



МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ 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

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

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

Результатом производственной 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"> – установки и настройки программных средств защиты информации; – тестирования функций, диагностики, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; – учета, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности.
Уметь	<ul style="list-style-type: none"> – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – использовать типовые программные криптографические средства, в том числе электронную подпись; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – 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.
Знать	<ul style="list-style-type: none"> – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; – основные понятия криптографии и типовых криптографических методов и средств защиты информации.

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 2.1 – ПК 2.6	Инструктаж по охране труда и технике безопасности	2 часа
	Раздел 1. Основные принципы программной и программно-аппаратной защиты информации	
	Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	8 часов
	Тема 1.2. Защищенная автоматизированная система	8 часов
	Тема 1.3. Дестабилизирующее воздействие на объекты защиты	18 часов
	Раздел 2. Защита автономных автоматизированных систем	
	Тема 2.2. Защита программ от изучения	8 часов
	Тема 2.1. Основы защиты автономных автоматизированных систем	8 часов
	Тема 2.3. Вредоносное программное обеспечение	8 часов
	Раздел 3. Защита информации в локальных сетях	
	Тема 3.1. Защита программ и данных от несанкционированного копирования	12 часов
	Тема 3.2. Защита информации на машинных носителях	8 часов
	Тема 3.3. Аппаратные средства идентификации и аутентификации пользователей	6 часов
	Тема 3.4. Системы обнаружения атак и вторжений	8 часов
	Тема 3.5. Основы построения защищенных сетей	4 часов
	Раздел 4. Защита информации в сетях общего доступа	
	Тема 4.1. Обеспечение безопасности межсетевое взаимодействия	8 часов
	Раздел 5. Защита информации в базах данных	
	Тема 5.1. Защита информации в базах	2 часа

	данных	
	ИТОГО:	108 часов

2.2. Содержание практики

Наименование разделов профессионального модуля (ПМ) и профессиональных компетенций	Содержание работ		Объём часов
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами			108 часов
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.	Производственная практика		
	Виды работ		
	1	Знакомство с предприятием. Прохождение инструктажей по ТБ.	4
	2	Анализ принципов построения систем информационной защиты производственных подразделений.	12
	3	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	18
	4	Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	16
	5	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	16
	6	Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	18
	7	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	18
	8	Оформление отчетной документации	6
ИТОГО:			108

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

Оборудование лабораторий

- Стол - рабочее место обучающегося для работы за компьютером – 15 шт.
- Стул п/мягкий - 15 шт.
- Шкаф для хранения сумок, пакетов студентов -1 шт.
- Жалюзи - 2 шт.
- Проектор – 1 шт.
- Экран – 1 шт.
- Огнетушители – 1 шт.
- Персональный компьютер – рабочее место обучающегося – 15 шт.
- Локальная сеть – есть
- Учебный стенд "Программные средства криптографии", SCRYPTO – 1 шт

Программное Обеспечение

- ОС Windows 10
- Visual Management Studio
- Microsoft Visio
- Архиватор WinRAR
- Приложения MS Office 2016
- Adobe Reader X
- Notepad++
- Google Chrome
- Консультант Плюс
- MS SQL-Server
- Oracle VM Virtual Box
- CrypTool
- ItMan
- Snort и Suricata
- Wireshark
- Nmap Free Security Scanner
- ОС Linux: Lubuntu и Kali Linux
- Cisco

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. Дергачев К.В. Защита информации: лабораторный практикум: учебное пособие / Дергачев К.В., Титарев Д.В. — Москва: Русайнс, 2021. — 158 с. — ISBN 978-5-4365-6774-7. — URL: <https://book.ru/book/940250> (дата обращения: 23.04.2021). — Текст: электронный.
2. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для студентов высших учебных заведений / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В., Славнов. — М.: Горячая линия – Телеком, 2018г.
3. Сагдеев К.М. Физические основы защиты информации Бакалавриат: учебное пособие / Сагдеев К.М., Петренко В.И., Чипига А.Ф. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 394 с. — URL: <https://book.ru/book/928736> (дата обращения: 23.04.2021). — Текст: электронный.
4. Бабаш А.В. Криптографические методы защиты информации: учебник / Бабаш А.В., Баранова Е.К. — Москва: КноРус, 2020. — 189 с. — ISBN 978-5-406-00169-1. — URL: <https://book.ru/book/933943> (дата обращения: 23.04.2021). —

Текст: электронный.

5. Баранова Е.К. Криптографические методы защиты информации. Лабораторный практикум +CD: учебное пособие / Баранова Е.К., Бабаш А.В. — Москва: КноРус, 2017. — 196 с. — (для бакалавров). — ISBN 978- 5-406-03802-4. — URL: <https://book.ru/book/920017> (дата обращения: 23.04.2021). — Текст: электронный.

6. Баричев С.Г. Основы современной криптографии: учебный курс для студентов высших учебных заведений / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — М.: Горячая линия-Телеком, 2017г.

7. Криптографические методы защиты информации: лабораторный: практикум / сост. Калмыков И.А., Науменко Д.О., Гиш Т.А. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — URL: <https://book.ru/book/928786> (дата обращения: 23.04.2021). — Текст: электронный.

Дополнительные источники:

1. Москвитин Г.И. Комплексная защита информации в организации: монография / Москвитин Г.И. — Москва: Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: <https://book.ru/book/934814> (дата обращения: 23.04.2021). — Текст: электронный.

2. Нестандартные методы защиты информации: лабораторный: практикум / сост. Пашинцев В.П., Ляхов А.В. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 196 с. — URL: <https://book.ru/book/928802> (дата обращения: 23.04.2021). — Текст: электронный.

3. Тараскин М.М. Комплексная защита информации в организации: монография / Тараскин М.М., и др. — Москва: Русайнс, 2017. — 353 с. — ISBN 978-5-4365-1561-8. — URL: <https://book.ru/book/922538> (дата обращения: 23.04.2021). — Текст: электронный.

4. Царегородцев А.В. Методы и средства защиты информации в государственном управлении: учебное пособие / Царегородцев А.В., Тараскин М.М. — Москва: Проспект, 2017. — 205 с. — ISBN 978-5-392- 20353-6. — URL: <https://book.ru/book/922352> (дата обращения: 23.04.2021). — Текст: электронный.

5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студентов СПО. - М.: ИД "ФОРУМ": ИНФРА-М, 2016г.

6. Мельников В.П. Информационная безопасность: учебное пособие для студентов средних профессиональных учебных заведений. - М.: Издательский центр "Академия", 2010г.

4.3. Интернет-ресурсы:

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 <http://depobr.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» <http://www.law.edu.ru/>
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
10. Сайт Научной электронной библиотеки www.elibrary.ru

Общие требования к организации производственной практики

Производственная практика проводится при освоении обучающимися профессиональных компетенций в рамках профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными 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.