



МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

**ПМ.03 Защита информации в информационно-телекоммуникационных
системах и сетях с использованием технических средств защиты**

**Специальность 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем**

**Москва
2025**

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	7
3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ	12
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ	16

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

1.1. Цель и планируемые результаты освоения профессионального модуля

Результатом учебной практики профессионального модуля ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты является овладение обучающимися видом деятельности по направлению: Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК.01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК.02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК.03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК.04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК.05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учётом особенностей социального и культурного контекста.
ОК.06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учётом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК.07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК.08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК.09	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

ВД	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
ПК 3.1	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях
ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации

	используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	<ul style="list-style-type: none"> – установка, монтаж и настройка технических средств защиты информации; – техническое обслуживание технических средств защиты информации; – применение основных типов технических средств защиты информации; – выявление технических каналов утечки информации; – участие в мониторинге эффективности технических средств защиты информации; – диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; – проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; – проведение измерений параметров фоновых шумов, а также физических полей, – создаваемых техническими средствами защиты информации; – установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты
Уметь	<ul style="list-style-type: none"> – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации
Знать	<ul style="list-style-type: none"> – порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

	<ul style="list-style-type: none"> – физические основы формирования технических каналов утечки информации, – способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – структуру и условия формирования технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты информации; – номенклатуру применяемых средств физической защиты объектов информатизации <p>– особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;</p> <p>– основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;</p> <p>– основные понятия криптографии и типовые криптографические методы защиты информации.</p>
--	--

1.3. Количество недель (часов) на освоение программы учебной практики

Всего: 2 недели, 72 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

2.1. Тематический план

Коды формируемых компетенций	Наименование тем профессионального модуля учебной практики	Объем времени, отведенный на практику (часах)
ОК 01– ОК 09 ПК 3.1- ПК.3.4	Инструктаж по охране труда и технике безопасности. Знакомство с заданием учебной практики.	2 часа
	Раздел 1. Установка и настройка технических средств защиты информации.	
	Тема 1.1. Установка и настройка технических средств защиты информации. Монтаж различных типов датчиков.	6 часов
	Тема 1.2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	8 часов
	Тема 1.3. Измерение параметров физических полей. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.	8 часов
	Раздел 2. Рассмотрение системы контроля и управления доступом.	
	Тема 2.1. Рассмотрение системы контроля и управления доступом.	8 часов
	Тема 2.2. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.	8 часов
	Тема 2.3. Рассмотрение датчиков периметра, их принципов работы.	8 часов
	Тема 2.4. Выполнение звукоизоляции помещений системы шумления.	8 часов
	Раздел 3. Реализация защиты от утечки по цепям электропитания и заземления.	
	Тема 3.1. Разработка организационных и технических мероприятий по заданию преподавателя.	8 часа
	Тема 3.2. Разработка основной документации по инженерно-технической защите информации.	6 часов
	Тема 3.3. Отчетная документация за учебную практику	2 часа
	ИТОГО:	72 часа

2.2. Содержание практики

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов, с указанием тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	Изучение инструкций по охране труда и технике безопасности	Инструкции по охране труда и технике безопасности.	Инструктаж по охране труда и технике безопасности. Знакомство с заданием учебной практики	2 часа
	Теоретические основы инженерно-технической защиты информации	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты. МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты. Раздел 1. Установка и настройка технических средств защиты информации. Тема 1.1. Установка и настройка технических средств защиты информации. Монтаж различных типов датчиков.	6 часов

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов, с указанием тем, обеспечивающих выполнение видов работ	Количество часов (недель)
	Технические каналы утечки информации. Методы и средства технической разведки	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты. Раздел 1. Установка и настройка технических средств защиты информации. Тема 1.2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	8 часов
	Использование технических каналы утечки информации. Методы и средства технической разведки	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты. МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты. Раздел 1. Установка и настройка технических средств защиты информации. Тема 1.3. Измерение параметров физических полей. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.	8 часов

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов, с указанием тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	Выявление целей и задач физической защиты объектов информатизации	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты. МДК.03.02. Физическая защита линий связи ИТКС Раздел 2. Рассмотрение системы контроля и управления доступом. Тема 2.1. Рассмотрение системы контроля и управления доступом.	8 часов
	Применение системы телевизионного наблюдения	Система телевизионного наблюдения. Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты. МДК.03.02. Физическая защита линий связи ИТКС Раздел 2. Рассмотрение системы контроля и управления доступом. Тема 2.2. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.	8 часов

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов, с указанием тем, обеспечивающих выполнение видов работ	Количество часов (недель)
	Применение системы обнаружения комплекса инженерно-технических средств физической защиты.	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Место системы контроля и управления доступом(СКУД) в системе обеспечения информационной безопасности Особенности построения и размещения СКУД.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты МДК.03.02. Физическая защита линий связи ИТКС Раздел 2. Рассмотрение системы контроля и управления доступом. Тема 2.3. Рассмотрение датчиков периметра, их принципов работы.	8 часов
	Применение системы контроля и управления доступом.	Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты. МДК.03.02. Физическая защита линий связи ИТКС Раздел 2. Рассмотрение системы контроля и управления доступом. Тема 2.4. Выполнение звукоизоляции помещений системы шумоизоляции.	8 часов

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов, с указанием тем, обеспечивающих выполнение видов работ	Количество часов (недель)
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	Применение системы сбора, обработки, отображения и документирования информации	Система сбора, обработки, отображения и документирования информации. Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты Раздел 3. Реализация защиты от утечки по цепям электропитания и заземления. Тема 3.1. Разработка организационных и технических мероприятий по заданию преподавателя.	8 часов
	Разработка основной документации по инженерно-технической защите информации.	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по инженерно-технической защите информации защиты от внутренних угроз.	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты Раздел 3. Реализация защиты от утечки по цепям электропитания и заземления. Тема 3.2. Разработка основной документации по инженерно-технической защите информации.	6 часов
	Реализация защиты от утечки по цепям электропитания и заземления.	Написание документации за учебную практику	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты Раздел 3. Реализация защиты от утечки по цепям электропитания и заземления. Тема 3.3. Отчетная документация за учебную практику	2 часа
ВСЕГО:				72 часа

3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ

3.1. Требования к документации, необходимой для проведения практики:

- рабочая программа учебной практики;
- журнал профессионального модуля и видов практики;
- дневник учебной практики;
- отчёт по учебной практике.

3.2. Требования к учебно-методическому обеспечению практики:

- комплект учебно-методической документации;
- учебные стенды технических средств физической защиты объектов информатизации;
- комплект специального программного обеспечения.

3.3. Требования к материально-техническому обеспечению:

Учебная практика проводится в лаборатории и рабочих мест лаборатории информационных технологий, программирования и баз данных:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- дистрибутив устанавливаемой операционной системы;
- виртуальная машина для работы с операционной системой (гипервизор);
- СУБД;
- CASE-средства для проектирования базы данных;
- инструментальная среда программирования;
- пакет прикладных программ.

Оборудование лаборатории и рабочих мест лаборатории сетей и систем

передачи информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- стенды сетей передачи данных;
- структурированная кабельная система;
- эмулятор (эмуляторы) активного сетевого оборудования;
- программное обеспечение сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории программных и программно- аппаратных средств защиты информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- антивирусный программный комплекс;
- программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности.

3.4. Информационное обеспечение реализации программы:

3.4.1. Основные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

5. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/. – М.: Издательский центр «Академия», 2017. – 336с

6. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2012.

7. Электронный конспект лекций «Инженерно-техническая защита информации». Составитель: И.Н. Драч, преподаватель ГБОУ СПО РО «РКСИ»

8. Электронный конспект лекций «Криптографическая защита информации». Составитель: Шигаева С.В., преподаватель ГБОУ СПО РО «РКСИ»

9. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

3.4.3. Дополнительные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

2. Информационный портал по безопасности www.SecurityLab.ru.

3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>

4. Российский биометрический портал www.biometrics.ru

5. Сайт журнала Информационная безопасность <http://www.itsec.ru>

6. Сайт Научной электронной библиотеки www.elibrary.ru

7. Справочно-правовая система «Гарант» www.garant.ru

8. Справочно-правовая система «Консультант Плюс» www.consultant.ru

9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

10. Федеральный портал «Информационно-коммуникационные технологии в образовании» www.ict.edu.ru

11. Федеральный портал «Российское образование» www.edu.ru

3.5. Требования к руководителям практики от образовательного учреждения:

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу:

- наличие высшего профессионального образования, соответствующего профилю модуля «Защита информации техническими средствами» или первой и высшей квалификационной категории преподавателя специальных дисциплин.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав:

- дипломированные специалисты — преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин: «Технические средства информатизации», «Теория информационных систем», «Основы информационной безопасности», «Теория информации и кодирования».

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ

1. Дневник по практике, в котором указаны: лист инструктажей, характеристика базы практики и рабочего места, индивидуальный план работы студента в течение каждой недели учебной практики, лист самоанализа.

2. Отчёт о практике, в котором указаны виды работ по изученным разделам профессионального модуля с указанием самооценки освоенных профессиональных и общих компетенций и заключением руководителя учебной практики по пятибальной системе.

По итогам учебной практики проводятся защита отчётов по практике, предусмотрена за счёт часов отведённых на практику. Отчёты по практике и дневники сдаются руководителю учебной практики от колледжа.

Для оценки сформированности профессиональных и общих компетенций по итогам учебной практики оформляются аттестационные листы и итоговая оценочная ведомость.

Выполненная программа учебной практики, сданные дневники и отчёты, аттестационные листы и оценочные ведомости являются основанием успешного освоения ВД Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, отвечающих за предоставление студента к экзамену по модулю.