



**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное учреждение  
высшего образования**

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

**Колледж программирования и кибербезопасности**

**РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

**ПМ.03 Защита информации техническими средствами**

**Специальность 10.02.05 Обеспечение информационной безопасности  
автоматизированных систем**

**Москва  
2025**

## **СОДЕРЖАНИЕ**

<b>1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ .....</b>	<b>3</b>
<b>2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ.....</b>	<b>6</b>
<b>3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ.....</b>	<b>132</b>
<b>4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ.....</b>	<b>134</b>

# 1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

## ПМ.03 Защита информации техническими средствами

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

Результатом производственной 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 3	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"> <li>– установки, монтажа и настройки технических средств защиты информации;</li> <li>– технического обслуживания технических средств защиты информации;</li> <li>– применения основных типов технических средств защиты информации;</li> <li>– выявления технических каналов утечки информации;</li> <li>– участия в мониторинге эффективности технических средств защиты информации;</li> <li>– диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;</li> <li>– 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;</li> <li>– проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;</li> <li>– установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.</li> </ul>
Уметь	<ul style="list-style-type: none"> <li>– применять технические средства для криптографической защиты информации конфиденциального характера;</li> <li>– применять технические средства для уничтожения информации и носителей информации;</li> <li>– применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;</li> <li>– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;</li> <li>– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</li> <li>– применять инженерно-технические средства физической защиты объектов информатизации.</li> </ul>
Знать	<ul style="list-style-type: none"> <li>– порядок технического обслуживания технических средств защиты информации;</li> <li>– номенклатура применяемых средств защиты информации от несанкционированной утечки по техническим каналам;</li> <li>– физические основы, структура и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификация существующих физических полей и технических каналов утечки информации;</li> </ul>

	<ul style="list-style-type: none"> <li>– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;</li> <li>– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;</li> <li>– номенклатура и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;</li> <li>– основные принципы действия и характеристики технических средств физической защиты;</li> <li>– основные способы физической защиты объектов информатизации;</li> <li>– номенклатура применяемых средств физической защиты объектов информатизации.</li> </ul>
--	---

## 1.2. Количество недель (часов) на освоение программы производственной практики

Всего: 3 недели, 108 часа.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

### 2.1. Тематический план

Коды формируемых компетенций	Наименование тем профессионального модуля производственной практики	Объем времени, отведенный на практику (часах)
ОК.01 – ОК.09 ПК 3.1 – ПК 3.5	Инструктаж по охране труда и технике безопасности	2 часа
	<b>Раздел 1. Применение технической защиты информации</b>	
	<b>Тема 1.1.</b> Монтаж, обслуживание и эксплуатация технических средств защиты информации	32 часа
	<b>Тема 1.2.</b> Монтаж, обслуживание и эксплуатация средств защиты информации от несанкционированного съёма и утечки информации	32 часа
	<b>Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации</b>	
	<b>Тема 2.1.</b> Монтаж, обслуживание и эксплуатация инженерно-технической охраны объектов	32 часов
	<b>Тема 2.2.</b> Нормативно правовые акты как средства обеспечения защиты информации	8 часов
	<b>Раздел 3. Отчетная документация производственной практики</b>	
	<b>Тема 3.1.</b> Работа над отчетной документацией по производственной практике	2 часов
	<b>ИТОГО:</b>	<b>108 часов</b>

## 2.2. Содержание практики

Наименование разделов профессионального модуля (ПМ) и профессиональных компетенций	Содержание работ		Объём часов
ПМ.03 Защита информации техническими средствами			108 часов
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.	Производственная практика Виды работ		
	1	Инструктаж по охране труда и технике безопасности.	2
	2	Монтаж, обслуживание и эксплуатация технических средств защиты информации.	32
	3	Монтаж, обслуживание и эксплуатация средств защиты информации от несанкционированного съёма и утечки информации.	32
	4	Монтаж, обслуживание и эксплуатация инженерно-технической охраны объектов.	32
	5	Нормативно правовые акты как средства обеспечения защиты информации.	8
	6	Работа над отчетной документацией по производственной практике.	2
	ИТОГО:		

### **3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

#### **3.1. Требования к документации, необходимой для проведения практики:**

- Рабочая программа производственной практики;
- Журнал профессионального модуля и видов практики;
- Дневник производственной практики;
- Отчёт по производственной 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.

### **4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

#### **4.1. Требования к минимальному материально-техническому обеспечению**

Реализация рабочей программы производственной практики предполагает наличие следующей материально-технической базы:

- учебных кабинетов – лекционные аудитории с мультимедийным оборудованием;
- лаборатория программных и программно-аппаратных средств обеспечения информационной безопасности.

Лаборатория инженерно-технических средств защиты информации:

- Маркерная доска
- АРМ обучающихся по количеству обучающихся
- АРМ преподавателя
- Шкаф
- Проектор
- МФУ

Реализация рабочей программы производственной практики предполагает наличие на предприятии рабочих мест на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет.



## **4.2. Информационное обеспечение практики**

### **Основные источники:**

1. Сагдеев, К. М. Физические основы защиты информации: учебное пособие. – Ставрополь: изд-во СКФУ, 2018. – 394 с. – Режим доступа: <https://rucont.ru/efd/578849>. – Загл. с экрана.
2. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс]: учеб. пособие. – Электрон. дан. – Москва: Горячая линия-Телеком, 2018. – 442 с. – Режим доступа: <https://e.lanbook.com/book/5155>. – Загл. с экрана.
3. Бабенко, Л.К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс]: учеб. пособие. – Электрон. дан.
4. Москва: Горячая линия-Телеком, 2018. – 304 с. – Режим доступа: <https://e.lanbook.com/book/63228>. – Загл. с экрана.
5. Акмаров, П.Б. Кодирование и защита информации: учебное. – Ижевск: ФГБОУ ВО Ижевская ГСХА, 2019. – 136 с. – Режим доступа: <https://rucont.ru/efd/363163>. – Загл. с экрана.

### **Дополнительные источники:**

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

### **Интернет-ресурсы:**

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru).
2. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>.
3. Федеральный портал «Российское образование [www.edu.ru](http://www.edu.ru).
4. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru).

### **Общие требования к организации производственной практики**

Производственная практика проводится при освоении обучающимися профессиональных компетенций в рамках профессионального модуля ПМ.03 Защита информации техническими средствами и реализуются в соответствии с графиком учебного процесса.

Общее руководство производственной практикой осуществляет ответственный за организацию практики. Ответственный за организацию практики утверждает общий план её проведения, обеспечивает контроль

проведения со стороны руководителей производственного обучения, организует и проводит инструктивное совещание с руководителями практики, обобщает информацию по аттестации студентов, готовит отчет по итогам практики.

Производственная практика осуществляется на основе договоров между РТУ МИРЭА КПК и Организациями, в соответствии с которыми Организации предоставляют места для прохождения практики. В договоре РТУ МИРЭА КПК и Организация оговаривают все вопросы, касающиеся проведения практики. Консультирование по выполнению заданий, контроль посещения мест производственной практики, проверка отчетов по итогам практики и выставление оценок осуществляется руководителем практики от РТУ МИРЭА КПК. С началом практики проводится организационное собрание.

Организационное собрание проводится с целью ознакомления студентов с приказом, сроками практики, порядком организации работы во время практики в организации, оформлением необходимой документации, правилами техники безопасности, распорядком дня, видами и сроками отчетности и т.п.

Аттестация по итогам производственной практики проводится на основании результатов, подтвержденных документами соответствующих организаций (отзыв-характеристика, дневник-отчет).

## **5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

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

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

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

Основанием успешного освоения производственной практики являются выполненная программа производственной практики, сданные дневники и отчёты, аттестационные листы и оценочные ведомости.