



**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 автоматизированных системах  
программными и программно-аппаратными средствами**

**Специальность 10.02.05 Обеспечение информационной безопасности  
автоматизированных систем**

**Москва  
2025**

## **СОДЕРЖАНИЕ**

<b>1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ .....</b>	<b>4</b>
<b>2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ .....</b>	<b>7</b>
<b>3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ .....</b>	<b>11</b>
<b>4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ .....</b>	<b>16</b>

# 1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

### 1.1. Цель и планируемые результаты освоения профессионального модуля

Результатом учебной практики профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами является овладение обучающимися видом деятельности по направлению: Защита информации в автоматизированных системах программными и программно-аппаратными 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 в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно- аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

### 1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	<ul style="list-style-type: none"> <li>– установки, настройки программных средств защиты информации в автоматизированной системе;</li> <li>– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;</li> <li>– тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;</li> <li>– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;</li> <li>– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;</li> <li>– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;</li> <li>– работы с подсистемами регистрации событий;</li> <li>– выявления событий и инцидентов безопасности в автоматизированной системе.</li> </ul>
Уметь	<ul style="list-style-type: none"> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</li> <li>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li> <li>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>– использовать типовые программные криптографические средства, в том числе электронную подпись;</li> <li>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;</li> <li>– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.</li> </ul>
Знать	<ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в</li> </ul>

	<p>операционных системах, компьютерных сетях, базах данных;</p> <ul style="list-style-type: none"> <li>– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;</li> <li>– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;</li> <li>– основные понятия криптографии и типовых криптографических методов и средств защиты информации</li> </ul>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### **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 2.6	Инструктаж по охране труда и технике безопасности. Знакомство с заданием учебной практики.	2 часа
	<b>Раздел 1.</b> Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.	
	<b>Тема 1.1.</b> Подготовка виртуальных машин для работы.	4 часа
	<b>Тема 1.2.</b> Настройка контроллера домена. Настройка DLP сервера. Установка и настройка сервера агентского мониторинга.	8 часов
	<b>Тема 1.3.</b> Установка агента мониторинга на машине нарушителя. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler).	8 часов
	<b>Тема 1.4.</b> Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.	6 часов
	<b>Раздел 2.</b> Технологии защиты узла и агентский мониторинг.	
	<b>Тема 2.1.</b> Настройка политик для структурных подразделений.	6 часов
	<b>Тема 2.2.</b> Настройка групповой политики домена.	8 часов
	<b>Раздел 3.</b> Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.	
	<b>Тема 3.1.</b> Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	20 часов
	<b>Тема 3.2.</b> Отчетная документация за учебную практику	2 часа
<b>ИТОГО:</b>		<b>72 часа</b>

## 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 автоматизированных системах программными и программно-аппаратными средствами	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
	Изучение принципов программно-аппаратной защиты информации от несанкционированного доступа	Особенности информации как предмета защиты. Виды, источники и носители защищаемой информации. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации.	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами. <b>МДК.02.01.</b> Программные и программно-аппаратные средства защиты информации. <b>Раздел 1.</b> Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз. <b>Тема 1.1.</b> Подготовка виртуальных машин для работы.	4 часа
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	Понятие и особенности утечки информации. Изучение современных программно-аппаратных комплексов.	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами <b>МДК.02.01.</b> Программные и программно-аппаратные средства защиты информации. <b>Раздел 1.</b> Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз. <b>Тема 1.2.</b> Настройка контроллера домена. Настройка DLP сервера. Установка и настройка сервера агентского мониторинга.	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)
	Установка агента мониторинга на машине нарушителя. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler).	Классификация технических средств разведки. Средства несанкционированного доступа к информации. Средства дистанционного съема информации.	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами. <b>МДК.02.01.</b> Программные и программно-аппаратные средства защиты информации. <b>Раздел 1.</b> Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз. <b>Тема 1.3.</b> Установка агента мониторинга на машине нарушителя. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler).	8 часов
	Мониторингсистем защиты	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами. <b>МДК.03.01.</b> Защита информации в ИТКС с использованием технических средств защиты. <b>Раздел 1.</b> Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз. <b>Тема 1.4.</b> Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.	6 часов



<b>Виды деятельности</b>	<b>Виды работ</b>	<b>Содержание освоенного учебного материала, необходимого для выполнения видов работ</b>	<b>Наименование учебных дисциплин, междисциплинарных курсов, с указанием тем, обеспечивающих выполнение видов работ</b>	<b>Количество часов (недель)</b>
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Настройка политик для структурных подразделений	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами. <b>МДК.02.02.</b> Криптографические средства защиты информации <b>Раздел 2.</b> Технологии защиты узла и агентский мониторинг. <b>Тема 2.1.</b> Настройка политик для структурных подразделений.	6 часов
	Технологии защиты узла и агентский мониторинг.	Установка программных агентов. Передача данных в центральную систему управления. Проактивное обнаружение проблем. Centreon. Kaspersky Endpoint Security Cloud.	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами. <b>МДК.02.02.</b> Криптографические средства защиты информации. <b>Раздел 2.</b> Технологии защиты узла и агентский мониторинг. <b>Тема 2.2.</b> Настройка групповой политики домена.	8 часов

<b>Виды деятельности</b>	<b>Виды работ</b>	<b>Содержание освоенного учебного материала, необходимого для выполнения видов работ</b>	<b>Наименование учебных дисциплин, междисциплинарных курсов, с указанием тем, обеспечивающих выполнение видов работ</b>	<b>Количество часов (недель)</b>
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	Система сбора, обработки, отображения и документирования информации. Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации.	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами. <b>Раздел 3.</b> Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз. <b>Тема 3.1.</b> Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.	20 часов
	Разработка основной документации по защите информации в автоматизированных системах программными и программно-аппаратными средствами.	Написание документации за учебную практику.	<b>ПМ.02</b> Защита информации в автоматизированных системах программными и программно-аппаратными средствами. <b>Раздел 3.</b> Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз. <b>Тема 3.2.</b> Отчетная документация за учебную практику.	2 часов
			<b>ВСЕГО:</b>	<b>72 часа</b>

### **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](http://www.fstec.ru)

2. Информационный портал по безопасности [www.SecurityLab.ru](http://www.SecurityLab.ru).

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

4. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)

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

6. Сайт Научной электронной библиотеки [www.elibrary.ru](http://www.elibrary.ru)

7. Справочно-правовая система «Гарант» [www.garant.ru](http://www.garant.ru)

8. Справочно-правовая система «Консультант Плюс» [www.consultant.ru](http://www.consultant.ru)

9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)

10. Федеральный портал «Информационно-коммуникационные технологии в образовании» [www.ict.edu.ru](http://www.ict.edu.ru)

11. Федеральный портал «Российское образование» [www.edu.ru](http://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 автоматизированных системах программными и программно-аппаратными средствами, отвечающих за предоставление студента к экзамену по модулю.