

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Агабекян Раиса Левоновна

Должность: ректор

Дата подписания: 29.05.2024 18:15:13

Уникальный программный ключ:

4237c7c5b9b9e111bbaf1f4fcda9201d015c4dbaa123ff774747307b9b9fbcbe

**Негосударственное аккредитованное некоммерческое частное образовательное
учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»**

(г. Краснодар)

Академический колледж

УТВЕРЖДАЮ

Проректор по учебной работе,

доцент Н.И. Севрюгина

08 апреля 2024 г.

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

Рабочая программа профессионального модуля

Для студентов специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

технический профиль

квалификация выпускника - Техник по защите информации

Краснодар, 2024

Рассмотрено
на заседании предметно цикловой комиссии
Протокол № 9 от 05 апреля 2024 г.
Председатель ПЦК Купенко А.А.
Зав отделением Борей Т.В.

Принято
педагогическим советом
Академического колледжа
Протокол № 9
от 05 апреля 2024 г.

Рабочая программа разработана на основе основной профессиональной образовательной программы среднего профессионального образования программы подготовки специалистов среднего звена, специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, Федерального закона Российской Федерации от 29 декабря 2012 г. № 273-ФЗ Об образовании в Российской Федерации (редакция от 25.12.2018 г.) и требований ФГОС среднего профессионального образования (приказ от 09.12.2016г. № 1553 Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Зарегистрировано в Минюсте России 26 декабря 2016 г. N 44938) технического профиля профессионального образования.

Содержание программы реализуется в процессе освоения студентами основной профессиональной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем технического профиля (на базе основного общего образования) в соответствии с требованиями ФГОС СПО на 3-4 курсе (ах) в 5-8 семестре (ах).

Рецензенты:

Ким Т. И./ Заместитель директора по учебно-методической работе ЧУ ПОО КТУИС г. Краснодар

Директор ООО «НТП» г. Краснодар, Поташкова Н.И.

Генеральный директор АО «Опытное конструкторское бюро «Икар» г. Краснодар,
А.Н. Качковский

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. 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:

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.

1.1.2. Общие компетенции

Код	Наименование видов деятельности и профессиональных 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 поддержания необходимого уровня физической подготовленности.

ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных

	<p>системах, компьютерных сетях, базах данных;</p> <ul style="list-style-type: none"> – 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 486 час, из них

на освоение МДК – 324 часов, в том числе

на промежуточную аттестацию по МДК – 10 часов,

на практики – 175 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа ⁸
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
лабораторных и практических занятий	курсовая работа (проект), часов							
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации	224	174	48	30	50	–	–
ПК 2.4 ОК 1-ОК 10	Раздел 2 модуля. Применение криптографических средств защиты информации	165	140	56	–	25	–	–
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	100					100	–
	Промежуточная аттестация⁹	10	10	–	–	–	–	–
	Экзамен по профессиональному модулю ¹⁰	-	-	–	–	–	–	–
	Всего:	499	324	104	30	75	100	–

⁸Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

⁹ Выбор формы промежуточной аттестации в основных образовательных программах определяется образовательной организацией самостоятельно.

¹⁰ Часы на экзамен по профессиональному модулю выделяются за счет вариативной части.

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		230
МДК.02.01. Программные и программно-аппаратные средства защиты информации		180
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание Предмет и задачи программно-аппаратной защиты информации Основные понятия программно-аппаратной защиты информации Классификация методов и средств программно-аппаратной защиты информации	6
Тема 1.2. Стандарты безопасности	Содержание Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты) Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Тематика практических занятий и лабораторных работ Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов. Обзор стандартов. Работа с содержанием стандартов	4
Тема 1.3. Защищенная	Содержание	4

автоматизированная система	Автоматизация процесса обработки информации	
	Понятие автоматизированной системы.	
	Особенности автоматизированных систем в защищенном исполнении.	
	Основные виды АС в защищенном исполнении.	
	Методы создания безопасных систем	
	Методология проектирования гарантированно защищенных КС	
	Дискреционные модели	
	Мандатные модели	
	Тематика практических занятий и лабораторных работ	6
	Учет, обработка, хранение и передача информации в АИС	
	Ограничение доступа на вход в систему.	
	Идентификация и аутентификация пользователей	
	Разграничение доступа.	
	Регистрация событий (аудит).	
Контроль целостности данных		
Уничтожение остаточной информации.		
Управление политикой безопасности. Шаблоны безопасности		
Криптографическая защита. Обзор программ шифрования данных		
Управление политикой безопасности. Шаблоны безопасности		
Тема 1.4.	Содержание	4
Дестабилизирующее воздействие на объекты защиты	Источники дестабилизирующего воздействия на объекты защиты	
	Способы воздействия на информацию	
	Причины и условия дестабилизирующего воздействия на информацию	
	Тематика практических занятий и лабораторных работ	4
	Распределение каналов в соответствии с источниками воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной защиты информации от	Содержание	6
	Понятие несанкционированного доступа к информации	
	Основные подходы к защите информации от НСД	

несанкционированного доступа	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	4
	Доступ к данным со стороны процесса	
	Особенности защиты данных от изменения. Шифрование.	
	Тематика практических занятий и лабораторных работ	
	Организация доступа к файлам	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных автоматизированных систем	Содержание	6
	Работа автономной АС в защищенном режиме	
	Алгоритм загрузки ОС. Штатные средства замыкания среды	
	Расширение BIOS как средство замыкания программной среды	
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	
Тема 2.2. Защита программ от изучения	Содержание	6
	Изучение и обратное проектирование ПО	
	Способы изучения ПО: статическое и динамическое изучение	
	Задачи защиты от изучения и способы их решения	
	Защита от отладки.	
	Защита от дизассемблирования	
	Защита от трассировки по прерываниям.	
Тема 2.3. Вредоносное программное обеспечение	Содержание	4
	Вредоносное программное обеспечение как особый вид разрушающих воздействий	
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	
	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие	

	информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	
	Бот-неты. Принцип функционирования. Методы обнаружения	
	Классификация антивирусных средств. Сигнатурный и эвристический анализ	
	Защита от вирусов в "ручном режиме"	
	Основные концепции построения систем антивирусной защиты на предприятии	
	Тематика практических занятий и лабораторных работ	2
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	
Промежуточная аттестация по МДК.02.01		2
Тема 2.4. Защита программ и данных от несанкционированного копирования	Содержание	4
	Несанкционированное копирование программ как тип НСД	
	Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.	
	Привязка ПО к аппаратному окружению и носителям.	
	Защитные механизмы в современном программном обеспечении на примере MS Office	
	Тематика практических занятий и лабораторных работ	2
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	
Тема 2.5. Защита информации на машинных носителях	Содержание	6
	Проблема защиты отчуждаемых компонентов ПЭВМ.	
	Методы защиты информации на отчуждаемых носителях. Шифрование.	
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	
	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	
	Безвозвратное удаление данных. Принципы и алгоритмы.	
	Тематика практических занятий и лабораторных работ	8

	Применение средства восстановления остаточной информации на примере Foremost или аналога	
	Применение специализированного программно средства для восстановления удаленных файлов	
	Применение программ для безвозвратного удаления данных	
	Применение программ для шифрования данных на съемных носителях	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	Содержание	4
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	
	Устройства Touch Memory	
Тема 2.7. Системы обнаружения атак и вторжений	Содержание	4
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	
	Использование сетевых снифферов в качестве СОВ	
	Аппаратный компонент СОВ	
	Программный компонент СОВ	
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	Тематика практических занятий и лабораторных работ	2
Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений		
Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей	Содержание	4
	Сети, работающие по технологии коммутации пакетов	
	Стек протоколов TCP/IP. Особенности маршрутизации.	
	Штатные средства защиты информации стека протоколов TCP/IP.	
	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
Тема 3.2. Средства организации VPN	Содержание	4
	Виртуальная частная сеть. Функции, назначение, принцип построения	
	Криптографические и некриптографические средства организации VPN	
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	

	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Тематика практических занятий и лабораторных работ	2
	Развертывание VPN	
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Содержание	8
	Методы защиты информации при работе в сетях общего доступа.	
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности	
	Основные типы firewall. Симметричные и несимметричные firewall.	
	Уровень 1. Пакетные фильтры	
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	
	Уровень 3. Проху-сервера прикладного уровня	
	Однохостовые и мультихостовые firewall.	
	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	
	Требования по сертификации межсетевых экранов	
	Тематика практических занятий и лабораторных работ	4
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	
Изучение различных способов закрытия "опасных" портов		
Раздел 5. Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных	Содержание	6
	Основные типы угроз. Модель нарушителя	
	Средства идентификации и аутентификации. Управление доступом	
	Средства контроля целостности информации в базах данных	
	Средства аудита и контроля безопасности. Критерии защищенности баз данных	
	Применение криптографических средств защиты информации в базах данных	
	Тематика практических занятий и лабораторных работ	4
Изучение механизмов защиты СУБД MS Access		

	Изучение штатных средств защиты СУБД MSSQL Server	
Промежуточная аттестация по МДК.02.01		2
Раздел 6. Мониторинг систем защиты		
Тема 6.1. Мониторинг систем защиты	Содержание	6
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	
	Классификация отслеживаемых событий. Особенности построения систем мониторинга	
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	
	Классификация сетевых мониторов	
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	Тематика практических занятий и лабораторных работ	2
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	
	Проведение аудита ЛВС сетевым сканером	
Тема 6.2. Изучение мер защиты информации в информационных системах	Содержание	2
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	
	Тематика практических занятий и лабораторных работ	2
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 6.3. Изучение современных программно-аппаратных комплексов.	Тематика практических занятий и лабораторных работ	8
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других	

	аналогов	
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	
Курсовая работа		30
Примерная тематика курсовых работ		
<ol style="list-style-type: none"> 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		
<ol style="list-style-type: none"> 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		2
Примерные виды самостоятельных работ при изучении раздела 1 модуля		
<p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.</p>		

Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.		
Учебная практика по разделу 1 модуля		50
Виды работ:		
<ul style="list-style-type: none"> – Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах – Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности – Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности – Составление документации по учету, обработке, хранению и передаче конфиденциальной информации – Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации – Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. – Устранение замечаний по результатам проверки – Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. – Применение математических методов для оценки качества и выбора наилучшего программного средства 		
Раздел 2 модуля. Применение криптографических средств защиты информации		169
МДК.02.02. Криптографические средства защиты информации		144
Введение	Содержание	2
	Предмет и задачи криптографии. История криптографии. Основные термины	
Раздел 1. Математические основы защиты информации		
Тема 1.1. Математические основы криптографии	Содержание	24
	Элементы теории множеств. Группы, кольца, поля.	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм	

	быстрого возведения в степень по модулю.	
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	Китайская теорема об остатках.	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	Арифметические операции над большими числами.	
	Эллиптические кривые и их приложения в криптографии.	
	Тематика практических занятий и лабораторных работ	6
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	
	Проверка чисел на простоту	
	Решение задач с элементами теории чисел.	
Раздел 2. Классическая криптография		
Тема 2.1. Методы криптографического защиты информации	Содержание	8
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	
	Методы перестановки. Табличная перестановка, маршрутная перестановка	
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	Тематика практических занятий и лабораторных работ	6
	Применение классических шифров замены	
	Применение классических шифров перестановки	
	Применение метода гаммирования	
Тема 2.2. Криптоанализ	Содержание	6
	Основные методы криптоанализа. Криптографические атаки.	
	Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхoffsа	
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Тематика практических занятий и лабораторных работ	10

	Криптоанализ шифра простой замены методом анализа частотности символов	
	Криптоанализ классических шифров методом полного перебора ключей	
	Криптоанализ шифра Вижинера	
Промежуточная аттестация по МДК.02.02		2
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	Содержание учебного материала	4
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Тематика практических занятий и лабораторных работ	2
	Применение методов генерации ПСЧ	
Раздел 3. Современная криптография		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Содержание учебного материала	6
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	
	Тематика практических занятий и лабораторных работ	8
	Кодирование информации	
	Программная реализация классических шифров	
	Изучение реализации классических шифров замены и перестановки в программе СгупTool или аналоге.	
Тема 3.2. Симметричные системы шифрования	Содержание учебного материала	4
	Общие сведения. Структурная схема симметричных криптографических систем	
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	
	Тематика практических занятий и лабораторных работ	4
	Изучение программной реализации современных симметричных шифров	

Тема 3.3. Асимметричные системы шифрования	Содержание учебного материала	4
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	
	Элементы теории чисел в криптографии с открытым ключом.	
	Тематика практических занятий и лабораторных работ	4
	Применение различных асимметричных алгоритмов. Изучение программной реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	Содержание учебного материала	4
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Тематика практических занятий и лабораторных работ	8
	Применение различных функций хеширования, анализ особенностей хешей Применение криптографических атак на хеш-функции.	
	Изучение программно-аппаратных средств, реализующих основные функции ЭП	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	Содержание учебного материала	4
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	
	Тематика практических занятий и лабораторных работ	6
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 3.6. Криптозащита информации в сетях передачи данных	Содержание учебного материала	4
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 3.7. Защита	Содержание учебного материала	4

информации в электронных платежных системах	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Тематика практических занятий и лабораторных работ	4
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	
Тема 3.8. Компьютерная стеганография	Содержание учебного материала	4
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Тематика практических занятий и лабораторных работ	4
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	Реализация простейших стеганографических алгоритмов	
Примерная тематика самостоятельной работы при изучении МДК.02.02		
<ol style="list-style-type: none"> 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии 		
Промежуточная аттестация по МДК.02.02		2

<p>Примерные виды самостоятельной работы при изучении раздела 2 модуля</p> <p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.</p>	
<p>Учебная практика раздела 2 модуля</p> <p>Виды работ:</p> <ul style="list-style-type: none"> – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи 	25
<p>Производственная практика по ПМ.02</p> <p>Виды работ</p> <ul style="list-style-type: none"> – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. 	100
<p>Экзамен по профессиональному модулю</p>	
<p>Всего:</p>	486

2.4 Оценочные средства и контрольные вопросы

1. Что такое информационная безопасность и почему она важна для автоматизированных систем?
2. Какие основные угрозы информационной безопасности могут возникнуть при эксплуатации автоматизированных систем?
3. Какие программные средства могут использоваться для защиты от вредоносного программного обеспечения?
4. Что такое антивирусное программное обеспечение и как оно может помочь в защите информации в автоматизированных системах?
5. Какие меры безопасности следует принимать при использовании программного обеспечения для защиты информации от несанкционированного доступа?
6. Какие программные инструменты могут быть использованы для шифрования данных в автоматизированных системах?
7. Какие средства аутентификации и авторизации могут быть использованы для обеспечения безопасности доступа к информации в автоматизированных системах?
8. Какие методы контроля доступа к данным могут быть применены с использованием программных средств?
9. Какие программные средства могут помочь в обнаружении и предотвращении утечек конфиденциальной информации?
10. Какие программные инструменты могут помочь в мониторинге сетевой активности для выявления потенциальных угроз безопасности?
11. Какие программные средства могут быть использованы для защиты от атак типа "отказ в обслуживании" (DDoS)?
12. Какие программные инструменты могут помочь в обеспечении целостности данных в автоматизированных системах?
13. Какие средства шифрования файлов и дискового пространства могут быть использованы для обеспечения безопасности данных?
14. Какие программные средства могут быть использованы для контроля за физическим доступом к серверам и другому оборудованию?
15. Какие программные инструменты могут помочь в обнаружении и удалении уязвимостей в программном обеспечении автоматизированных систем?
16. Какие методы резервного копирования данных рекомендуется использовать для обеспечения безопасности информации?
17. Какие программные средства могут помочь в обеспечении безопасности при работе с облачными сервисами?
18. Какие средства аудита безопасности информации могут быть применены для выявления нарушений безопасности в автоматизированных системах?
19. Какие программные инструменты могут помочь в обеспечении конфиденциальности информации при передаче через открытые сети?
20. Какие программные средства могут помочь в обеспечении безопасности при работе с мобильными устройствами для доступа к автоматизированным системам?
21. Какие программные инструменты могут помочь в управлении уязвимостями и исправлении ошибок для обеспечения безопасности информации?
22. Какие методы шифрования сетевого трафика рекомендуется использовать для обеспечения безопасности при передаче данных в автоматизированных системах?
23. Какие программные средства могут помочь в контроле за изменениями в конфигурации информационной системы для обеспечения ее целостности и безопасности?
24. Какие программные инструменты могут помочь в обеспечении безопасности при удаленном доступе к автоматизированным системам через виртуальные частные сети (VPN)?
25. Какие программные средства могут помочь в управлении сертификатами шифрования для обеспечения подлинности пользователей и серверов при передаче данных?
26. Какие программные инструменты могут помочь в обнаружении и реагировании на инциденты безопасности в автоматизированных системах?
27. Какие методы контроля целостности данных рекомендуется использовать при

- эксплуатации информационных систем для обеспечения безопасности?
28. Какие программные средства могут помочь в обеспечении физической безопасности серверных помещений и оборудования информационной системы?
 29. Какие программные инструменты могут помочь в контроле за физическим доступом к серверным помещениям и оборудованию информационной системы?
 30. Какие методы шифрования электронной почты рекомендуется использовать для обеспечения конфиденциальности переписки в автоматизированных системах?
 31. Какие программные средства могут помочь в управлении политиками безопасности для определения правил доступа и контроля параметров безопасности в информационной системе?
 32. Какие программные инструменты могут помочь в контроле доступа к данным для предотвращения несанкционированного доступа к конфиденциальной информации?
 33. Какие программные средства могут помочь в обнаружении и предотвращении утечек данных из автоматизированных систем?
 34. Какие методы шифрования файлов и дискового пространства рекомендуется использовать для обеспечения безопасности данных в автоматизированных системах?
 35. Какие программные инструменты могут помочь в анализе логов и журналов событий для выявления несанкционированных действий?
 36. Какие методы контроля за изменениями в конфигурации серверов и сетевого оборудования рекомендуется использовать для предотвращения уязвимостей в автоматизированных системах?
 37. Какие программные средства могут помочь в аудите доступа к данным для выявления несанкционированного доступа или злоупотреблений пользователями?
 38. Какие методы контроля за физической безопасностью серверных помещений и центров обработки данных рекомендуется использовать для обеспечения непрерывности работы автоматизированных систем?
 39. Какие программные инструменты могут помочь в управлении правами доступа пользователей и групп пользователей для определения различных уровней доступа к данным и функциональности в автоматизированных системах?
 40. Какие программные средства могут помочь в оценке эффективности механизмов защиты информации для постоянного улучшения политики безопасности и процессов эксплуатации?
 41. Какие программные инструменты могут помочь в обнаружении и блокировании сетевых атак, таких как сканирование портов и отказ в обслуживании?
 42. Какие методы шифрования сетевого трафика рекомендуется использовать для обеспечения конфиденциальности данных при передаче через открытые сети?
 43. Какие программные средства могут помочь в обнаружении и удалении вредоносного программного обеспечения на рабочих станциях и серверах?
 44. Какие средства мониторинга безопасности сети могут быть использованы для выявления необычной активности и потенциальных угроз?
 45. Какие программные инструменты могут помочь в обеспечении безопасности при работе с мобильными устройствами, подключенными к корпоративной сети?
 46. Какие методы шифрования дискового пространства рекомендуется использовать для защиты данных на компьютерах и серверах?
 47. Какие программные средства могут помочь в обнаружении и реагировании на утечки конфиденциальной информации из автоматизированных систем?
 48. Какие методы аутентификации могут быть использованы для обеспечения безопасности доступа к информации в автоматизированных системах?
 49. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к системам и данным?
 50. Какие программные средства могут помочь в обеспечении безопасности при работе с удаленными серверами и облачными сервисами?
 51. Какие методы шифрования электронной почты рекомендуется использовать для защиты конфиденциальности переписки в автоматизированных системах?
 52. Какие программные инструменты могут помочь в обеспечении целостности данных при передаче через сеть или хранении на серверах?
 53. Какие средства аудита безопасности информации могут быть применены для контроля за

действиями пользователей в автоматизированных системах?

54. Какие программные средства могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей автоматизированных систем?

55. Какие методы контроля доступа к данным рекомендуется использовать для предотвращения утечек конфиденциальной информации из системы?

56. Какие программные инструменты могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?

57. Какие программные средства могут помочь в обеспечении безопасности при работе с Wi-Fi сетями для предотвращения атак на беспроводные соединения?

58. Какие методы шифрования файлов на уровне операционной системы рекомендуется использовать для защиты данных на компьютерах и серверах?

59. Какие программные инструменты могут помочь в обеспечении безопасности при работе с периферийными устройствами, такими как USB-накопители?

60. Какие методы контроля за физическим доступом к серверам и оборудованию рекомендуется использовать для обеспечения безопасности информационной системы?

2.5 Фонд оценочных средств

1. Какие основные принципы безопасной эксплуатации информационных систем?

2. Какие меры безопасности следует принимать при установке обновлений программного обеспечения на информационной системе?

3. Что такое многофакторная аутентификация и как она может повысить безопасность эксплуатации информационной системы?

4. Какие методы резервного копирования данных рекомендуется использовать для обеспечения надежности эксплуатации информационной системы?

5. Какие средства мониторинга безопасности информационной системы могут помочь выявить необычную активность или атаки?

6. Какие меры следует принимать для защиты информации от утечек при работе с внешними контрагентами через информационные системы?

7. Какие программные инструменты могут помочь в обнаружении и блокировании вредоносных программ в информационной системе?

8. Какие методы шифрования данных рекомендуется использовать для обеспечения конфиденциальности при хранении и передаче информации?

9. Какие меры безопасности следует принимать при работе с удаленными серверами и облачными сервисами?

10. Какие средства аудита информационной безопасности могут помочь в контроле за действиями пользователей в информационной системе?

11. Какие меры предосторожности следует принимать при работе с Wi-Fi сетями для предотвращения атак на беспроводные соединения?

12. Какие методы контроля доступа к данным рекомендуется использовать для предотвращения несанкционированного доступа к информации в информационной системе?

13. Какие программные инструменты могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей информационной системы?

14. Какие методы шифрования электронной почты рекомендуется использовать для защиты конфиденциальности переписки в информационной системе?

15. Какие меры безопасности следует принимать при работе с мобильными устройствами, подключенными к корпоративной сети?

16. Какие программные средства могут помочь в обнаружении и реагировании на утечки конфиденциальной информации из информационной системы?

17. Какие методы шифрования дискового пространства рекомендуется использовать для защиты данных на компьютерах и серверах?

18. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к системам и данным?

19. Какие методы контроля за физическим доступом к серверам и оборудованию рекомендуется использовать для обеспечения безопасности информационной системы?

20. Какие программные средства могут помочь в обеспечении целостности данных при передаче через сеть или хранении на серверах?
21. Какие методы контроля за физическим доступом к серверам и оборудованию рекомендуется использовать для обеспечения безопасности информационной системы?
22. Какие программные инструменты могут помочь в обеспечении безопасности при работе с периферийными устройствами, такими как USB-накопители?
23. Какие средства мониторинга безопасности сети могут быть использованы для выявления необычной активности и потенциальных угроз?
24. Какие программные инструменты могут помочь в обеспечении безопасности при работе с Wi-Fi сетями для предотвращения атак на беспроводные соединения?
25. Какие методы контроля доступа к данным рекомендуется использовать для предотвращения утечек конфиденциальной информации из системы?
26. Какие программные средства могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?
27. Какие программные инструменты могут помочь в обеспечении безопасности при работе с удаленными серверами и облачными сервисами?
28. Какие методы шифрования файлов на уровне операционной системы рекомендуется использовать для защиты данных на компьютерах и серверах?
29. Какие программные инструменты могут помочь в обнаружении и блокировании сетевых атак, таких как сканирование портов и отказ в обслуживании?
30. Какие методы шифрования сетевого трафика рекомендуется использовать для обеспечения конфиденциальности данных при передаче через открытые сети?
31. Какие программные средства могут помочь в обнаружении и удалении вредоносного программного обеспечения на рабочих станциях и серверах?
32. Какие средства аудита безопасности информации могут быть применены для контроля за действиями пользователей в информационных системах?
33. Какие программные средства могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей информационных систем?
34. Какие методы контроля за физическим доступом к серверам и оборудованию рекомендуется использовать для обеспечения безопасности информационных систем?
35. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к информационным системам и данным?
36. Какие методы контроля доступа к данным рекомендуется использовать для предотвращения утечек конфиденциальной информации из информационных систем?
37. Какие программные средства могут помочь в обеспечении целостности данных при передаче через сеть или хранении на серверах?
38. Какие методы шифрования дискового пространства рекомендуется использовать для защиты данных на компьютерах и серверах?
39. Какие программные инструменты могут помочь в обеспечении безопасности при работе с мобильными устройствами, подключенными к корпоративной сети?
40. Какие средства мониторинга безопасности информации могут быть использованы для выявления необычной активности и потенциальных угроз?
41. Какие методы шифрования электронной почты рекомендуется использовать для защиты конфиденциальности переписки в информационных системах?
42. Какие программные инструменты могут помочь в обеспечении безопасности при работе с периферийными устройствами, такими как USB-накопители?
43. Какие методы шифрования файлов на уровне операционной системы рекомендуется использовать для защиты данных на компьютерах и серверах?
44. Какие программные инструменты могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?
45. Какие программные средства могут помочь в обеспечении безопасности при работе с Wi-Fi сетями для предотвращения атак на беспроводные соединения?

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Лаборатория «Программных и программно-аппаратных средств защиты информации» 20 столов, 22 стула, рабочее место преподавателя - 1 шт., персональные компьютеры с выходом в интернет - 20 шт., доска учебная - 1 шт., многофункциональное устройство - 1 шт., мультимедийный проектор - 1 шт., проекционный экран - 1 шт., соответствующее программное обеспечение, соответствующие программные средства

Информационное обеспечение обучения

3.1.1 Основные печатные источники:

1. Емельянова, Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование).

2. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2024. — 352 с. — (Среднее профессиональное образование).

3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с.

3.2.2. Дополнительные печатные источники:

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
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 недеklarированных 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.

3.2.3. Периодические издания:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/>

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

3.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» [http\\:www.ict.edu.ru](http://www.ict.edu.ru)
10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	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 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	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 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	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 2.4. 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	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

компьютерных атак.		
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<ul style="list-style-type: none"> – обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач 	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p> <p>Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам</p> <p>Экзамен квалификационный</p>
ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	<ul style="list-style-type: none"> - демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы; 	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	<ul style="list-style-type: none"> - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных) 	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке	<ul style="list-style-type: none"> - грамотность устной и письменной речи, - ясность формулирования и изложения мыслей 	

с учетом особенностей социального и культурного контекста.		
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, 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	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

