

Министерство просвещения Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.01.02.0 «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»**

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль программы «Информационные технологии (по элективным модулям*)»

Автор(ы): ст. преп. В.В. Мешков
ст. преп. Т.В. Рыжкова

Одобрена на заседании кафедры информационных систем и технологий. Протокол от «20» января 2022 г. №5.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией института ИПО РГППУ. Протокол от «26» января 2022 г. №6.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Техническая защита информации»: формирование у студентов знаний по основам защиты информации. развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением аппаратной защиты информации.

Задачи:

- изучение основ построения подсистем защиты информации в информационно-коммуникационных системах различной архитектуры;
- освоение принципов функционирования современных систем идентификации и аутентификации;
- оценки защищенности и обеспечения информационной безопасности объектов информатизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Техническая защита информации» относится к части, формируемой участниками образовательных отношений, учебного плана.

Для изучения учебной дисциплины необходимы знания, умения и владения, формируемые следующими дисциплинами:

1. Архитектура ПК и периферийные устройства.
2. Прикладная математика и математическая логика.
3. Основы алгоритмизации и программирования.

Перечень учебных дисциплин, для которых необходимы знания, умения и владения, формируемые данной учебной дисциплиной:

1. Микропроцессорная техника.
2. Криптографические методы защиты информации.
3. Электроника.
4. Программные средства защиты информации.
5. Мехатроника.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- ПКС-2.1 Способен проводить работы по установке и техническому обслуживанию средств защиты информации;
- ПКС-2.2 Способен обеспечить бесперебойную работу средств связи сетей электросвязи (СССЭ), а также программных, программно-аппаратных (в



том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа (НСД).

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

31. Виды угроз и методы защиты информации;
32. Аппаратные и программные средства резервного копирования данных;
33. Методы обеспечения защиты информации от несанкционированного доступа;
34. Специализированные средства борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами;
35. Состав мероприятий по защите персональных данных.

Уметь:

- У1. Обеспечивать резервное копирование данных;
- У2. Осуществлять меры по защите информации от несанкционированного доступа;
- У3. Применять специализированные средства борьбы с вирусами, несанкционированными рассылками, вредоносными программами;
- У4. Осуществлять мероприятия по защите информации.

Владеть:

- В1. Навыками работы с профессиональными аппаратными средствами защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 час.), семестр изучения – 5, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоёмкости дисциплины по видам работ

Вид работы	Форма обучения
	очная
	Семестр изучения
	5 сем.
	Кол-во часов
Общая трудоёмкость дисциплины по учебному плану	108
Контактная работа, в том числе:	32
Лекции	8



Лабораторные работы	24
Самостоятельная работа студента	76
Промежуточная аттестация, в том числе:	
Экзамен	5 сем.

**Распределение трудоемкости по видам контактной работы для заочной формы обучения (при наличии) корректируется в соответствии с учебным планом заочной формы обучения.*

4.2 Содержание и тематическое планирование дисциплины

Таблица 2. Тематический план дисциплины

Наименование разделов и тем дисциплины (модуля)	Сем.	Всего, час.	Вид контактной работы, час.			СРС
			Лекции	Практ. занятия	Лаб. работы	
1. Концепция технической защиты информации	5	14	2	-	-	12
2. Утечка информации по техническим каналам	5	14	2	-	-	12
3. Основные принципы технической защиты информации	5	20	2	-	6	12
4. Организационные основы технической защиты информации	5	20	2	-	6	12
5. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов	5	18	-	-	4	14
6. Моделирование процессов технической защиты информации	5	22	-	-	8	14

**Распределение часов по разделам (темам) дисциплины для заочной формы обучения осуществляется научно-педагогическим работником, ведущим дисциплину.*

4.3 Содержание разделов (тем) дисциплин

Раздел 1. Концепция технической защиты информации

Системный подход к защите информации. Характеристика защиты информации. Основные параметры системы защиты информации. Основные концептуальные положения защиты информации. Принципы защиты информации техническими средствами. Основные направления защиты информации.



Раздел 2. Утечка информации по техническим каналам

Информации как предмет защиты. Виды, источники и носители защищаемой информации.

Демаскирующие признаки объектов наблюдения, сигналов и веществ. Источники опасных сигналов. Основные и вспомогательные технические средства и системы, их классификация и характеристика. Опасные сигналы, образующиеся в результате акустоэлектрических преобразований. Виды побочных опасных электромагнитных излучений. Паразитные связи и наводки опасных сигналов. Характеристика технической разведки. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки по добыванию разведывательной информации. Технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

Раздел 3. Основные принципы технической защиты информации

Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов.

Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов/

Раздел 4. Организационные основы технической защиты информации

Государственная система защиты информации. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.

Основные организационные и технические меры по защите информации. Контроль эффективности инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам Виды технического контроля.

Раздел 5. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов

Распространение сигналов в технических каналах утечки информации. Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи.

Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе. Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей.



Экранирование электрических, магнитных, и электромагнитных полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

Раздел 6. Моделирование процессов технической защиты информации

Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.

Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по оценке эффективности защиты информации.

Оценка эффективности защиты видовых признаков объектов наблюдения. Оценка дальности перехвата опасных сигналов.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для изучения дисциплины используются различные образовательные технологии:

1. Организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Традиционные образовательные технологии, которые ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

3. При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;

- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) университета, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС университета и других информационно-коммуникационных технологий (видеоконференцсвязь, облачные технологии и сервисы, др.);



- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1 Основная литература

1. Малюк А. А. Защита информации в информационном обществе / Малюк А. А. — Москва : Горячая линия-Телеком, 2017. — 230 с. — Режим доступа: <http://e.lanbook.com/book/111078>.

2. Никифоров С. Н. Защита информации. Защита от внешних вторжений : учебное пособие. - Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 84 с. - Режим доступа: <http://www.iprbookshop.ru/74381>.

3. Никифоров С. Н. Защита информации. Защищенные сети : учебное пособие. - Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 80 с. - Режим доступа: <http://www.iprbookshop.ru/74382>.

4. Булатов В. Н., Худорожков О. В. Микропроцессорная техника. Схемотехника и программирование : учебное пособие. - Оренбург : Оренбургский государственный университет, 2016. - 377 с. - Режим доступа: <http://www.iprbookshop.ru/61377>.

5. Сергеев А. И., Черноусова А. М., Русяев А. С. Программирование контроллеров систем автоматизации : учебное пособие. - Оренбург : Оренбургский государственный университет, 2016. - 126 с. - Режим доступа: <http://www.iprbookshop.ru/71315>.

6.2 Дополнительная литература

1. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т. Р. Методы и средства инженерно-технической защиты информации : учебное пособие. - Брянск : Брянский государственный технический университет, 2012. - 187 с. - Режим доступа: <http://www.iprbookshop.ru/7000>.

2. Щеглов А. Ю., Щеглов К. А. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие. - Санкт-Петербург : Университет ИТМО, 2015. - 93 с. - Режим доступа: <http://www.iprbookshop.ru/67260>.

3. Петров А. А. Компьютерная безопасность. Криптографические методы защиты : монография. - Саратов : Профобразование, 2017. - 446 с. - Режим доступа: <http://www.iprbookshop.ru/63800>.



6.3 Программное обеспечение и Интернет-ресурсы

Интернет-ресурсы:

1. ITSec.Ru - портал для профессионалов информационной безопасности.

Режим доступа: <http://www.itsec.ru/>

2. Научная электронная библиотека eLIBRARY. Режим доступа: <https://elibrary.ru/defaultx.asp>

3. Яндекс Практикум. Режим доступа: <https://praktikum.yandex.ru/>

Программное обеспечение:

1. FTP-клиент FileZilla.

2. Браузер Yandex Browser.

3. Операционная система Windows.

4. Программное обеспечение для информационной безопасности Snort.

Информационные системы и платформы:

1. Система дистанционного обучения «Moodle».

2. Информационная система «Таймлайн».

3. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Лаборатория мехатроники и автоматике - компьютерный класс.

2. Помещения для самостоятельной работы.

3. Учебная аудитория "Учебный центр радиоэлектронных и информационных технологий "Tesla"".

4. Компьютерный класс.

5. Учебная аудитория для проведения занятий лекционного типа.

