МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УДМУРТСКОЙ РЕСПУБЛИКИ

АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ УДМУРТСКОЙ РЕСПУБЛИКИ

«ТЕХНИКУМ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ АЛЕКСАНДРА ВАСИЛЬЕВИЧА ВОСКРЕСЕНСКОГО»

СОГЛАСОВАНО:
_____

_____/_____/
«___»_____ 20___г.

УТВЕРЖДЕНО:
Директор АПОУ УР «ТРИТ им. А.В. Воскресенского»
_____Е.А. Кривоногова
«___»_____ 20___г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

по специальности среднего профессионального образования

11.02.15 Инфокоммуникационные сети и системы связи

20___г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО)

11.02.15 Инфокоммуникационные сети и системы связи

Организация-разработчик: Автономное профессиональное образовательное учреждение Удмуртской Республики «Техникум радиоэлектроники и информационных» (далее АПОУ УР «ТРИТ им. А.В. Воскресенского»)

Разработчики:

1. Москова О.М., зам.директора АПОУ УР «ТРИТ им. А.В. Воскресенского»
2. Масалёв В.Г., мастер производственного обучения АПОУ УР «ТРИТ им. А.В. Воскресенского»

Рассмотрено и рекомендовано методическим объединением профессионального цикла

Протокол № ____ от «____»_____ 20___ г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

1.1 Область применения программы

Программа профессионального модуля (далее рабочая программа) – является частью основной профессиональной образовательной программы, разработанной в соответствии с ФГОС СПО с учетом примерной основной образовательной программой по специальности 11.02.15 Инфокоммуникационные сети и системы связи.

1.2 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся осваивает основной вид деятельности (ОВД): «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие и профессиональные компетенции:

1.2.1 Перечень общих компетенций (ОК)

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 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 учетом 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 учетом 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 документациейна государственном и иностранном языках

1.2.2 Перечень профессиональных компетенций (ПК)

Код	Наименование профессиональных компетенций
ВД.3	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
ПК 3.1.	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности
ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
ПК 3.3.	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.

1.2.3 Перечень знаний и умений, осваиваемых в процессе овладения основным видом деятельности:

С целью овладения указанным основным видом деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен показать следующие результаты обучения:

Критерий обучения	Результат обучения
Владеть навыками	– анализа сетевой инфраструктуры; – выявления угроз и уязвимости в сетевой инфраструктуре; – разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; – осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи; – использования специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи; – разработки и оформления требований к программным модулям по предложенной документации; – разработки тестовых наборов (пакетов) для программного модуля; разработки тестовых сценариев программного средства; – инспектирования разработанных программных модулей на предмет соответствия стандартам кодирования; – интегрирования модулей в программное обеспечение; – отладки программных модулей.
Уметь	– классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; – определять оптимальные способы обеспечения информационной безопасности; – осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; – выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов; – выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; – защищать базы данных при помощи специализированных программных продуктов; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – 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; – анализировать проектную и техническую документацию; – использовать специализированные графические средства построения и анализа архитектуры программных продуктов; – организовывать заданную интеграцию модулей в программные средства на базе имеющейся архитектуры и автоматизации бизнес-процессов; – определять источники и приемники данных; – проводить сравнительный анализ; – выполнять отладку, используя методы и инструменты условной компиляции (классы Debug и Trace); – разрабатывать тестовые пакеты и тестовые сценарии; – выполнять тестирование интеграции; – организовывать постобработку данных; – выполнять ручное и автоматизированное тестирование программного модуля.
Знать	– принципы построения информационно-коммуникационных сетей; – международные стандарты информационной безопасности; акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; – технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; – классификацию угроз сетевой безопасности; – методы и способы защиты информации, передаваемой по кабельным направляющим системам; – правила проведения возможных проверок, согласно нормативных документов ФСТЭК; – средства защиты различных операционных систем и среды передачи информации; – модели процесса разработки программного обеспечения; – основные принципы процесса разработки программного обеспечения; основные подходы к интегрированию программных модулей; – основные протоколы доступа к данным; – методы и способы идентификации сбоев и ошибок при интеграции приложений; – графические средства проектирования архитектуры программных продуктов; – методы организации работы в команде разработчиков; – стандарты качества программной документации; – основные методы отладки; – современные технологии и инструменты интеграции.

1.1.4. Перечень личностных результатов[1]

Код	Наименование личностных результатов
ЛР 3	Демонстрирующий приверженность традиционным духовно-нравственным ценностям, культуре народов России, принципам честности, порядочности, открытости. Действующий и оценивающий свое поведение и поступки, поведение и поступки других людей с позиций традиционных российских духовно-нравственных, социокультурных ценностей и норм с учетом осознания последствий поступков. Готовый к деловому взаимодействию и неформальному общению с представителями разных народов, национальностей, вероисповеданий, отличающий их от участников групп с деструктивным и девиантным поведением. Демонстрирующий неприятие социально опасного поведения окружающих и предупреждающий его. Проявляющий уважение к людям старшего поколения, готовность к участию в социальной поддержке нуждающихся в ней
ЛР 4	Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию в течение жизни Демонстрирующий позитивное отношение к регулированию трудовых отношений. Ориентированный на самообразование и профессиональную переподготовку в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 6	Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации
ЛР 9	Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде
ЛР 13	Поддерживающий коллективизм и товарищество в организации инженерной деятельности, развитие профессионального и общечеловеческого общения, обеспечение разумной свободы обмена научно-технической информацией, опытом
ЛР 14	Добросовестный, исключающий небрежный труд при выявлении несоответствий установленным правилам и реалиям, новым фактам, новым условиям, стремящийся добиваться официального, законного изменения устаревших норм деятельности
ЛР 15	Настойчивый в доведении новых инженерных решений до их реализации, в поиске истины, в разрешении сложных проблем
ЛР 16	Стремящийся к постоянному повышению профессиональной квалификации, обогащению знаний, приобретению профессиональных умений и компетенций, овладению современной компьютерной культурой, как необходимому условию

[1] Коды личностных результатов, которые необходимы для освоения дисциплины (профессионального модуля), определяются преподавателем в соответствии с Рабочей программой воспитания ООП.

	освоения новейших методов познания, проектирования, разработки экономически грамотных, научно обоснованных технических решений, организации труда и управления, повышению общей культуры поведения и общения
ЛР 17	Борющийся с невежеством, некомпетентностью, технофобией, повышающий свою техническую культуру;
ЛР 18	Организованный и дисциплинированный в мышлении и поступках
ЛР 19	Ответственный за выполнение взятых обязательств, реализацию своих идей и последствия инженерной деятельности, открыто признающий ошибки
ЛР 20	Соблюдающий общепринятые этические нормы и правила делового поведения, корректный, принципиальный, проявляющий терпимость и непредвзятость в общении с гражданами
ЛР 21	Способствующий своим поведением установлению в коллективе товарищеского партнерства, взаимоуважения и взаимопомощи, конструктивного сотрудничества
ЛР 23	Стремящийся в любой ситуации сохранять личное достоинство, быть образцом поведения, добропорядочности и честности во всех сферах общественной жизни;
ЛР 24	Стремящийся к повышению уровня самообразования, своих деловых качеств, профессиональных навыков, умений и знаний
ЛР 25	Соответствующий по внешнему виду общепринятому деловому стилю

1.3 Количество часов, отводимое на освоение профессионального модуля:

Всего часов – 490,
в том числе практическая подготовка – 294 часа.
Из них учебная нагрузка обучающегося на освоение МДК – 338 часов, в том числе:
самостоятельная работа обучающегося – 40 часов;
консультации – 10 часов
Практики: учебная – 72 часов,
производственная – 72 часа
промежуточная аттестация, в том числе экзамен по модулю – 8 часов

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

Коды профессиональны х, общих компетенций	**Наименования разделов профессионального модуля**	**Всего часов** *(макс. учебная нагрузка и практики)*	в т.ч. в форме практ. подготовки	**Объем времени, отведенный на освоение междисциплинарного курса (курсов) (МДК)**					**Практика**		**Промежуточная аттестация**
				Обязательная аудиторная учебная нагрузка обучающегося			**Самостоя-тельная работа обучаю-щегося**	**Консультации**	**Учебная,** часов	**Производ-ственная,** часов	
				Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая проект (работа),** часов					
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
ПК 3.1. – 3.3. ОК 01. – 19.	Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационн ых системах и сетях связи	**170**	**78**	**170**	78	-	20	6			
ПК 3.1. – 3.3. ОК 01. – 10.	Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационн ых системах и сетях связи	**168**	**72**	**168**	72	-	**20**	4			
	Учебная практика	**72**							**72**		
	Производственная практика	**72**								**72**	
	Экзамен по модулю	**8**									**8**
	Всего:	**490**	**150**	**102**	**150**	**-**	**20**	**10**	**72**	**72**	**8**

2.2 Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающихся	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч
1	2	3
МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи		
Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		**170/78**
Тема 1.1. Основы безопасности информационных технологий	**Содержание**	
	Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий. Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность	4
	Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности. Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты.	6
	Принципы построения системы обеспечения безопасности информации в автоматизированной системе. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры. Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации	6
	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных Пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности	4
	Практическое занятие №1 Установка прав доступа с помощью СПО ЗИ.	4
	Практическое занятие №2 Законодательство в сфере защиты информации	2
	Практическое занятие №3 Разработка политики безопасности объекта.	2
Тема 1.2. Обеспечение безопасности информационных технологий	**Содержание**	
	Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ. Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации. Документы, регламентирующие правила парольной и	6

	антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты. Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуск сотрудников. Правила именования пользователей. Процедура авторизации сотрудников	
	Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация. Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем. Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов	6
	Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы. Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации. Концепция безопасности информационных технологий предприятия.	6
	Практическое занятие №4 Установка и снятие СЗИ с помощью программы СЗИ НСД**.**	4
	Практическое занятие №5 Исследование возможностей управления пользователями с помощью СЗИ НСД**.**	4
	Практическое занятие №6 Исследование настройки маркировки документов с помощью СЗИ НСД	4
	Практическое занятие №7 Разработка инструкции по организации защиты данных пользователя	4
	Практическое занятие №8 Организация процедуры экстренной модификации	4
	Практическое занятие №9 Разработка плана защиты и обеспечения непрерывной работы автоматизированной системы	4
	Практическое занятие №10 Разработка концепции информационной безопасности организации	4
Тема 1.3. Средства защиты информации от несанкционированного доступа	**Содержание**	
	Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов. Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации	4

	Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOCK). Назначение, состав и возможности СЗИ (например, «Блокпост- 2000» и «Блокпост-сеть»). Назначение и особенности применения СЗИ НСД (например, «Страж NT»). Назначение и специфика применения комплекса ЗИ (например, «Соболь»)	4
	Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей. Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей. Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана. Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа	4
	Практическое занятие №11 Ввод информации в САПР СЗИ. Расчет радиуса контролируемой зоны с помощью САПР СЗИ	4
	Практическое занятие №12 Исследование механизма доступа в систему с использованием СПО ЗИ и УП	4
	Практическое занятие №13 Сравнение средств защиты информации от НСД	4
	Практическое занятие №14 Разработка алгоритма генерации одноразовых паролей	4
	Практическое занятие №15 Организация разграничения доступа к ресурсам системы	4
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей	**Содержание**	
	Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация. Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов.	4
	Анализ содержимого почтового и WEB-трафика. HTTP-трафик. Виртуальные частные сети. Решение на базе ОС Windows 2003. VPN на основе криптошлюза (например, «Континент-К»)	4
	Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности. Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак	4
	Практическое занятие №16 Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП	4
	Практическое занятие №17 Исследование проблемных ситуаций с использованием СПО ЗИ и УП	4
	Практическое занятие №18 Сравнение типов межсетевых экранов	4
	Практическое занятие №19 Проведение анализа трафика сайта	4
	Практическое занятие №20 Сравнение средств анализа защищенности	4
Самостоятельная работа обучающегося		**20**
Законодательство в области защиты информации		2
Разработка инструкции по организации парольной и антивирусной защиты		4
Проведение сравнительного анализа программных средств, реализующих инфраструктуру открытых ключей		4
Проведение сравнительного анализа сетевых агентов сканирования		4

Проведение анализа трафика сайта		4
Подготовка к дифференцированному зачету по МДК 3.01		2
Консультации		**6**
Консультация по теме 1.2		2
Консультация по теме 1.3		2
Консультация по теме 1.4		2
Дифференцированный зачет по МДК 03.01		**4**
МДК 03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи		
Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи		**168/72**
Тема 2.1. Основы информационной безопасности	**Содержание**	
	Основные понятия информационной безопасности. Сущность и понятия защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	4
	Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности	4
	Практическое занятие №21 Исследование возможностей многофункционального поискового прибора	4
	Практическое занятие №22 Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга	4
Тема 2.2. Организационно-правовые аспекты защиты информации	**Содержание**	
	Структура правовой защиты информации. Система документов в области защиты информации. Организационные основы защиты информации. Принципы организационной защиты информации. Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации	4
	Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере	4
	Практическое занятие №23 Исследование возможностей работы фильтров сетевых помехоподавляющих	4
	Содержание	

Тема 2.3. Комплексная система защиты информации	Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации. Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна	6
	Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны. Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение. Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз	4
	Практическое занятие №24 Исследование уязвимостей и построение модели угроз объекта защиты.	4
	Практическое занятие №25 Исследование возможностей устройства для защиты объектов информатизации	4
	Практическое занятие №26 Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств	4
	Практическое занятие №27 Организация мер по комплексному обследованию защищенности информационной системы	2
Тема 2.4. Инженерно-техническая защита информации	**Содержание**	
	Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты. Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации. Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации. Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации. Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД	6
	Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи. Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания	6
	Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок. Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания. Контроль слаботочных цепей. Принципы контроля линий заземления	6

	Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации. Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники	6
	Практическое занятие №28 Исследование возможностей системы оценки защищенности оптических линий связи.	4
	Практическое занятие №29 Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	4
	Практическое занятие №30 Исследование возможностей системы оценки защищенности выделенных помещений.	4
	Практическое занятие №31 Исследование возможностей индикаторов поля	4
Тема 2.5. Криптографическая защита информации	**Содержание**	
	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных. Требования, предъявляемые к криптографическим системам. Симметричные и ассиметричные криптосистемы	4
	Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования. Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом	4
	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа	4
	Практическое занятие №32 Поиск и локализация скрытых видеокамер	4
	Практическое занятие 33 Исследование методов защиты сотовых телефонов от несанкционированного прослушивания	4
	Практическое занятие №34 Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов	4
	Практическое занятие №35 Поиск устройств негласного съема информации с помощью многофункционального поискового прибора	4
	Практическое занятие №36 Исследование методов криптографической защиты информации	2
Тема 2.6. Аттестация и лицензирование объектов защиты	**Содержание**	
	Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ. Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний	4
	Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании	4

	Практическое занятие №37 Исследование работы генератора шума по сети электропитания и линиям заземления	4
	Практическое занятие №38 Поиск и обнаружение радиоизлучающих средств	4
	Практическое занятие №39 Разработка инструкции по аттестации объектов информатизации	2
Самостоятельная работа обучающегося		**20**
Практическое применение антивирусных программ для защиты информации от несанкционированного доступа.		4
Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.		4
Составление доклада по перспективным направлениям развития средств комплексной защиты информации		2
Разработка пакета документации по инженерно-технической защите информации на объекте		4
Изучение возможностей инженерно-технических средств защиты информации		2
Изучение технических характеристик инженерно-технических средств защиты информации		2
Подготовка к дифференцированному зачету по МДК 3.02		2
Консультации		**4**
Консультация по темам 2.1-2.3		
Консультация по темам 2.4-2.6		
Дифференцированный зачет по МДК 03.02		**4**
Учебная практика **Виды работ:** - установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов; - установка и настройка типовых программно-аппаратных средств защиты информации; - использование программно-аппаратных и инженерно-технических средств; - настройка, регулировка и ремонт оборудования средств защиты; - выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой; - проведение типовых операции настройки средств защиты операционных систем; - проведение аттестации объектов защиты; - определение источников несанкционированного доступа, исходя из модели угроз; - определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта; - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств; - защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК; - защита информации организационными методами в соответствии с инструкциями на объекте.		**72**
Промежуточная аттестация по учебной практике: дифференцированный зачёт, 4 семестр		
Производственная практика Виды работ: 1. Участие в создании комплексной системы защиты на предприятии. 2. Применение программно-аппаратных средств защиты информации на предприятии 3. Применение инженерно-технических средств защиты информации на предприятии. 4. Применение криптографических средств защиты информации на предприятии.		**72**
Промежуточная аттестация по производственной практике: дифференцированный зачёт, 4 семестр		
Промежуточная аттестация по модулю в форме Экзамена по модулю		**8**
	Всего	**490**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Требования к материально-техническому обеспечению

Для реализации всех видов занятий, предусмотренных программой профессионального модуля, используются следующие специальные помещения: Кабинет «Компьютерного моделирования», лаборатории: «Информационной безопасности телекоммуникационных систем».

Кабинет «Компьютерного моделирования»

Оборудование кабинета:

– автоматизированные рабочие места обучающихся (ПК с доступом в интернет и программным обеспечением общего и профессионального назначения;

– автоматизированное рабочее место преподавателя (ПК с доступом в интернет и программным обеспечением общего и профессионального назначения;

− доска;

− комплект учебно-наглядных пособий и плакатов по дисциплине;

− мультимедийное оборудование.

Лаборатория «Информационной безопасности телекоммуникационных систем»

Оборудование лаборатории:

− автоматизированные рабочие места обучающихся (ПК с доступом в интернет и программным обеспечением общего и профессионального назначения;

− автоматизированное рабочее место преподавателя (ПК с доступом в интернет и программным обеспечением общего и профессионального назначения;

− доска;

− комплект учебно-наглядных пособий и плакатов;

− мультимедийное оборудование;

− программно-аппаратный межсетевой экран (комплекс сетевой защиты);

− комплекс антивирусного программного обеспечения;

− комплекс программного обеспечения шифрования и дешифрования данных с использованием различных систем шифрования;

− устройства защиты слаботочных систем коммуникаций (телефонная линия, радиотрансляция).

Перечень лицензионного программного обеспечения:

– системы электротехнического моделирования.

В рамках изучения междисциплинарных курсов предусмотрена практическая подготовка на рабочих местах предприятий, направление деятельности которых соответствует виду деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи».

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и иные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе

3.2.1 Основные источники:

1. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие для спо / Р. Н. Гилязова. – 2-е изд., стер. – Санкт-Петербург : Лань, 2021. – 44 с. – ISBN 978- 5-8114-8249-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/173796 (дата обращения: 16.11.2021). – Режим доступа: для авториз. пользователей.

2. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учеб-ное пособие / С. Н. Никифоров. – Санкт-Петербург : Лань, 2020. – 96 с. – ISBN 978-5-8114-5720-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL:

https://e.lanbook.com/book/146802 (дата обращения: 27.11.2020). – Режим доступа: для авториз. пользователей.

3.2.2 Дополнительные источники:

1. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие для спо / С. Н. Никифоров. – 2-е изд., стер. – Санкт-Петербург : Лань, 2021. – 96 с. – ISBN 978-5-8114-7907-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/167186 (дата обращения: 16.11.2021). – Режим доступа: для авториз. пользователей.
2. Петренко, В. И. Защита персональных данных в информационных системах. Практи-кум : учебное пособие для спо / В. И. Петренко, И. В. Мандрица. – Санкт-Петербург : Лань, 2021. – 108 с. – ISBN 978-5-8114-6924-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/153678 (дата обращения: 16.11.2021). – Режим до-ступа: для авториз. пользователей.
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 (дата обращения: 16.11.2021). – Режим доступа: для авториз. пользователей.

3.2.3 Иные ресурсы

Сети и системы связи

Сводный реферативный журнал «Связь»

Журнал «Системы безопасности»

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Формы и методы контроля и оценки результатов обучения
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	-грамотность устной и письменной речи; - ясность формулирования и изложения мыслей	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	- эффективность выполнения правил ТБ вовремя учебных занятий, при прохождении учебной и производственной практик	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен
ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	- классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно; - анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный; - возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно; мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме; недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме; - тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности	Текущий контроль: – тестирование; – письменный опрос; – устный опрос; – оценка выступления с докладом; – оценка результатов выполнения практических работ; – экспертное наблюдение выполнения практических работ. Промежуточная аттестация: – дифференцированный зачёт (оценка процесса и результатов выполнения видов работ на учебной и производственной практике); – экзамен.

	определен верно	
ПК 3.2 Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи	- для обеспечения информационной безопасности выбраны оптимальные способы; - выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях	Текущий контроль: – тестирование; – письменный опрос; – устный опрос; – оценка выступления с докладом; – оценка результатов выполнения практических работ; – экспертное наблюдение выполнения практических работ. Промежуточная аттестация: – дифференцированный зачёт (оценка процесса и результатов выполнения видов работ на учебной и производственной практике); – экзамен.
ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования	- мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными; - политика безопасности сетевых элементов и логических сетей разработана в полном объеме; - расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами; - установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами; - конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной	Текущий контроль: – тестирование; – письменный опрос; – устный опрос; – оценка выступления с докладом; – оценка результатов выполнения практических работ; – экспертное наблюдение выполнения практических работ. Промежуточная аттестация: – дифференцированный зачёт (оценка процесса и результатов выполнения видов работ на учебной и производственной практике); – экзамен.

	безопасности и отраслевыми стандартами; - базы данных максимально защищены при помощи специализированных программных продуктов; - ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами	