

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»

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 ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**ПМ. 03 Обеспечение информационной безопасности в
телекоммуникационных системах и сетях вещания**

для специальности 11.02.10


Радиосвязь, радиовещание и телевидение

(очная форма обучения)

Нижний Новгород, 2021 г.

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

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	стр. 4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	6
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	13

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

1.1. Область применения программы

Рабочая программа профессионального модуля является программой подготовки специалистов среднего звена (ППССЗ) в соответствии с ФГОС по специальности СПО **11.02.10– «Радиосвязь, радиовещание и телевидение»** в части освоения основного вида профессиональной деятельности (ВПД): **Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания** и соответствующих профессиональных компетенций (ПК):

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.

Рабочая программа профессионального модуля может быть использована при повышении квалификации и переподготовке работников связи при наличии профессионального образования.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным ВПД и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь 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 дисциплины

Максимальная учебная нагрузка обучающегося – 156 часов, из них:

- обязательная учебная нагрузка обучающегося – 104 часа;
- самостоятельная работа обучающегося – 52 часа.

Учебная практика – 36 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

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.
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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК.3.1	Раздел 1 Применение комплексной системы защиты информации	78	52	22	-	26	-	18	-
ПК-3.2-3.3	Раздел 2. Применение программно-аппаратных средств защиты информации	78	52	22	-	26	-	18	-
	Учебная практика	36							-
	Производственная практика (по профилю специальности)	-							
Всего:		192	104	44	-	52	-	36	-

3.2. Содержание обучения по профессиональному модулю ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1 Применение комплексной системы защиты информации		78	2
МДК 3.1 Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания		78	
Тема 1.1. Основы информационной безопасности	Содержание	12	
	1. Понятие информационной безопасности, характеристика ее составляющих. Классификация и анализ угроз информационной безопасности в телекоммуникационных системах.	2	
	2. Средства инженерной защиты.	2	
	3. Охранно-пожарная сигнализация.	2	
	4. Телевизионные системы охраны.	2	
	5. Системы управления доступом.	2	
	6. Интегрированные системы охраны.	2	
	Практические занятия	10	
	1 Применение систем сигнализации и охраны.	2	
	2 Применение систем пожарной сигнализации	2	
	3 Применение систем телевизионной охраны	2	
	4 Применение систем управления доступа на объект информатизации.	2	
	5 Применение интегрированных систем охраны.	2	

Тема 1.2. Правовое обеспечение информационной безопасно- сти	Содержание			
			6	
	1	Информация как объект права. Нормативно-правовые основы информационной безопасности в РФ.	2	
	2	Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации.	2	2
	3	Несанкционированные и непреднамеренные воздействия.	2	2
	Практические занятия		2	
	1	Средства противодействия несанкционированным и непреднамеренным воздействиям.	2	
	Содержание		12	
	1.	Оптический канал утечки информации.	2	
	2.	Акустический канал утечки информации.	2	2
Тема 1.3 Организационное обеспече- ние информационной без- опасности	3.	Электрический и электромагнитный каналы утечки информации	2	
	4.	Специальные проверки.	2	
	5.	Защита систем связи.	2	2
	6.	Выбор механизмов и средств обеспечения информационной безопасности.	2	2
	Практические занятия		10	
	1	Выявление и блокирование оптических каналов утечки информации	2	
	2	Выявление и блокирование акустических каналов утечки информации	2	
	3	Выявление и блокирование электрических и электромагнитных каналов утечки информации	2	
	4	Методы и средства проведения специальных проверок. Методы и средства защиты систем связи	2	
	5	Методы и средства обеспечения информационной безопасности.	2	
Самостоятельная работа при изучении раздела ПМ 1			26	
Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).				

Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Поиск информации в Интернет. Примерная тематика внеаудиторной самостоятельной работы: 1. Нормативно-правовые основы информационной безопасности в РФ. 2. Сравнительный анализ законодательства в сфере ИБ 3. Изучение систем сигнализации и охраны. 4. Системы телевизионной охраны 5. Системы управления доступа на объект информатизации. 6. Способы кодирования информационных сообщений в системах связи. 7. Система доступа в сетях сотовой связи.				
Учебная практика по МДК.3.1 1. Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации. Изучение мировых стандартов по защите информации 2. Модели защиты информационных систем. Организация работы персонала с конфиденциальной информацией. 3. Анализ информационных рисков предприятия. Исследование системы анализа рисков и проверки политики информационной безопасности предприятия			18	
Раздел 2. Применение программно-аппаратных средств защиты информации			78	
МДК 3.2 Технология использования систем условного доступа в сетях вещания			78	
Тема 2.1 Программно-аппаратные средства защиты информации	Содержание		16	
	1.	Термины и определения в области информационной безопасности.	2	
	2	Вредоносное программное обеспечение.	2	
	3	Вредоносные утилиты.	2	
	4	Классы IP-адресов.	2	
	5	Деление сети на подсети. Расчет масок и подсетей.	2	
	6	Доктрина информационной безопасности Российской Федерации	2	

Тема 2.2 Системы условного доступа в сетях вещания	7	Криптология.	2	
	8	Информационная безопасность в телекоммуникационных и информационно-комму- никационных сетях.	2	
	Практические занятия		12	2
	1	Лицензионные и свободно распространяемые программные продукты.	2	
	2	Обязанности пользователей и ответственных за обеспечение безопасности ИТ.	2	
	3	Установка и анализ виртуальной операционной системы.	2	
	4	Расчет сетей и масок протокола IPv4.	2	
	5	Деление сети с классовой IP-адресацией на подсети.	2	
	6	Деление сети на подсети с заданными хостами.	2	
	Содержание		14	2
	9	Спутниковое телевизионное вещание.	2	
	10	Система условного доступа.	2	
	11	Разработка политики безопасности.	2	
	12	Система условного доступа - программно-аппаратный механизм.	2	
	13	Технологии безопасности беспроводных сетей.	2	
	14	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.	2	
	15	Выбор системы условного доступа.	2	
	Практические занятия		10	
	7	Распределенные DoS атаки.	2	
	8	Электронная цифровая подпись.	2	
	9	Создание резервных копий на различных носителях информации.	2	
	10	Способы аутентификации пользователей на основе биометрических данных.	2	
	11	Изучение и настройка BIOS.	2	

<p>Самостоятельная работа при изучении раздела ПМ Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Поиск информации в Интернет. Практическая отработка навыков аутентификации и идентификации в сетевых операционных системах.</p>	<p>26</p>	
<p>Учебная практика по МДК.3.2 1. 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. 2. Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. 3. 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.</p>	<p>18 6 6 6</p>	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

- 1 – ознакомительный (узнавание ранее изученных объектов, свойств);
- 2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
- 3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие следующих помещений для проведения занятий:

1. Учебная аудитория для проведения лекционных занятий, укомплектованная специализированной мебелью и техническими средствами обучения.
2. Учебная аудитория для проведения практических занятий и лабораторных работ - лабораторий «Информационной безопасности»; «Звукового вещания».
3. Учебная аудитория для проведения текущего контроля и промежуточной аттестации, оснащенная компьютерной техникой.
4. Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду ВВФ МТУСИ.

Оборудование лабораторий и рабочих мест лабораторий:

1. Информационной безопасности

Коммутатор ComrexSRX2224, интерактивная доска ClassicSolution, дистрибутив ПО ViPNetClient, дистрибутив СКЗИ "КриптоПроCSP" версии 4.0, дистрибутив ПО ViPNetAdministrator, персональные компьютеры, классная доска, экран, проектор, комплект учебно-методической документации.

2. Звукового вещания

Аппаратно-студийный блок ПТС, частотомер ЧЗ-57, генератор НЧ сигналов ГЗ-112, генератор НЧ сигналов ГЗ-109, осциллографы: С1-68, С1-81, С1-65, радиоприемник "Ишим", компьютер (монитор, системный блок, мышь), акустические системы, цифровой генератор сигналов FM, передатчик сигналов радиовещательного диапазона ОМВ FMExciter 87,5-108МГц, осциллограф телевизионный С9-32, генератор телетеста ЛАПСИ ТТ-03, генератор испытательных сигналов ТВ Г6-8, блок питания Г6-30, макет передатчика проводного вещания ПТПВ-500/250, тестовый телевизор аналогового ТВ, телевизионный модулятор МТ-300, транскодер телевизионный Лапси ТКВ-03, измеритель АЧХ Х1-50, компьютеры для преподавателя и обучающихся, классная доска, экран, проектор, комплект учебно-методической документации.

Реализация программы модуля предполагает обязательную учебную практику, которую рекомендуется проводить в учебной аудитории для проведения практических занятий – компьютерные мастерские.

Оборудование компьютерных мастерских:

Коммутатор ComrexSRX2224, интерактивная доска ClassicSolution, дистрибутив ПО ViPNetClient, дистрибутив СКЗИ "КриптоПроCSP" версии 4.0, дистрибутив ПО ViPNetAdministrator, оборудованное рабочее место для преподавателя, персональные компьютеры, классная доска, экран, проектор.

Используемое программное обеспечение:

- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal.
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);

- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex.Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- AdobeReader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

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 PROФобразование : [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 PROФобразование : [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 PROФобразование : [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/>

Электронные базы периодических изданий:

ЭБС eLIBRARY.RU: <https://elibrary.ru/>

Электронные ресурсы:

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 «PROФобразование»: <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.prlib.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>

4.3. Общие требования к организации образовательного процесса

Образовательное учреждение обязано ежегодно обновлять основную профессиональную образовательную программу (в части профессионального модуля), программы производственных практик; методических материалов, обеспечивающих реализацию соответствующих образовательных технологий с учетом запросов работодателей в контексте сложившегося уровня развития науки, техники, технологии, социальной сферы, а также действующего законодательства. Должна обеспечиваться эффективная самостоятельная работа обучающихся в сочетании с совершенствованием управления ею со стороны преподавателей.

4.4. Кадровое обеспечение образовательного процесса

Реализация рабочей программы профессионального модуля должна обеспечиваться педагогическими кадрами, имеющими высшее образование, соответствующее профилю профессионального модуля.