Приложение II.2

к программе СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

2023

Составители:
АНО ПО "БИТ"

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

наименование профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам**.**
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2.	*Защита информации в автоматизированных системах программными и программно-аппаратными средствами*
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и

	программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В ходе освоения профессионального модуля учитывается движение к достижению личностных результатов обучающимися ЛР 15,16,17

В результате освоения профессионального модуля студент должен:

Иметь практический опыт в	− установки, настройки программных средств защиты информации в автоматизированной системе; − обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; − тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ; − решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; − применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; − учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; − работы с подсистемами регистрации событий; − выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; − устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; − диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; − применять программные и программно-аппаратные средства для защиты информации в базах данных; − проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; − применять математический аппарат для выполнения криптографических преобразований; − использовать типовые программные криптографические средства, в том числе электронную подпись; − применять средства гарантированного уничтожения информации; − 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
знать	− особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; − методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; − типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

	− основные понятия криптографии и типовых криптографических методов и средств защиты информации; − особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; − типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов – 802 часа, в том числе:

- 250 часов вариативной части, направленных на усиление обязательной части программы профессионального модуля.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Суммарный объем нагрузки, час	Объем профессионального модуля, час						
			Обучение по МДК				Практика		Промежуточная аттестация
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Самостоятельная работа	Учебная, часов	Производственная (по профилю специальности), часов	
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	**Раздел 1.** Применение программных и программно-аппаратных средств защиты информации	**274**	**244**	112	20	**17**			**6**
ПК 2.3	**Раздел 2.** Применение криптографических средств защиты информации	**162**	**162**	76	10	**14**			**6**
ПК 2.1-ПК 2.3	**Учебная практика**						**108**		
ПК 2.1-ПК 2.3	**Производственная практика (по профилю специальности)**, часов							**252**	
	Промежуточная аттестация (экзамен (квалификационный)) – демонстрационный экзамен								**7**
	Всего:							**802**	

2.2. Тематический план и содержание профессионального модуля (ПМ)

*Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся , курсовая работ (проект)		Объем часов
1	2		3
Раздел 1. Применение программных и программно-аппаратных средств защиты информации			128
МДК.2.1 Программные и программно-аппаратные средства защиты информации			273
Тема 1.1. Защищенная автоматизированная система	**Содержание**		**46**
	1	Автоматизация процесса обработки информации	2
		Домашнее задание: чтение и анализ литературы [1] стр. 165-172	
	2	Понятие автоматизированной системы.	2
		Домашнее задание: чтение и анализ литературы [3] стр. 123-125	
	3	Особенности автоматизированных систем в защищенном исполнении.	2
		Домашнее задание: чтение и анализ литературы [4] стр. 123-125	
	4	Основные виды АС в защищенном исполнении.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 165-172	
	5	Методы создания безопасных систем	2
		Домашнее задание: чтение и анализ литературы [3] стр. 123-125	
	6	Методология проектирования гарантированно защищенных КС	2
		Домашнее задание: чтение и анализ литературы [4] стр. 123-125	
	7	Дискреционные модели	2
		Домашнее задание: чтение и анализ литературы [1] стр. 165-172	
	8	Мандатные модели	2
		Домашнее задание: чтение и анализ литературы [3] стр. 123-125	
	Практические занятия		**20**
	1	Учет, обработка, хранение и передача информации в АИС	
	2	Ограничение доступа на вход в систему.	
	3	Идентификация и аутентификация пользователей	
	4	Разграничение доступа.	
	5	Регистрация событий (аудит).	
	6	Контроль целостности данных	
	7	Уничтожение остаточной информации.	
	8	Управление политикой безопасности. Шаблоны безопасности	
	9	Криптографическая защита. Обзор программ шифрования данных	
	10	Управление политикой безопасности. Шаблоны безопасности	

Тема 1.2. Дестабилизирующее воздействие на объекты защиты	**Содержание**		**8**
	1	Источники дестабилизирующего воздействия на объекты защиты	2
		Домашнее задание: чтение и анализ литературы [1] стр. 123-125	
	2	Способы воздействия на информацию	2
		Домашнее задание: чтение и анализ литературы [1] стр. 126-129	
	3	Причины и условия дестабилизирующего воздействия на информацию	2
		Домашнее задание: чтение и анализ литературы [1] стр. 165-172	
	Практические занятия		**2**
	1	Распределение каналов в соответствии с источниками воздействия на информацию	
Тема 1.3. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**		**14**
	1	Понятие несанкционированного доступа к информации	2
		Домашнее задание: чтение и анализ литературы [1] стр. 123-125	
	2	Основные подходы к защите информации от НСД	2
		Домашнее задание: чтение и анализ литературы [1] стр. 126-129	
	3	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	2
		Домашнее задание: чтение и анализ литературы [1] стр. 165-172	
	4	Доступ к данным со стороны процесса	2
		Домашнее задание: чтение и анализ литературы [1] стр. 123-125	
	5	Особенности защиты данных от изменения. Шифрование.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 126-129	
	Практические занятия		**4**
	1	Организация доступа к файлам	
	2	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	
Раздел 2. Защита автономных автоматизированных систем			128
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**		**10**
	1	Работа автономной АС в защищенном режиме	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Алгоритм загрузки ОС. Штатные средства замыкания среды	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Расширение BIOS как средство замыкания программной среды	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	2

		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
Тема 2.2. Защита программ от изучения	**Содержание**		**12**
	1	Изучение и обратное проектирование ПО	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Способы изучения ПО: статическое и динамическое изучение	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Задачи защиты от изучения и способы их решения	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Защита от отладки.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Защита от дизассемблирования	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	6	Защита от трассировки по прерываниям.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
Тема 2.3. Вредоносное программное обеспечение	**Содержание**		**14**
	1	Вредоносное программное обеспечение как особый вид разрушающих воздействий	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Бот-неты. Принцип функционирования. Методы обнаружения	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Классификация антивирусных средств. Сигнатурный и эвристический анализ	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	6	Защита от вирусов в "ручном режиме"	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	7	Основные концепции построения систем антивирусной защиты на предприятии	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
Промежуточная аттестация по МДК.02.01			2

Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**		**12**
	1	Несанкционированное копирование программ как тип НСД	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Привязка ПО к аппаратному окружению и носителям.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Защитные механизмы в современном программном обеспечении на примере MS Office	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	Практические занятия		**4**
	1	Защита информации от несанкционированного копирования с использованием специализированных программных средств	
	2	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	
Тема 2.5. Защита информации на машинных носителях	**Содержание**		**18**
	1	Проблема защиты отчуждаемых компонентов ПЭВМ.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Методы защиты информации на отчуждаемых носителях. Шифрование.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Безвозвратное удаление данных. Принципы и алгоритмы.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	Практические занятия		**8**
	1	Применение средства восстановления остаточной информации на примере Foremost или аналога	
	2	Применение специализированного программно средства для восстановления удаленных файлов	
	3	Применение программ для безвозвратного удаления данных	
	4	Применение программ для шифрования данных на съемных носителях	
Тема 2.6. Аппаратные средства идентификации и	**Содержание**		**4**
	1	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2

аутентификации пользователей		**Домашнее задание:** чтение и анализ литературы [1] стр. 66-72	
	2	Устройства Touch Memory	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**		**12**
	1	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Использование сетевых снифферов в качестве СОВ	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Аппаратный компонент СОВ	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Программный компонент СОВ	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	Практические занятия		**2**
	1	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	
Раздел 3. Защита информации в локальных сетях			
Тема 3.1. Основы построения защищенных сетей	**Содержание**		**8**
	1	Сети, работающие по технологии коммутации пакетов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Стек протоколов TCP/IP. Особенности маршрутизации.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Штатные средства защиты информации стека протоколов TCP/IP.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
Тема 3.2. Средства организации VPN	**Содержание**		**12**
	1	Виртуальная частная сеть. Функции, назначение, принцип построения	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Криптографические и некриптографические средства организации VPN	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	

	3	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	Практические занятия		**2**
	1	Развертывание VPN	
Раздел 4. Защита информации в сетях общего доступа			
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	**Содержание**		**22**
	1	Проблема защиты отчуждаемых компонентов ПЭВМ.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Методы защиты информации на отчуждаемых носителях. Шифрование.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Безвозвратное удаление данных. Принципы и алгоритмы.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	6	Проблема защиты отчуждаемых компонентов ПЭВМ.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	7	Методы защиты информации на отчуждаемых носителях. Шифрование.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	8	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	9	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	Практические занятия		**4**
	1	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	
	2	Изучение различных способов закрытия "опасных" портов	
Раздел 5. Защита информации в базах данных			

Тема 5.1. Защита информации в базах данных	**Содержание**		**14**
	1	Основные типы угроз. Модель нарушителя	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Средства идентификации и аутентификации. Управление доступом	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Средства контроля целостности информации в базах данных	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Средства аудита и контроля безопасности. Критерии защищенности баз данных	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Применение криптографических средств защиты информации в базах данных	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	Практические занятия		**4**
	1	Изучение механизмов защиты СУБД MS Access	
	2	Изучение штатных средств защиты СУБД MSSQL Server	
Раздел 6. Мониторинг систем защиты			
Тема 6.1. Изучение мер защиты информации в информационных системах	**Содержание**		**4**
	1	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	Практические занятия		**2**
	1	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 6.2. Изучение современных программно-аппаратных комплексов.	**Содержание**		**10**
	1	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Изучение современных систем антивирусной защиты на примере корпоративных решений	2

		KasperskyLab или других аналогов	
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	5	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
Курсовая работа			**30**
Примерная тематика курсовых работ 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах 6. Защита сред виртуализации			
Примерная тематика самостоятельной работы при изучении МДК.02.01 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты **5.** Сравнительный анализ современных программных и программно-аппаратных средств защиты			
Промежуточная аттестация по МДК.02.01			10
Раздел 2 модуля. Применение криптографических средств защиты информации			162
МДК.02.02. Криптографические средства защиты информации			148
Раздел 1. Математические основы защиты информации			
Тема 1.1. Математические основы криптографии	**Содержание**		**24**
	1	Элементы теории множеств. Группы, кольца, поля.	2
		Домашнее задание: чтение и анализ литературы [6] стр. 10-13	
	2	Делимость чисел. Признаки делимости. Простые и составные числа..	2
		Домашнее задание: составить таблицу с примерами программного обеспечения	
	3	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2

		Домашнее задание: чтение и анализ литературы [6] стр. 13-16	
	4	Отношения сравнимости. Свойства сравнений. Модулярная арифметика..	2
		Домашнее задание: составить список современного инструментального программного обеспечения	
	5	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	2
		Домашнее задание: чтение и анализ литературы [6] стр. 16-20	
	6	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида..	2
		Домашнее задание: чтение и анализ литературы [6] стр. 20-25	
	7	Китайская теорема об остатках.	2
		Домашнее задание: конспект [6] стр. 25-27	
	8	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена	2
		Домашнее задание: составление плана конспекта лекции	
	9	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда	2
		Домашнее задание: провести анализ системы контроля версий	
	10	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2
		Домашнее задание: составить план конспекта лекции	
	11	Арифметические операции над большими числами.	2
		Домашнее задание: составление плана конспекта лекции	
	12	Эллиптические кривые и их приложения в криптографии.	2
		Домашнее задание:подготовка к тестированию по теме 1.1.	
	Практические занятия		6
	1	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	
	2	Проверка чисел на простоту	
	3	Решение задач с элементами теории чисел	
	Самостоятельная работа		4
	Подготовить выступление на тему «Проверка чисел на простоту с использованием скриптовых языков программирования»		
	Подготовить выступление на тему «Решение криптографических задач с использованием языков программирования»		
Раздел 2. Классическая криптография			
Тема 2.1. Методы криптографического защиты информации	**Содержание**		**8**
	1	Классификация основных методов криптографической защиты. Методы симметричного шифрования	2

		Домашнее задание: составление плана конспекта лекции	
	2	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2
		Домашнее задание: составить план конспекта лекции	
	3	Методы перестановки. Табличная перестановка, маршрутная перестановка	2
		Домашнее задание: составление плана конспекта лекции	
	4	Гаммирование. Гаммирование с конечной и бесконечной гаммами	2
		Домашнее задание:подготовка к тестированию по теме 2.1.	
	Практические занятия		6
	4	Применение классических шифров замены	
	5	Применение классических шифров перестановки	
	6	Применение метода гаммирования	
	Самостоятельная работа		2
	Подготовить выступление на тему «Реализация методов криптографического защиты информации с помощью языков программирования»		
Тема 2.2. Криптоанализ	**Содержание**		**6**
	1	Основные методы криптоанализа. Криптографические атаки	2
		Домашнее задание: чтение и анализ литературы [6] стр. 64-66	
	2	Криптогафическая стойкость. Абсолютно стойкие криптосистемы.	2
		Домашнее задание: составить план конспекта лекции	
	3	Перспективные направления криптоанализа, квантовый криптоанализ.	2
		Домашнее задание: чтение и анализ литературы [6] стр. 66-72	
	Практические занятия		10
	7	Криптоанализ шифра простой замены методом анализа частотности символов	
	8	Криптоанализ классических шифров методом полного перебора ключей	
	9	Криптоанализ шифра Вижинера	
Промежуточная аттестация по МДК.02.02			**2**
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание**		**4**
	1	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	2
		Домашнее задание: чтение и анализ литературы [6] стр. 75-79	
	2	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	2
		Домашнее задание: чтение и анализ литературы [6] стр. 75-79	
	Практические занятия		2
	10	Применение методов генерации ПСЧ	
	Самостоятельная работа		2

	Подготовить выступление на тему «Применение методов генерации ПСЧ с использованием скриптовых языков программирования»		
Раздел 3. Современная криптография			
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание**		**6**
	1	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.	2
		Домашнее задание: чтение и анализ литературы [6] стр. 86-91	
	2	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	4
		Домашнее задание: чтение и анализ литературы [6] стр. 91-106	
	Практические занятия		
	11	Кодирование информации	
	12	Программная реализация классических шифров на языке Python	
	13	Изучение реализации классических шифров замены и перестановки на языке Python	
			2
Тема 3.2. Симметричные системы шифрования	**Содержание**		**4**
	1	Общие сведения. Структурная схема симметричных криптографических систем. Симметричные алгоритмы DES, AES, **ГОСТ 28147-89, RC4**	2
		Домашнее задание: чтение и анализ литературы [5] стр. 6-21	
	2	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.	2
		Домашнее задание: чтение и анализ литературы [5] стр. 21-26	
	Практические занятия		4
	14	Программная реализация современных симметричных шифров на языке Python	
Тема 3.3. Асимметричные системы шифрования	**Содержание**		**4**
	1	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	2
		Домашнее задание: Чтение и анализ литературы [5] стр. 111-117	
	2	Элементы теории чисел в криптографии с открытым ключом	4
		Домашнее задание: Чтение и анализ литературы [5] стр. 117-122	
	Практические занятия		**8**
	15-16	Применение различных асимметричных алгоритмов	
	17-18	Изучение программной реализации асимметричного алгоритма RSA	
			2

Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание**		**4**
	1	Аутентификация данных. Общие понятия. ЭП. MAC	4
		Домашнее задание: Чтение и анализ литературы [2] стр. 3-11	
	2	Однонаправленные хеш-функции. Алгоритмы цифровой подписи.	4
		Домашнее задание: Чтение и анализ литературы [2] стр. 11-27	
	Практические занятия.		6
	19	Применение функций хеширования, анализ особенностей хешей	
	20	Применение криптографических атак на хеш-функции	
	21	Изучение программно-аппаратных средств, реализующих основные функции ЭП	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание**		**4**
	1	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации.	**4**
		Домашнее задание: чтение и анализ литературы [1] стр. 344-347	
	2	Взаимная аутентификация. Односторонняя аутентификация.	**2**
		Домашнее задание: чтение и анализ литературы [1] стр. 348-351	
	Практические занятия		6
	22	Применение протокола Диффи-Хеллмана для обмена ключами шифрования	
	23	Изучение принципов работы протоколов аутентификации	
	24	Изучение работы протокола Kerberos	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание**		**4**
	1	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	2
		Домашнее задание: чтение и анализ литературы [1] стр. 352-362	
	2	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	4
		Домашнее задание: чтение и анализ литературы [1] стр. 362-367	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание**		**4**
	1	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	**2**
		Домашнее задание: чтение и анализ литературы [7] стр. 362-367	
	2	Применение криптографических протоколов для обеспечения безопасности электронной коммерции	**2**
		Домашнее задание: чтение и анализ литературы [8] стр. 362-367	
	Практические занятия		**4**
	25	Применение аутентификации по одноразовым паролям.	

	26	Реализация алгоритмов создания одноразовых паролей на языке Python	
	Самостоятельная работа		**2**
	Изучение методов реализации и распространения одноразовых паролей		
Тема 3.8. Компьютерная стеганография	**Содержание**		**4**
	1	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав	**2**
		Домашнее задание: чтение и анализ литературы [6] стр. 32-37	
	2	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	**4**
		Домашнее задание: чтение и анализ литературы [6] стр. 62-67	
	Практические занятия		**8**
	27-28	Работа с Kali Linux	
	29-30	Реализация простейших стеганографических алгоритмов	
Учебная практика(по профилю специальности) **Виды работ**			
1 Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. 2 Ознакомление с гипервизором VMWare ESXI. Создание групп портов, пользователей, снапшотов. 3 Ознакомление, установка, базовая настройка Cisco FirePower и Pfsense 4 Ознакомление с маршрутизатором Mikrotik RouterOS. Импортирование, базовая настройка. 5 Создание базовой инфраструктуры сети, построение маршрутов в Mikrotik RouterOS. 6 Настройка DNS 7 Настройка DHCP 8 Настройка правил разграничения трафика файервола. 9 Развертывание Active Directory.Создание пользователей 10 Поднятие центра сертификации. Выпуск сертификата 11 Настройка активной аутентификации 12 Проверка работы правил фаейрвола 13 Проверка работы активной аутентификации 14 Оформление отчета. Участие в зачет-конференции по учебной практике 15 Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. 16 Ознакомление с гипервизором VMWare ESXI. Создание групп портов, пользователей, снапшотов. 17 Ознакомление, установка, базовая настройка NGFW и Pfsense 18 Ознакомление с маршрутизатором Mikrotik RouterOS. Импортирование, базовая настройка.			**108**
Производственная практика(по профилю специальности)			

Виды работ	
1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения 3. Настройка программного обеспечения с соблюдением требований по защите информации 4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 6. Настройка встроенных средств защиты информации программного обеспечения 7. Проверка функционирования встроенных средств защиты информации программного обеспечения 8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения 9. Обслуживание средств защиты информации в компьютерных системах и сетях 10. Обслуживание систем защиты информации в автоматизированных системах 11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем 12. Проверка работоспособности системы защиты информации автоматизированной системы 13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 14. Контроль стабильности характеристик системы защиты информации автоматизированной системы 15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	**180**
Промежуточная аттестация (экзамен (квалификационный))	**4**
Всего:	**?**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лаборатории корпоративной защиты от внутренних угроз информационной безопасности или кибербезопасности.

Оборудование лаборатории:
- Стол учительский -1 шт.
- Стул учительский - 1 шт.
- Кресло 16 шт.
- Стул -16 шт.
- Стол компьютерный -16 шт.
- Доска маркерная -1 шт.
- Плакат 5 шт.
- Стенд 1 шт.

Технические средства обучения:
- персональные компьютеры (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i5, оперативная память DDR4 объемом не менее 32 Гб; HD 1000 Gb SDD 500ГБ, видеокарта, БП 650 Ватт), объединенные в учебную локально- вычислительную сеть с выходом в сеть Интернет, по количеству обучающихся с лицензионным программным обеспечением: ОС Windows 10, ОС Astra Linux/RedOS;
- DLP система InfoWatch;
- монитор с возможностью поворота экрана не менее 90 градусов, не менее 23,8 дюйма, HDMI, USB;
- криптошлюз ПАК ViPNet Coordinator HW100 и учебный комплект VipNet ;
- коммутатор L2 уровень, 16 портов Ethernet стандарта 1000BASE-T;
- маршрутизатор 4 порта Ethernet стандарта 1000BASE-T;
- АПМДЗ Соболь PCI-E.
- Проектор BenQ – 1 шт.

3.2. Информационное обеспечение обучения

Основные источники:

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.
2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.
5. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с
6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с.

7. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Дополнительные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711- 1. — Текст : электронный // ЭБС Юрайт [сайт].

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711- 1. — Текст :электронный // ЭБС Юрайт [сайт]

3 Руководство администратора Криптон-замок

4. Руководство администратора ППКОП «Астра»

5. Руководство администратора КТМ-256

6. Учебное пособие Структурированная кабельная система NIKOMAX»

Интернет ресурсы:

1. 1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г

1.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

44. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

46. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

51. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ПО РАЗДЕЛАМ)

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
Раздел модуля 1. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		
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.	Оценка «**отлично**» - установлены, настроены, испытаны и сконфигурированы программные и программно-аппаратные (в том числе криптографических) средств защиты информации в оборудовании ИТКС; Оценка «**хорошо**» - установлены, настроены, испытаны программные и программно-аппаратные (в том числе криптографических) средств защиты информации в оборудовании ИТКС; Оценка «**удовлетворительно**» - установлены, настроены программные и программно-аппаратные (в том числе криптографических) средств защиты информации в оборудовании ИТКС;	Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 2.2 Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.	Оценка «**отлично**» - Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. Оценка «**хорошо**» - Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. Оценка «**удовлетворительно**» - Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств	Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью

	защиты информации в информационно – телекоммуникационных системах и сетях.	обучающегося в процессе практики
Раздел модуля 2. Методы криптографической защиты информации		
ПК 2.3 Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	Оценка «**отлично**» - осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями. Оценка «**хорошо**» - осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями. Оценка «**удовлетворительно**» - осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов

		выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Приложение 1
Обязательное

КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ

Личностные результаты	**Содержание урока (тема, тип урока, воспитательные задачи)**	**Способ организации деятельности**	**Продукт деятельности**	**Оценка процесса формирования ЛР**
ЛР 15 Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем ЛР 17 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	Тема: «Проблемы информационной безопасности» (4 ч.) Тип урока: комплексного применения знаний и способов деятельности – деловая игра Воспитательная задача: - закрепление и углубление имеющихся навыков и умений; - развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ	Викторина по информационной безопасности и информационным технологиям с использование электронных средств и проектов. Состоит из 2 частей, теоретическая игра Quiz и защита проектов по ИБ	День специалиста ИТ Выступление и проекты по ИБ студентов, а так же комплексное закрепление и применение знаний.	- эмоциональное отношение к своей будущей профессии - умение работать и выполнять требования трудовой дисциплины
ЛР 17 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием	Тема 1 марта Урок-турнир «День создания биометрического паспорта»(6 ч.) Тип урока: проверки и оценки знаний и способов деятельности	Соревновательное состязание, в ходе которого участники за отведенное время подключают и настраивают биометрические средства	Биометрический паспорт	- эмоциональное отношение к своей будущей профессии - умение работать и выполнять требования трудовой дисциплины

программных и программно-аппаратных, в том числе криптографических средств защиты ЛР 16 Самостоятельно осуществляющий эксплуатацию информационно-телекоммуникационных систем и сетей	- исследовательская лабораторная работа Воспитательная задача: - закрепление и углубление имеющихся навыков и умений; - развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ	аутентификации.		