



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 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 ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	3
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	5
3. УСЛОВИЯ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	10
4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	10
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	12

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ 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 производственной 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 информационно-телекоммуникационных систем и сетей, 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 1	Эксплуатация информационно-телекоммуникационных систем и сетей
------	--

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 оборудование 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;

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 2.3	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 телекоммуникационная сеть	8 часов
	Тема 1.3. Дестабилизирующее воздействие на объекты защиты	18 часов
	Раздел 2. Защита телекоммуникационных систем	
	Тема 2.1. Основы защиты телекоммуникационной систем	8 часов
	Тема 2.2. Защита программ от изучения	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

Коды формируемых компетенций	Наименование тем профессионального модуля производственной практики	Объем времени, отведенный на практику (часах)
	Тема 3.5. Основы построения защищенных сетей	4 часа
	Раздел 4. Защита информации в сетях общего доступа	
	Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	8 часов
	Раздел 5. Защита информации в базах данных	
	Тема 5.1. Защита информации в базах данных	2 часов
	ИТОГО	108

2.2. Содержание практики

Наименование разделов профессионального модуля (ПМ) и профессиональных компетенций	Содержание работ		Объём часов
ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты			108 часов
<p>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.</p> <p>ПК 2.2 Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.</p> <p>ПК 2.3 Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей с использованием программных и программно-аппаратных, в том числе криптографических средств защиты</p>	Производственная практика Виды работ		
	1	Предмет и задачи программно-аппаратной защиты информации	8 часов
	2	Защищенная телекоммуникационная сеть	8 часов
	3	Дестабилизирующее воздействие на объекты защиты	18 часов
	4	Основы защиты телекоммуникационной систем	8 часов
	5	Защита программ от изучения	8 часов
	6	Вредоносное программное обеспечение	8 часов
	7	Защита программ и данных от несанкционированного копирования	12 часов

Наименование разделов профессионального модуля (ПМ) и профессиональных компетенций	Содержание работ		Объём часов
информации.	8	Защита информации на машинных носителях	8 часов
	9	Аппаратные средства идентификации и аутентификации пользователей	6 часов
	10	Системы обнаружения атак и вторжений	8 часов
	11	Основы построения защищенных сетей	4 часа
	12	Обеспечение безопасности межсетевого взаимодействия	8 часов
	13	Защита информации в базах данных	2 часа
	14	Работа над отчетной документацией по производственной практике.	2 часа
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.

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. Телекоммуникационные системы и сети: Учебное пособие в 3 томах. Том 2 – Радиосвязь, радиовещание, телевидение / Катунин Г.П., Мамчев Г.В., Попантопуло В.Н., В.П. Шувалов; под ред. Профессора В.П. Шувалова. – изд. 2-е и до. – М.: Горячая линия – Телеком, 2016.
2. Садовомовский А.С., Приемо-передающие радиоустройства и системы связи: Учебное пособие для студентов специальности 21020165 / А.С. Кадомовский. – Ульяновск: УлГТУ, 2016.
3. Парфенов Ю.А. Кабели электросвязи. М.: Эко-Трендз, 2016;
4. Иоргачев Д.В. Бондаренко О.В. Волоконно-оптические кабели и линии связи. – М.:ЭКО_ТРЕНДЗ, 2016;
5. <http://izmer-ls.ru/>Руководство по эксплуатации линейно-кабельных сооружений местных сетей связи. (Утв. ГОСКОМСВЯЗИ РФ 05.06.1998);
6. Ксенофонов С.Н. Портнов Э.Л. Направляющие системы электросвязи. Сборник задач; учебное пособие для ВУЗов. 2-е изд. стереотип, - М.:
7. Хрусталева З.А. Источники питания радиоаппаратуры: учебник для студ. Учреждений сред. проф. образования / З.А. Хрусталева, С.В. Парфенов. – М.: Издательский центр «Академия», 2016 – 240 с.

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

Общие требования к организации производственной практики

Производственная практика проводится при освоении обучающимися

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