



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 техническими средствами

**Специальность 10.02.05 Обеспечение информационной безопасности
автоматизированных систем**

**Москва
2025**

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	3
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	6
3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ	15

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

ПМ.03 Защита информации техническими средствами

1.1. Цель и планируемые результаты освоения профессионального модуля

Результатом учебной практики профессионального модуля ПМ.03 Защита информации техническими средствами является овладение обучающимися видом деятельности по направлению: Защита информации техническими средствами, 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 техническими средствами
ПК 3.1	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	<ul style="list-style-type: none"> – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления 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; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и 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 объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.

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 1– ОК 9 ПК 3.1 – ПК 3.5	Инструктаж по охране труда и технике безопасности	2 часа
	Раздел 1. Применение технической защиты информации	
	Тема 1.1. Защита информации от утечки по проводному каналу	8 часов
	Тема 1.2. Защита информации от утечки по телефонному каналу	8 часов
	Тема 1.3. Защита информации от утечки по оптическому каналу	8 часов
	Тема 1.4. Применение технических средств защиты информации	8 часов
	Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации	
	Тема 2.1. Система телевизионного наблюдения	16 часов
	Тема 2.2. Применение средств физической защиты объектов информатизации	12 часов
	Тема 2.3. Эксплуатация инженерно-технических средств физической защиты объектов информатизации	8 часов
	Раздел 3. Отчётная документация учебной практики	
	Тема 3.1. Работа над отчётной документацией по учебной практике	2 часов
	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 техническими средствами	Изучение инструкций по охране труда и технике безопасности	Инструкции по охране труда и технике безопасности.	ПМ.03. Защита информации техническими средствами Инструктаж по охране труда и технике безопасности	2 часа
	- Определение каналов утечки побочных электромагнитных излучений и наводок (ПЭМИН); - Проведение измерений параметров побочных электромагнитных излучений и наводок; - Реализация защиты от утечки информации по цепям электропитания и заземления.	Система коммуникаций в качестве соединительных проводов. Средства защиты информации от несанкционированной утечки по проводному каналу.	ПМ.03. Защита информации техническими средствами МДК.03.01 Техническая защита информации Раздел 1. Применение технической защиты информации Тема 1.1. Защита информации от утечки по проводному каналу	8 часов
	- Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; - Реализация защиты от утечки информации по телефонному каналу.	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Средства защиты информации от несанкционированной утечки по телефонному каналу.	ПМ.03. Защита информации техническими средствами МДК.03.01 Техническая защита информации Раздел 1. Применение технической защиты информации Тема 1.2. Защита информации от утечки по телефонному каналу	8 часов
	- Проведение измерений параметров оптических характеристик для использования технических средств защиты информации; - Реализация защиты от утечки	Системы защиты информации по оптическому каналу.	ПМ.03. Защита информации техническими средствами МДК.03.01 Техническая защита информации Раздел 1. Применение технической 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)
	информации по оптическому каналу.		Тема 1.3. Защита информации от утечки по оптическому каналу	
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 техническими средствами	- Установка и настройка технических средств защиты информации.	Технические средства для уничтожения информации и носителей информации.	ПМ.03. Защита информации техническими средствами МДК.03.01 Техническая защита информации Раздел 1. Применение технической защиты информации Тема 1.4. Применение технических средств защиты информации	8 часов
	- Рассмотрение системы контроля и управления доступом; - Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.	Аналоговые и цифровые системы видеонаблюдения. Видеокамеры. Объективы. Поворотные системы. Инфракрасные осветители. Детекторы движения.	ПМ.03. Защита информации техническими средствами МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации Тема 2.1. Система телевизионного наблюдения	16 часов
	- Рассмотрение датчиков периметра, их принципов работы; - Монтаж различных типов датчиков.	Периметровые и объектовые средства обнаружения физических объектов. Телевизионное наблюдение с автоматизированного	ПМ.03. Защита информации техническими средствами МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Раздел 2. Применение инженерно-технических средств физической защиты	12 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)
		рабочего места.	объектов информатизации Тема 2.2. Применение средств физической защиты объектов информатизации	
Защита информации техническими средствами	- Разработка основной документации по инженерно-технической защите информации; - Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.	Установка и настройка периметровых и объектовых технических средств обнаружения физических объектов. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	ПМ.03. Защита информации техническими средствами МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации Тема 2.3. Эксплуатация инженерно-технических средств физической защиты объектов информатизации	8 часов
	Создание отчётной документации по учебной практике	Работа над отчётной документацией по учебной практике.	ПМ.03. Защита информации техническими средствами Раздел 3. Отчетная документация учебной практики Тема 3.1. Работа над отчетной документацией по учебной практике	2 часов
			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 Информационной безопасности (спец.аудитория)*:

- компьютерная техника – 15шт. персональных компьютеров, с возможностью подключения к сети «Интернет»;
- мультимедийный проектор;
- экран;
- МФУ;
- тренажер «Импульс-3»,
«Соната-РЗ.1»,
«Бинафон-Н2».

- стенд «Система контроля доступа»,
специализированное оборудование по защите информации от утечки по акустическому каналу и каналу ПЭМИН, технические средства контроля эффективности защиты информации от утечки по указанным каналам.
Комплект проекционного оборудования.

Программно-аппаратный комплекс для проверки выполнения норм эффективности защиты речевой информации по акустическому, виброакустическому каналу «СПРУТ-7А» в составе:

- измерительный шумомер-вибромметр-анализатор «Спрут»;
- измерительный микрофон «7052Е»;
- измерительный акселерометр «АР-98-100-01»;
- измерительный усилитель «SZA1».

Комплекс оценки эффективности защиты речевой информации от утечки по акустическим и акустоэлектрическим каналам «СМАРТ» в составе:
многофункциональный анализатор НЧ сигналов СКМ-21; измерительный микрофон ММ-1 с кабелем; измерительный акселерометр АР98-100 с кабелем; дистанционно управляемый генератор тестовых сигналов «СМАРТ-ГШ1».

Программно-аппаратный комплекс проведения специальных исследований «Легенда-05М».

АИ5-1, Антенна дипольная активная;

Магнитная антенна П 6-50;

Электрическая антенна П 6-51;

Электрическая антенна П 6-61;

Электрическая антенна П 6-62;

Электрическая антенна П 6-23М;

Опорно-поворотное устройство для П6-23М;

Штатив для антенн усиленный;

Детектор поля ST-110 (4 шт.);

Обнаружитель цифровых радиопередающих устройств ST165;

Поисковый приемник ближней зоны «Контур»;

Анализатор спектра «Anritsu» MS2720T-0720, со следящим генератором MS2720T-0820;

Генератор сигналов НЧ и ВЧ диапазонов HM8135, «NAMEG»;

Генератор ВЧ диапазона Г4-176;

Генератор НЧ диапазона ГЗ-109;

Поворотная платформа

Активная виброакустическая защита помещений от утечки информации по вибрационным и акустическим каналам. Система активной акустической и виброакустической защиты «Соната» в составе:

- универсальный блок питания

Соната-ИП2;

аппаратура дист. управления Соната-ДУ модель ДУ2 mini;

- виброизлучатель Соната-СВ- 45М (5 шт.);

- аудиоизлучатель Соната-СА-65М (1 шт.).

Активная защита объектов ЭВТ от утечки информации в форме информативных электрических сигналов и наводок по сети электропитания, системе заземления, инженерным коммуникациям, а также за счет ПЭМИН Соната-Р2

Право на использование модулей защиты от НСД и контроля устройств средства защиты информации Secret Net Studio 8.

Право на использование модулей защиты диска и шифрования контейнеров средства защиты информации Secret Net Studio 8.

Право на использование модуля персонального межсетевого экрана средства защиты информации Secret Net Studio 8.

Право на использование комплекта "Дополнительная защита" средства защиты информации Secret Net Studio 8.

Право на использование Средства защиты информации Secret Net 7. Клиент (автономный режим работы).

Право на использование Средства защиты информации Secret Net 7. Сервер безопасности класса С.

Право на использование Средства защиты информации Secret Net 7. Клиент (сетевой режим работы).

Право на использование Средства защиты информации Secret Net 7. Терминальное подключение.

Право на использование Средства защиты информации Secret Net LSP.

Право на использование Средства защиты информации TrustAccess для защиты 1 сервера

Право на использование Средства защиты информации TrustAccess для защиты 1 рабочей станции

Право на использование Сервера авторизации Средства защиты информации vGate R2 Standard (за 1 экземпляр Сервера авторизации)

Право на использование резервного Сервера авторизации vGate R2 (за 1 экземпляр Сервера авторизации vGate).

Право на использование Средства защиты информации vGate R2 Standard для защиты ESXi-хостов (за 1 физический процессор на защищаемом ESXi-хосте)

Право на использование Средства защиты информации vGate R2 Standard для Hyper-V для защиты хостов (за 1 физический процессор на защищаемом Hyper-V-хосте)

Право на использование резервного Сервера авторизации vGate для Hyper-V (за 1 экземпляр Сервера авторизации vGate).

Право на использование vGate для Hyper-V для защиты хостов (за 1 физический процессор на защищаемом Hyper-V-хосте).

Договор с ООО «Код безопасности» №КБ/27621/1/22 от 13.12.2017 г.;

-Virtual Box, Denver, Notepad++, MS Visual Studio 2015 Pro;

-комплект учебно-наглядных пособий;

-электронные пособия.

3.4. Информационное обеспечение реализации программы:

3.4.1. Основные печатные источники:

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – Москва : Академия. 2020.
2. Нестеров С.А. Основы информационной безопасности. Учебник для СПО. – Санкт-Петербург : Лань. 2022.

3.4.2. Основные электронные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд – Москва : Юрайт, 2024. – URL: <https://urait.ru/bcode/542340>
2. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования – 2-е изд. – Москва : Юрайт, 2024. – URL: <https://urait.ru/bcode/557735>

3.4.3. Дополнительные источники:

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

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике derobr.gov35.ru
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование» www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» www.law.edu.ru
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно-коммуникационные технологии в образовании» www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru
11. ЭБС «BOOK.ru» <https://book.ru>
12. Электронный Ресурс ЦОС СПО PROОбразование <https://profspo.ru>
13. Электронные учебники преподавателей РТУ МИРЭА <https://ibc.mirea.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 техническими средствами, отвечающих за предоставление студента к экзамену по модулю.