



МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

**ПМ.02 Защита информации в информационно-телекоммуникационных
системах и сетях с использованием программных и программно-
аппаратных (в том числе, криптографических) средств защиты**

**Специальность 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем**

**Москва
2025**

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	3
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	6
3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ	12
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ	16

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

1.1. Цель и планируемые результаты освоения профессионального модуля

Результатом учебной практики профессионального модуля ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты является овладение обучающимися видом деятельности по направлению: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении, 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	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и

	сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	<ul style="list-style-type: none"> – определения необходимых средств криптографической защиты информации; – использования программно-аппаратных криптографических средств защиты информации; – установки, настройки специализированного оборудования криптографической защиты информации; – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации.
Уметь	<ul style="list-style-type: none"> – выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – производить установку и настройку типовых программно-аппаратных средств защиты информации; – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации.
Знать	<ul style="list-style-type: none"> – типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; – основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; – основные понятия криптографии и типовые криптографические методы защиты информации.

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 2.1 – ПК 2.3	Инструктаж по охране труда и технике безопасности. Знакомство с заданием учебной практики.	6 часов
	Раздел 1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.	
	Тема 1.1. Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	8 часов
	Тема 1.2. Произвести установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы.	8 часов
	Тема 1.3. Обеспечение бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	8 часов
	Раздел 2. Защита информации в автоматизированных системах программными средствами.	
	Тема 2.1. Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации.	6 часов
	Тема 2.2. Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	6 часов
	Тема 2.3. Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации.	8 часов
	Тема 2.4. Осуществление обработки, хранения и передачи информации ограниченного доступа.	8 часов
	Раздел 3. Защита информации в автоматизированных системах программно-аппаратными средствами.	
	Тема 3.1. Защита информации в автоматизированных системах программно-аппаратными средствами.	6 часов
	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 программных и программно-аппаратных (в том числе, криптографических) 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	6 часов
	Обеспечение безопасности операционных систем	Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав. Параметры безопасности. Аппаратные средства шифрования Криптон 4,8 настройка, эксплуатация. Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование. Восстановление информации типовыми средствами. Программы восстановления информации.	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты Раздел 1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. Тема 1.1. Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	8 часов
	Технологии разграничения доступа	Программы надежного удаления информации. Архивирование информации. Программные средства резервного копирования. Настройка RAID-массивов Инсайдерская	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием	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)
		информация. Программы сбора информации о ПК. Настройка межсетевого экрана.	программных и программно-аппаратных средств защиты Раздел 1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. Тема 1.2. Произвести установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	
	Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей	Основные действия с виртуальной машиной. Работа с контрольными точками. Установка и настройка ПО eToken PKIClient. Настройка TMS в среде Active Directory. Настройка политик TMS. Настройка использования виртуального токена. Установка и настройка СКЗИ «КриптоПроCSP»	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты Раздел 1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. Тема 1.3. Обеспечение бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	8 часов
Защита информации в информационно-телекоммуникационных системах и сетях	Основы криптографических методов защиты информации	Свойства информационной безопасности. Свойства информационной безопасности, обеспечиваемые	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	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)
с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты		криптографическими методами защиты информации.	МДК.02.02. Криптографическая защита информации Раздел 2. Защита информации в автоматизированных системах программными средствами Тема 2.1. Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации.	
	Современные стандарты шифрования	Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES.	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты МДК.02.02. Криптографическая защита информации Раздел 2. Защита информации в автоматизированных системах программными средствами Тема 2.2. Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	6 часов
	Криптографические методы обеспечения безопасности сетевых технологий	Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES.	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты МДК.02.02. Криптографическая защита информации Раздел 2. Защита информации в автоматизированных системах	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)
			программными средствами Тема 2.3. Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации	
	Криптографические методы обеспечения безопасности сетевых технологий	Российские стандарты симметричного шифрования . Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147- 89. ГОСТ Р 34.12-2015.	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты МДК.02.02. Криптографическая защита информации программных и программно-аппаратных средств защиты Раздел 2. Защита информации в автоматизированных системах программными средствами Тема 2.4. Осуществление обработки, хранения и передачи информации ограниченного доступа	8 часов
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографичес	Теоретические основы корпоративной защиты от внутренних угроз.	Классификация нарушителей корпоративной ИБ. Особенности оценки ущерба. Исследование (аудит) организации с целью защиты от внутренних угроз.	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты МДК.02.03. Корпоративная защита от внутренних угроз информационной безопасности Раздел 3. Защита информации в автоматизированных системах программно-аппаратными средствами Тема 3.1. Защита информации в автоматизированных системах программно-аппаратными средствами	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)
ких) средств защиты	Обновление ОС и приложений через WSUS/yum/apt. Откат обновлений при возникновении ошибок.	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по корпоративной защите информации защиты от внутренних угроз. Обзор практики право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты МДК.02.03. Корпоративная защита от внутренних угроз информационной безопасности Раздел 3. Защита информации в автоматизированных системах программно-аппаратными средствами Тема 3.2. 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. 129
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 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении, отвечающих за предоставление студента к экзамену по модулю.