение монитора, клавиатуры и мыши к системному блоку проведено в соответствие с инструкцией по эксплуатации ЗТСОИ. Подключение системного блока и монитора к электросети проведено с соблюдением правил электробезопасности.
- Место установки генератора шума системы активной защиты ПЭВМ (САЗ) от утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) выбрано в соответствие с инструкцией по эксплуатации САЗ. Антенны развернуты и подключены к генератору шума в соответствие с инструкцией по эксплуатации САЗ.

Подключение генератора шума к электросети проведено с соблюдением правил электробезопасности.

- Программно-аппаратный комплекс защиты от несанкционированного доступа к информации установлен на ПЭВМ в соответствие с инструкцией по эксплуатации (руководства администратора).
- программно-аппаратный комплекс защиты от несанкционированного доступа к информации (ПАК ЗИНСД) настроен в соответствие с инструкцией по эксплуатации (руководства администратора).
- При настройке ПАК ЗИНСД применен шаблон класса защищенности 1В.
- При настройке системы идентификации и проверки подлинности субъектов доступа при входе в систему каждому пользователю установлен идентификатор и пароль временного действия длиной не менее шести символов.
- Настройка правил дискреционного доступа проведена в соответствии матрицей доступа и метками конфиденциальности.
- Проведена проверка возможности печати конфиденциальной информации пользователями в соответствии с метками конфиденциальности.

Оценка «5» за выполнение задания выставляется, если выполнены все критерии.

Оценка «4» за выполнение задания выставляется, если выполнены все критерии, но имеются отдельные неточности, не влияющие на состояние защищенности ПЭВМ.

Оценка «3» за выполнение задания выставляется, если не выполнены отдельные критерии, или имеются нарушения инструкций по эксплуатации, не влияющие на состояние защищенности ПЭВМ.

Оценка «2» за выполнение задания выставляется, если не выполнены отдельные критерии или имеются нарушения инструкций по эксплуатации, влияющие на состояние защищенности ПЭВМ.

Оценка за практический этап выставляется по 5-ти балльной шкале. При выставлении оценки используется шкала, приведенная в таблице 5.2.

Таблица 5.2

**Критерии выставления оценки за практический этап**

| Оценки за выполнение практических заданий | Оценка за практический этап |
|---|---|
| Оценка за выполнение каждого из заданий 5. | 5 |
| Оценка за выполнение каждого из заданий не ниже 4, но не выполняются критерии для выставления оценки 5. | 4 |
| Оценка за выполнение каждого из заданий не ниже 3, но не выполняются критерии для выставления оценки 4. | 3 |
| Оценка за выполнение одного из заданий 2. | 2 |

При выставлении оценки за экзамен используется шкала, приведенная в таблице 5.3.

Таблица 5.3

**Критерии выставления оценки за экзамен**

| Критерии оценки | Оценка |
|---|---|
| Оценка за теоретический этап не ниже 4.<br>Оценка за практический этап 5. | 5 |
| Оценка за теоретический этап не ниже 3.<br>Оценка за практический этап не ниже 4. | 4 |
| Оценка за теоретический этап не ниже 3.<br>Оценка за практический этап 3. | 3 |
| Оценка за теоретический этап не ниже 3.<br>Оценка за практический этап 2. | 2 |

**Разработчики программы:**

Заведующий кафедрой Информационная безопасность А.А. Хорев

Профессор кафедры Информационная безопасность А.В. Душкин

**Согласовано:**

Начальник АНОК И.М. Никулина

Заведующий кафедрой Информационная безопасность А.А. Хорев