

Министерство цифрового развития, связи и массовых коммуникаций  
Российской Федерации  
Волго-Вятский филиал  
ордена Трудового Красного Знамени федерального государственного  
бюджетного образовательного учреждения высшего образования  
«Московский технический университет связи и информатики»  
(ВВФ МТУСИ)

СОГЛАСОВАНО:  
Генеральный директор  
ООО «Альфа-сервис»

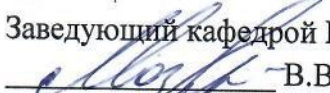
УТВЕРЖДЕНА  
(с учетом изменений и дополнений)  
на заседании кафедры  
инфокоммуникационных  
и профессиональных дисциплин

Протокол заседания № 7  
от «22» марта 2021 г.


 /Судаев С.В./  
«11» марта 2021 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ**  
**ПМ.03 Обеспечение информационной безопасности в**  
**телекоммуникационных системах и сетях вещания**  
для специальности  
11.02.10 Радиосвязь, радиовещание и телевидение

Нижний Новгород, 2021

Заведующий кафедрой ИКиПД  
 В.В. Мазниченко

Авторы:

Преподаватель кафедры ИКиПД  
А.В. Лимонов 

Разработано на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования

**11.02.10 Радиосвязь, радиовещание и телевидение**, утверждённого приказом Министерства образования и науки РФ от 28 июля 2014 г. № 812.

## Содержание

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	3
2. СОДЕРЖАНИЕ ПРАКТИКИ	6
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ	7
4. КРИТЕРИИ ОЦЕНКИ ВЫПОЛНЕНИЯ ЗАДАНИЙ ПРАКТИКИ	8
5. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА	10
6. ТРЕБОВАНИЯ К СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ И ПОЖАРНОЙ БЕЗОПАСНОСТИ	10
7. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ И ИНТЕРНЕТ-РЕСУРСОВ	11
ПРИЛОЖЕНИЕ 1. АТТЕСТАЦИОННЫЙ ЛИСТ	12

# **1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

## **1.1. Область применения программы учебной практики**

Программа учебной практики является составной частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС 3+ по специальности 11.02.10 «Радиосвязь, радиовещание и телевидение».

Учебная практика является частью учебного процесса и направлена на формирование у студентов **профессиональных и общих компетенций**:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.

ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование сетей вещания.

## **1.2. Цели и задачи практики**

Учебная практика базируется на междисциплинарных курсах профессиональных модулей:

*МДК.03.01. Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания.*

*МДК.03.02. Технология использования систем условного доступа в сетях вещания.*

В результате прохождения практики обучающийся должен получить **практический опыт:**

- выявления каналов утечки информации;
- определения необходимых средств защиты;
- проведения аттестации объекта защиты (проверки уровня защищенности);
- разработки политики безопасности для объекта защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявления возможных атак на автоматизированные системы;
- установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;
- конфигурирования автоматизированных систем и информационно-коммуникационных сетей;
- проверки защищенности автоматизированных систем и информационно-коммуникационных сетей;
- защиты баз данных;
- организации защиты в различных операционных системах и средах;
- шифрования информации;

**уметь:**

- классифицировать угрозы информационной безопасности;
- проводить выборку средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
- использовать программные продукты, выявляющие недостатки систем защиты;
- производить установку и настройку средств защиты;
- конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- выполнять тестирование систем с целью определения уровня защищенности;
- использовать программные продукты для защиты баз данных;
- применять криптографические методы защиты информации;

**знать:**

- каналы утечки информации;
- назначение, классификацию и принципы работы специализированного оборудования;
- принципы построения информационно-коммуникационных сетей;
- возможные способы несанкционированного доступа;
- законодательные и нормативные правовые акты в области информационной безопасности;
- правила проведения возможных проверок;
- этапы определения конфиденциальности документов объекта защиты;
- структуру систем условного доступа и принцип их работы;
- возможные способы, места установки и настройки программных продуктов;
- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- собственные средства защиты различных операционных систем и сред;
- способы и методы шифрования информации.

### **1.3. Количество часов на освоение программы учебной практики**

Рабочая программа рассчитана на прохождение обучающимися практики в объеме 36 часов.

## Содержание учебной практики

п/п	Наименование МДК заданий практики по ПМ03	Количество часов
	<p><i>МДК.03.01. Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания.</i></p> <p><i>МДК.03.02. Технология использования систем условного доступа в сетях вещания.</i></p>	<b>36</b>
1	Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации. Изучение мировых стандартов по защите информации	6
2	Модели защиты информационных систем. Организация работы персонала с конфиденциальной информацией.	6
3	Анализ информационных рисков предприятия. Исследование системы анализа рисков и проверки политики информационной безопасности предприятия	6
4	Идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий (аудит) Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы.	6
5	Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам.	6
6	Шифрование с открытым ключом и электронная цифровая подпись на GPG. Метод шифрования с открытым ключом RSA. Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.	6

## Планируемые результаты освоения программы практики

Практика направлена на формирование у обучающегося общих и профессиональных компетенций. Результатом освоения программы практики является приобретение обучающимся практических профессиональных умений по основным видам профессиональной деятельности.

Контроль и оценка результатов освоения практики осуществляется руководителем практики.

Коды и наименования проверяемых компетенций или их сочетаний	Виды и объем работ, выполненных обучающимся во время практики
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.	Разработка политики безопасности для объекта защиты; установка, настройки специализированного оборудования по защите информации; выявление возможных атак на автоматизированные системы; установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей
ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.	выполнить расчет и установку специализированного оборудования для максимальной защищенности объекта; произвести установку и настройку средств защиты; конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; выполнять тестирование систем с целью определения уровня защищенности; использовать программные продукты для защиты баз данных; применить криптографические методы защиты информации;
ПК 3.3. Обеспечивать безопасное администрирование сетей вещания	Использовать технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов; конфигурации защищаемых сетей; алгоритмы работы тестовых программ; средства защиты различных операционных систем и сред; способы и методы шифрования информации

## Критерии оценки выполнения заданий практики

Задание практики	Объекты контроля	Показатели выполнения	Критерии оценки
Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации. Изучение мировых стандартов по защите информации	Организация рабочего места	Качество подготовки рабочего места	100% готовность к работам
	Процесс выполнения согласно инструкционной карте	Соблюдение алгоритма	Полное соблюдение
		Время подготовки	6 академических часов, включая отчет
	Результат	Точность и правильность выполнения	Соответствие с техническими требованиями
Модели защиты информационных систем. Организация работы персонала с конфиденциальной информацией.	Организация рабочего места	Качество подготовки рабочего места	100% готовность к работам
	Процесс выполнения согласно инструкционной карте	Соблюдение алгоритма	Полное соблюдение
		Время подготовки	6 академических часов, включая отчет
	Результат	Точность и правильность выполнения	Соответствие с техническими требованиями
Анализ информационных рисков предприятия. Исследование системы анализа рисков и проверки политики информационной безопасности предприятия	Организация рабочего места	Качество подготовки рабочего места	100% готовность к работам
	Процесс выполнения согласно инструкционной карте	Соблюдение алгоритма	Полное соблюдение
		Время подготовки	6 академических часов, включая отчет
	Результат	Точность и правильность выполнения	Соответствие с техническими требованиями
Идентификация и аутентификация пользователей; ограничение доступа в систему;	Организация рабочего места	Качество подготовки рабочего места	100% готовность к работам
	Процесс выполнения согласно инструкционной карте	Соблюдение алгоритма	Полное соблюдение
		Время подготовки	6 академических

разграничение доступа; регистрация событий (аудит) Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы.	Результат	Точность и правильность выполнения	часов, включая отчет
			Соответствие с техническими требованиями
Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам.	Организация рабочего места	Качество подготовки рабочего места	100% готовность к работам
	Процесс выполнения согласно инструкционной карте	Соблюдение алгоритма	Полное соблюдение
		Время подготовки	6 академических часов, включая отчет
	Результат	Точность и правильность выполнения	Соответствие с техническими требованиями
Шифрование с открытым ключом и электронная цифровая подпись на GPG. Метод шифрования с открытым ключом RSA. Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.	Организация рабочего места	Качество подготовки рабочего места	100% готовность к работам
	Процесс выполнения согласно инструкционной карте	Соблюдение алгоритма	Полное соблюдение
		Время подготовки	6 академических часов, включая отчет
	Результат	Точность и правильность выполнения	Соответствие с техническими требованиями

## **Оценка выполнения работы по заданию практики**

5 (Отлично) – «отлично» выставляется, если студент имеет глубокие знания теоретического материала по теме задания, показывает точность и правильность выполнения задания в соответствии с технологическими требованиями на 90-100%, смог ответить на все уточняющие и дополнительные вопросы.

4 (Хорошо) – «хорошо» выставляется, если студент показал знание теоретического материала по теме задания, показывает точность и правильность выполнения в соответствии с технологическими требованиями на 80-90%, смог ответить почти на все уточняющие и дополнительные вопросы.

3 (Удовлетворительно) – «удовлетворительно» выставляется, если студент в целом освоил теоретический материал по теме задания, показывает точность и правильность выполнения в соответствии с технологическими требованиями на 70-80%

2 (Неудовлетворительно) – «неудовлетворительно» выставляется студенту, если он имеет существенные пробелы в знаниях теоретического материала по теме задания, не сумел выполнить практическое задание на 70%.

## **Требования к оформлению отчета**

По завершению прохождения практики обучающийся должен подготовить и представить руководителю практики отчет, содержащий:

1. Рабочую тетрадь по учебной практике
2. Аттестационный лист

В рабочей тетради по учебной практике по каждой теме должно быть представлено задание, описан порядок его выполнения, представлены необходимые схемы, чертежи, рисунки и вычисления. По результатам выполнения задания должны быть сделаны выводы о выполнении задания.

Текущий учет результатов освоения учебной практики фиксируется в ведомости преподавателями, руководителями учебной практики по своим МДК.

## **Требования к соблюдению техники безопасности и пожарной безопасности**

Все работы во время прохождения учебной практики должны выполняться в строгом соответствии с правилами техники безопасности и пожарной безопасности КТ МТУСИ.

В случае прохождения учебной практики в организациях – базах практики, в первый день практики обучающиеся проходят инструктаж по технике безопасности и пожарной безопасности, о чем в соответствующем журнале свидетельствуют подписи инструктирующего и инструктируемого. Все работы во время прохождения учебной практики в организациях – базах практики должны выполняться в строгом соответствии с правилами техники безопасности и пожарной безопасности указанных организаций.

## Перечень рекомендуемой литературы и интернет-ресурсов

### Основная литература

1. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — Саратов : Профобразование, 2021. — 214 с. — ISBN 978-5-4488-1294-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО ПРОФобразование : [сайт]. — URL: <https://profspo.ru/books/108005/>
2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО ПРОФобразование : [сайт]. — URL: <https://profspo.ru/books/97562/>
3. Зубкова, Т. М. Технология разработки программного обеспечения : учебное пособие для СПО / Т. М. Зубкова. — Саратов : Профобразование, 2019. — 468 с. — ISBN 978-5-4488-0354-3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО ПРОФобразование : [сайт]. — URL: <https://profspo.ru/books/86208/>

### Дополнительная литература

1. Майстренко, А. В. Мультимедийные средства обработки информации : учебное пособие для СПО / А. В. Майстренко, Н. В. Майстренко. — Саратов : Профобразование, 2020. — 81 с. — ISBN 978-5-4488-0734-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/90169.html>
2. Соловьев, Н. А. Цифровая обработка информации в задачах и примерах : учебное пособие для СПО / Н. А. Соловьев, Н. А. Тишина, Л. А. Юркевская. — Саратов : Профобразование, 2020. — 122 с. — ISBN 978-5-4488-0596-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/92201.html>
3. Прохорова, О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. — ISBN 978-5-8114-7338-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/158939/>

### Интернет-источники:

1. ЭБС издательства «Лань»: <http://www.e.lanbook.com/>
2. ЭБС IPRbooks: <http://iprbookshop.ru>
3. Научная электронная библиотека eLIBRARY.RU: <https://elibrary.ru/>
4. ЭБС POLPRED.COM: <https://polpred.com/>
5. ЭР ЦОС СПО «ПРОФобразование»: <https://profspo.ru/>
6. Российская государственная библиотека (РГБ): <https://www.rsl.ru/>
7. Российская национальная библиотека (РНБ): <http://nlr.ru/>
8. Государственная публичная научно-техническая библиотека (ГПНТБ): <http://www.gpntb.ru/>

9. Президентская библиотека: <https://www.prilib.ru/>
10. Российский фонд фундаментальных исследований: <https://podpiska.rfbr.ru/>
11. Информационная система «Регламент»: <https://www.reglament.pro/>
12. Информационная система «Единое окно доступа к образовательным ресурсам»: <http://window.edu.ru/>
13. Росстандарт: <http://www.gost.ru/>
14. Сайт Европейской организации по стандартизации (ETSI): <http://www.etsi.org>
15. Сайт Международного союза электросвязи: <http://www.itu.int>

ПРИЛОЖЕНИЕ 1.

Министерство цифрового развития, связи и массовых коммуникаций  
Российской Федерации  
Волго-Вятский филиал  
ордена Трудового Красного Знамени федерального государственного  
бюджетного образовательного учреждения высшего образования  
«Московский технический университет связи и информатики»

**АТТЕСТАЦИОННЫЙ ЛИСТ ПО УЧЕБНОЙ ПРАКТИКЕ**  
по специальности

---

---

\_\_\_\_\_ *Фамилия, Имя, Отчество*  
обучающегося(аяся) на **3** курсе в группе \_\_\_\_\_  
успешно прошел(ла) учебную практику по профессиональному модулю \_\_\_\_\_  
программы подготовки специалистов среднего звена  
в объеме \_\_\_\_\_ часов с « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_\_ г. по « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_\_ г.

**Виды и качество выполнения работ**

Виды работ, выполненных обучающимся во время практики	Освоенные компетенции				Оценка выполнения работ
	ОК 1-9	ПК 3.1	ПК 3.2	ПК 3.3	
Итоговая, интегральная оценка					

**Характеристика профессиональной деятельности студента во время учебной практики**(отношение к работе, личные качества и т.д.)

---



---



---



---



---



---



---

Дата «\_\_» \_\_\_\_\_ 20\_\_ г.

Подпись руководителя практики \_\_\_\_\_/ФИО