Министерство образования, науки и молодежной политики
Краснодарского края
Государственное бюджетное профессиональное образовательное учреждение
Краснодарского края «Пашковский сельскохозяйственный колледж»

Рассмотрена на заседании методического объединения информационных технологий

Протокол № 1
от «28» сент. 2022г.
Ж.Я. Бунчарева

Рассмотрена на заседании педагогического совета
Протокол № 2
от «26» 10 2022г.

СОГЛАСОВАНО
Зам. директора по учебной работе
_____
«26» 10 2022г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

По специальности:

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Краснодар, 2022

Входит в структуру основной образовательной программы, предназначена для ее реализации в соответствии с требованиями ФГОС среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Приказ Минобрнауки России от 09.12.2016.г. №1553 (ред. 17.12.2020 г.), зарегистрировано в Минюсте России 26.121.2016 г., № 44938.

Организация разработчик: ГБПОУ КК ПСХК

Разработчик:

Глухова С.В., преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшей квалификационной категории, физик, преподаватель, преподавание информатики в общеобразовательных учреждениях

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА 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 поддержание 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	− 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. − *определение правил и процедур управления системой защиты информации автоматизированной системы;* − *определение правил и процедур выявления инцидента* − *определение правил и процедур реагирования на инцидент;* − *определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации;* − *выбор и обоснование критериев выбора эффективности функционирования защищенных автоматизированных систем;* − *проведение экспертизы состояния защищенности информации автоматизированных систем;* − *проведение предварительных испытаний системы защиты информации автоматизированной системы;* − *уточнение модели угроз безопасности информации автоматизированной системы;* − *проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы.*
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; – *применять нормативные документы по противодействию технической разведке;* – *применять нормативные документы для оценки уязвимости;* – *определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы;* – *реализовывать правила разграничения доступа персонала к объектам доступа;* – *настраивать параметры программного обеспечения системы защиты информации автоматизированной системы;* – *классифицировать каналы утечки информации;* – *реализовывать многоуровневую политику разграничения доступа средствами программно-аппаратного комплекса «Страж NT»;* – *реализовывать защитные механизмы в условно-бесплатных и свободно-распространяемого ПО;* – *устранять известные уязвимости автоматизированной системы, приводящих к возникновению угроз безопасности информации;* – *разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированной системы;* – *обеспечивать безопасность рабочих станций и серверов;* – *применять режимы работы блочных шифров, схемы кратного шифрования;*

	− *проводить криптоанализ алгоритмов с открытым ключом;* − *подбирать оборудование для реализации проекта беспроводной сети предприятия.*
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. − *доктрину информационной безопасности Российской Федерации, № Пр-18954 от 9 сентября 2000г.;* − *положение о методах и способах защиты информации в информационных системах персональных данных (Утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58);* − *руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;* − *основные методы снижения затрат на защиту информации в автоматизированных системах;* − *сущностные проявления угрозы;* − *определение причин и условий дестабилизирующего воздействия на информацию;* − *методику выявления способов воздействия на информацию;* − *защиту носителей информации* − *выбор надежного оборудования;* − *порядок создания автоматизированных систем в защищенном исполнении. Общие положения. ГОСТ Р-2014 Защита информации;* − *особенности построения защищенных автоматизированных систем на основе существующих компонентов;* − *уровни контроля на отсутствие недекларированных возможностей (НДВ) в ПО средств защиты информации;* − *средства ликвидации последствий от вредоносного ПО;* − *ответственность за создание, использование и распространение вредоносного ПО;*

	– построение системы антивирусной защиты серверов и рабочих станций; *– системы обнаружения и предотвращения вторжений (IDS, IPS);* *– разработка стратегического плана построения системы защиты;* *– разработка методов реагирования в случае инцидентов и восстановление;* *– классификация методов защиты информации от несанкционированного копирования;* *– альтернативные способы уничтожения данных* *– бесконтактные смарт-карты и usb-ключи;* *– направления совершенствования СОВ;* *– безопасность сетевых устройств OSI;* *– подготовка и технологии проведения и создания карты покрытия;* *– реализация технологий брандмауэра;* *– линейка оборудования для беспроводных сетей;* *– особенности обеспечения безопасности в беспроводных локальных сетях;* *– сервисы безопасности VPN;* *– классификация VPN по рабочему уровню модели OSI;* *– классификация VPN по архитектуре технического решения;* *– VPN-решения для построения защищенных корпоративных сетей;* *– технические и экономические преимущества внедрения технологий VPN в корпоративные сети;* *– технические и экономические преимущества внедрения технологий VPN в корпоративные сети;* *– обзор современных межсетевых экранов;* *– проблемы в сфере сертификации межсетевых экранов;* *– применение механизмов и служб защиты;* *– основные этапы создания СМИБ;* *– система централизованного управления событиями информационной безопасности;* *– система для децентрализованного управления безопасностью, событиями и информацией;* *– система выявления угроз в режиме онлайн;* *– меры защиты информации в государственных информационных системах;* *– содержание мер защиты информации в информационной системе;* *– комплексные средства обеспечения защиты рабочих станций и серверов на уровне данных, приложений, сети, ОС и периферийного оборудования;* *– отечественные типовые решения для построения VPN;*

	– *современная антивирусная индустрия: отечественные и зарубежные разработки;* – *правовые основы обеспечения антивирусной защиты информационных систем;* – *организация антивирусной защиты на предприятии;* – *DLP системы: назначение и принципы работы;* – *применение современных программных и аппаратных криптографических средств для организации защищенных компьютерных систем;* – *оценка защищенности систем электронных платежей.*

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 644 часов, в том числе практической подготовки – 232 часа.

Из них

– на освоение МДК.02.01 – 276 часа, в том числе практической подготовки – 122 часа, самостоятельной работы обучающегося – 22 часа, курсовая работа – 30 часов, промежуточной аттестации в форме дифференцированного зачета – 2 часа.

– на освоение МДК.02.02 – 224 часа, в том числе практической подготовки – 110 часов, самостоятельной работы обучающегося – 24 часа.

Промежуточная аттестация в форме экзамена.

Учебной практики – 72 часа, в том числе промежуточной аттестации в форме дифференцированного зачета – 2 часа.

Производственной практики – 72 часа, в том числе промежуточной аттестации в форме дифференцированного зачета – 2 часа.

Промежуточная аттестация по освоению профессионального модуля в форме экзамена.

2. СТРУКТУРА И СОДЕЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Объем профессионального модуля и виды учебной работы

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	**Объем профессионального модуля, час.**					
			Обучение по МДК, в час.				Практики	
			всего, часов	в том числе			учебная практика, часов	производственная практика, часов
				лабораторных и практических занятий	курсовая работа (проект), часов	Самостоятельная работа		
ПК 2.1 – ПК 2.6 ОК 1 – ОК 10	МДК 02.01 Программные и программно-аппаратные средства защиты информации	**276**	276	122	30	22	–	–
ПК 2.4 ОК 1 – ОК 10	МДК 02.02 Криптографические средства защиты информации	**224**	224	110	-	24	-	-
	УП.02 Учебная практика	**72**					72	–
	ПП.02 Производственная практика	**72**						72
	Промежуточная аттестация в форме экзамена по ПМ.02		–	–	–	–	–	–
	Всего:	**644**	**500**	**232**	**30**	**46**	**72**	**72**

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся		Объем часов	Уровень освоения
МДК.02.01. Программные и программно-аппаратные средства защиты информации			**276**	
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации			**74**	
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание учебного материала**		6	1,2
	1	Предмет и задачи программно-аппаратной защиты информации		
	2	Основные понятия программно-аппаратной защиты информации		
	3	Классификация методов и средств программно-аппаратной защиты информации		
Тема 1.2. Стандарты безопасности	**Содержание учебного материала**		8	2
	1	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).		
	2	*Доктрина информационной безопасности Российской Федерации, № Пр-18954 от 9 сентября 2000г. Положение о методах и способах защиты информации в информационных системах персональных данных (Утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58).*		
	3	*Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».*		
	4	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.		
	Практические занятия		8	

	1	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.		
	2	*Применение нормативных документов по противодействию технической разведке.*		
	3	Обзор стандартов. Работа с содержанием стандартов		
	4	*Применение нормативных документов для оценки уязвимости.*		
Тема 1.3. Защищенная автоматизированная система	**Содержание учебного материала**		6	2
	1	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем		
	2	*Основные методы снижения затрат на защиту информации в автоматизированных системах.*		
	3	Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели. *Отсутствие применимых средств реализации мандатного механизма разграничения доступа.*		
	Практические занятия		14	
	1	Учет, обработка, хранение и передача информации в АИС.		
	2	*Определение параметров настройки программного обеспечения и системы защиты информации автоматизированной системы.*		
	3	Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа. Регистрация событий (аудит).		
	4	*Реализация правил разграничения доступа персонала к объектам доступа.*		
	5	Контроль целостности данных. Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности.		
	6	*Настройка параметров программного обеспечения системы защиты информации автоматизированной системы.*		
	7	Криптографическая защита. Обзор программ шифрования данных. *Работа с программой шифрования данных kryptelite.*		
Тема 1.4. Дестабилизирующее	**Содержание учебного материала**		6	2
	1	Источники дестабилизирующего воздействия на объекты защиты		

воздействие на объекты защиты	2	*Сущностные проявления угрозы.*		
	3	Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию.		
	Практические занятия		8	
	1	*Определение причин и условий дестабилизирующего воздействия на информацию.*		
	2	*Методика выявления способов воздействия на информацию.*		
	3	Распределение каналов в соответствии с источниками воздействия на информацию		
	4	*Классификация каналов утечки информации.*		
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание учебного материала**		6	2
	1	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД.		
	2	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам		
	3	Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Шифрование.		
	Практические занятия		10	
	1	Организация доступа к файлам.		
	2	*Защита носителей информации.*		
	3	*Выбор надежного оборудования.*		
	4	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		
	5	*Реализация многоуровневой политики разграничения доступа средствами программно-аппаратного комплекса «Страж NT».*		
	Самостоятельная работа		2	
	1	*Средства защиты от несанкционированного доступа.*		
Раздел 2. Защита автономных автоматизированных систем			**86**	
Тема 2.1. Основы защиты автономных	**Содержание учебного материала**		6	2
	1	Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды.		

автоматизированных систем	2	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)		
	3	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.		
	Практические занятия		6	
	1	*Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. ГОСТ Р 51583-2014 Защита информации.*		
	2	*Особенности построения защищенных автоматизированных систем на основе существующих компонентов.*		
	3	*Уровни контроля на отсутствие недекларированных возможностей (НДВ) в ПО средств защиты информации.*		
Тема 2.2. Защита программ от изучения	**Содержание учебного материала**		6	2
	1	Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение.		
	2	Задачи защиты от изучения и способы их решения. Защита от отладки.		
	3	Защита от дизассемблирования. Защита от трассировки по прерываниям.		
	Самостоятельная работа		2	
	1	*Функции прикладного программирования, экспортируемые электронным ключом.*		
Тема 2.3. Вредоносное программное обеспечение	**Содержание учебного материала**		6	2
	1	Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.		
	2	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.		
	3	Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии.		
	Практические занятия		12	
	1	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО.		

	2	*Ответственность за создание, использование и распространение вредоносного ПО.*		
	3	*Построение системы антивирусной защиты серверов и рабочих станций.*		
	4	*Системы обнаружения и предотвращения вторжений (IDS, IPS).*		
	5	*Разработка стратегического плана построения системы защиты.*		
	6	*Разработка методов реагирования в случае инцидентов и восстановление.*		
	Самостоятельная работа		2	
	1	*Средства ликвидации последствий от вредоносного ПО.*		
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание учебного материала**		4	2
	1	Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. *Создание и использование систем защиты от копирования.*		
	2	Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office		
	Практические занятия		6	
	1	Защита информации от несанкционированного копирования с использованием специализированных программных средств		
	2	Защитные механизмы в приложениях (на примере MSWord, MS Excel, MS PowerPoint)		
	3	*Реализация защитных механизмов в приложениях свободно-распространяемого и условно-бесплатного ПО.*		
	Самостоятельная работа		2	
	1	*Классификация методов защиты информации от несанкционированного копирования.*		
Тема 2.5. Защита информации на машинных носителях	**Содержание учебного материала**		6	2
	1	Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование.		
	2	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.		
	3	Безвозвратное удаление данных. Принципы и алгоритмы.		
	Практические занятия		8	

	1	Применение средства восстановления остаточной информации на примере Foremost или аналога.		
	2	Применение специализированного программного средства для восстановления удаленных файлов. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.*		
	3	Применение программ для безвозвратного удаления данных		
	4	Применение программ для шифрования данных на съемных носителях. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.*		
	Самостоятельная работа		2	
	1	*Альтернативные способы уничтожения данных.*		
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание учебного материала**		4	2
	1	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ		
	2	Устройства Touch Memory.*Бесконтактные смарт-карты и usb-ключи.*		
	Самостоятельная работа		2	
	1	*Биометрическая идентификация и аутентификация пользователей.*		
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание учебного материала**		4	2
	1	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ. Программный компонент СОВ.		
	2	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.		
	Практические занятия		6	
	1	Моделирование проведения атаки.		
	2	Изучение инструментальных средств обнаружения вторжений. *Устранение известных уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации.*		
	3	*Анализ методов обнаружения злоупотреблений. Методы, основанные на моделировании поведения злоумышленника.*		
	Самостоятельная работа		2	
	1	*Направления совершенствования СОВ.*		

Раздел 3. Защита информации в локальных сетях			**24**	
Тема 3.1. Основы построения защищенных сетей	**Содержание учебного материала**		4	
	1	Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. *Безопасность сетевых устройств OSI.*		2
	2	Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.		
	Практические занятия		6	
	1	*Подготовка и технологии проведения и создания карты покрытия.*		
	2	*Реализация технологий брандмауэра.*		
	3	*Линейка оборудования для беспроводных сетей.*		
	Самостоятельная работа		2	
	1	*Особенности обеспечения безопасности в беспроводных локальных сетях.*		
Тема 3.2. Средства организации VPN	**Содержание учебного материала**		4	2
	1	Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN.		
	2	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки		
	Практические занятия		6	
	1	Развертывание VPN.		
	2	*Варианты построения виртуальных защищенных каналов типа ЛВС-ЛВС и клиент-ЛВС.*		
	3	*Разработка предложений по совершенствованию системы управления защиты информации автоматизированной системы.*		
	Самостоятельная работа		2	
	1	*Технические и экономические преимущества внедрения технологий VPN в корпоративные сети.*		
Раздел 4. Защита информации в сетях общего доступа			**14**	
Тема 4.1.	**Содержание учебного материала**		8	2

Обеспечение безопасности межсетевого взаимодействия	1	Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.		
	2	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. Proxy-сервера прикладного уровня		
	3	Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций		
	4	Требования по сертификации межсетевых экранов. *Проблемы в сфере сертификации межсетевых экранов.*		
	Практические занятия		4	
	1	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. *Управление рисками.*		
	2	Изучение различных способов закрытия "опасных" портов. *Применение механизмов и служб защиты.*		
	Самостоятельная работа		2	
	1	*Обзор современных межсетевых экранов.*		
Раздел 5. Защита информации в базах данных			**12**	
Тема 5.1. Защита информации в базах данных	**Содержание учебного материала**		6	2
	1	Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом.		
	2	Средства контроля целостности информации в базах данных.		
	3	Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных.		
	Практические занятия		6	
	1	Изучение механизмов защиты СУБД MS Access. *Правила безопасности и доступа.*		
	2	Изучение штатных средств защиты СУБД MSSQL Server. *Протокол SSL.*		
	3	Средства создания резервных копий и восстановления баз данных.		
Раздел 6. Мониторинг систем защиты			**44**	
	Содержание учебного материала		8	2

Тема 6.1. Мониторинг систем защиты	1	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.		
	2	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		
	3	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов.		
	4	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.		
	Практические занятия		8	
	1	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов		
	2	*Анализ программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем.*		
	3	Проведение аудита ЛВС сетевым сканером		
	4	*Определение методов управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе.*		
	Самостоятельная работа		2	
	1	*Основные этапы создания СМИБ.*		
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание учебного материала**		2	2
	1	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.		
	Практические занятия		4	
	1	Выбор мер защиты информации для их реализации в информационной системе. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.*		
	2	Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.*		

Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Практические занятия**		10	
	1	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов. *Обеспечение безопасности рабочих станций и серверов.*		
	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. *Обеспечение безопасности рабочих станций и серверов.*		
	3	Изучение типовых решений для построения VPN на примере VIP Net или других аналогов. *Обеспечение безопасности рабочих станций и серверов.*		
	4	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. *Обеспечение безопасности рабочих станций и серверов.*		
	5	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов. *Обеспечение безопасности рабочих станций и серверов.*		
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. 7. Виброакустические средства современных систем обеспечения информационной безопасности. 8. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 9. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 10. Средства обеспечения информационной безопасности банков данных.				3

11. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 12. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации. 13. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 14. Обеспечение защиты конфиденциальной информации в распределенных системах разграничения доступа. 15. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 16. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 17. Инструментальные средства анализа рисков информационной безопасности. 18. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 19. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности). 20. Анализ методов и средств анализа защищенности беспроводных сетей. 21. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения. 22. Программно-аппаратные средства защиты информационных ресурсов от несанкционированного использования и копирования. 23. Варианты решения антивирусной защиты корпоративной сети. 24. Корпоративная защита от внутренних угроз на базе DLP-системы. 25. Организация защиты информации техническими средствами на предприятии. 26. Организация защиты информации в системах контроля и управления доступом. 27. Организация защиты компьютерной сети предприятия от внешних вторжений. 28. Применение систем контроля и учета действий персонала на предприятии. 29. Применение программных снифферов для анализа сетевого трафика. 30. Организация защиты информации в современных центрах обработки данных.		
Промежуточная аттестация по МДК 02.01 в форме дифференцированного зачета	**2**	
Примерные виды самостоятельных работ при изучении МДК 02.01		

Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.				
МДК.02.02. Криптографические средства защиты информации			**224**	
Введение			**8**	
	Содержание учебного материала		4	1, 2
	1	Предмет и задачи криптографии. История криптографии. Основные термины		
	2	*Оценка надежности криптоалгоритмов. Классификация криптографических методов защиты информации.*		
	Самостоятельная работа		4	
	1	*История развития криптографии*		
	2	*Законодательство в области криптографической защиты информации*		
Раздел 1. Математические основы защиты информации			**38**	
Тема 1.1. Математические основы криптографии	**Содержание учебного материала**		24	2
	1	Элементы теории множеств. Группы, кольца, поля.		
	2	Делимость чисел. Признаки делимости. Простые и составные числа.		
	3	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.		
	4	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.		
	5	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.		
	6	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.		
	7	Китайская теорема об остатках.		
	8	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.		

	9	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.		
	10	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.		
	11	Арифметические операции над большими числами.		
	12	Эллиптические кривые и их приложения в криптографии.		
	Практические занятия		14	
	1	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений		
	2	*Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений*		
	3	Проверка чисел на простоту		
	4	*Проверка чисел на простоту*		
	5	*Алгоритм быстрого возведения в степень по модулю.*		
	6	Решение задач с элементами теории чисел.		
	7	*Решение задач с элементами теории чисел.*		
Раздел 2. Классическая криптография			**50**	
Тема 2.1. Методы криптографической защиты информации	**Содержание учебного материала**		8	2
	1	Классификация основных методов криптографической защиты. Методы симметричного шифрования		
	2	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр		
	3	Методы перестановки. Табличная перестановка, маршрутная перестановка		
	4	Гаммирование. Гаммирование с конечной и бесконечной гаммами		
	Практические занятия		12	
	1	Применение классических шифров замены		
	2	*Применение классических шифров замены*		
	3	Применение классических шифров перестановки		
	4	*Применение классических шифров перестановки*		
	5	Применение метода гаммирования		
	6	*Применение метода гаммирования*		

	Самостоятельная работа		2	
	1	*Программная реализация классических шифров*		
Тема 2.2. Криптоанализ	**Содержание учебного материала**		6	2
	1	Основные методы криптоанализа. Криптографические атаки.		
	2	Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса		
	3	Перспективные направления криптоанализа, квантовый криптоанализ.		
	Практические занятия		10	
	1	Криптоанализ шифра простой замены методом анализа частотности символов		
	2	Криптоанализ шифра простой замены методом анализа частотности символов		
	3	Криптоанализ классических шифров методом полного перебора ключей		
	4	Криптоанализ классических шифров методом полного перебора ключей		
	5	Криптоанализ шифра Вижинера		
	Самостоятельная работа		4	
	1	*Оптимизация методов частотного анализа моноалфавитных шифров.*		
	2	*Составление алгоритма криптоанализа шифра Вижинера.*		
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**		4	2
	1	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии		
	2	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.		
	Практические занятия		4	
	1	*Методы генерации ПСЧ*		
	2	Применение методов генерации ПСЧ		
Раздел 3. Современная криптография			**128**	
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**		10	2
	1	Кодирование информации. Символьное кодирование. Смысловое кодирование.		
	2	Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII		
	3	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств.		

	4	*Изучение современных программных и аппаратных криптографических средств*		
	5	*Применение современных программных и аппаратных криптографических средств для организации защищенных компьютерных систем.*		
	Практические занятия		12	
	1	Кодирование информации		
	2	*Исследование информации в двоичном коде в таблице ASCII*		
	3	Программная реализация классических шифров		
	4	*Программная реализация классических шифров*		
	5	Изучение реализации классических шифров замены в программе CrypTool или аналоге.		
	6	Изучение реализации классических шифров перестановки в программе CrypTool или аналоге.		
	Самостоятельная работа		4	
	1	*Методы механизации шифрования*		
	2	*Цифровое представление различных форм информации*		
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**		4	2
	1	Общие сведения. Структурная схема симметричных криптографических систем		
	2	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		
	Практические занятия		10	
	1	*Применение режимов работы блочных шифров. Схемы краткого шифрования.*		
	2	Изучение программной реализации современных симметричных шифров		
	3	Изучение программной реализации современных симметричных шифров		
	4	*Исследование общей структурной схемы симметричных криптографических систем.*		
	5	*Исследование отечественных алгоритмов Магма и Кузнечик*		
	Самостоятельная работа		2	
	1	*Анализ современных симметричных криптоалгоритмов*		
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**		4	2
	1	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.		
	2	Элементы теории чисел в криптографии с открытым ключом.		
	Практические занятия		6	

	1	Применение различных асимметричных алгоритмов.		
	2	*Проведение криптоанализа алгоритмов с открытым ключом*		
	3	Изучение программной реализации асимметричного алгоритма RSA		
	Самостоятельная работа		2	
	1	*Анализ современных ассиметричных криптоалгоритмов*		
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**		8	2
	1	Аутентификация данных. Общие понятия. ЭП. MAC.		
	2	Однонаправленные хеш-функции. Алгоритмы цифровой подписи		
	3	*Криптозащита информации в сетях передачи данных. Абонентское шифрование.*		
	4	*Пакетное шифрование. Защита центра генерации ключей.*		
	Практические занятия		10	
	1	Применение различных функций хеширования.		
	2	*Применение различных функций хеширования.*		
	3	Анализ особенностей хешей		
	4	Применение криптографических атак на хеш-функции.		
	5	Изучение программно-аппаратных средств, реализующих основные функции ЭП		
	Самостоятельная работа		2	
	1	*Сравнительный анализ функций хеширования*		
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**		6	2
	1	*Алгоритмы обмена ключей и протоколы аутентификации.*		
	2	Алгоритмы распределения ключей с применением симметричных и асимметричных схем		
	3	Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация		
	Практические занятия		12	
	1	Протокол Диффи-Хеллмана для обмена ключами шифрования.		
	2	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.		
	3	*Протоколы аутентификации в Windows*		
	4	*Исследование взаимной аутентификации*		
	5	*Исследование односторонней аутентификации*		
	6	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	2
	1	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр		
	2	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.		
	Практические занятия		4	
	1	*Применение протоколов WPA, WEP для организации безопасного функционирования беспроводной сети.*		
	2	*Подбор оборудования для реализации проекта беспроводной сети предприятия*		
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**		4	2
	1	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер		
	2	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.		
	Практические занятия		8	
	1	Применение аутентификации по одноразовым паролям.		
	2	*Применение аутентификации по одноразовым паролям.*		
	3	Реализация алгоритмов создания одноразовых паролей		
	4	*Применение криптографических протоколов для обеспечения безопасности электронной коммерции.*		
	Самостоятельная работа		2	
	1	*Оценка защищенности систем электронных платежей*		
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**		4	2
	1	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.		
	2	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ		
	Практические занятия		8	
	1	Обзор существующего ПО для встраивания ЦВЗ		
	2	*Сравнительный анализ существующего ПО для встраивания ЦВЗ.*		
	3	Реализация простейших стеганографических алгоритмов		
	4	*Реализация простейших стеганографических алгоритмов*		
	Самостоятельная работа		2	

1	*Перспективные направления криптографии*		
Промежуточная аттестация по МДК 02.02 экзамен			
Примерные виды самостоятельной работы при изучении МДК 02.02 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.			
Учебная практика по ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		**72**	3
1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. 2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности. 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации. 5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации. 6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 7. Устранение замечаний по результатам проверки. 8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. 9. Применение математических методов для оценки качества и выбора наилучшего программного средства. 10. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи. *11. Определение правил и процедур управления системой защиты информации автоматизированной системы.* *12. Определение правил и процедур выявления инцидента и реагирования на него.* ***Дифференцированный зачет***			

Производственная практика по ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	**72**	
1. Анализ принципов построения систем информационной защиты производственных подразделений; 2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы; 3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; 4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении; 5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; 6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики; *7. Определение правил и процедур управления системой защиты информации автоматизированной системы;* *8. Определение правил и процедур выявления инцидента и реагирования на него;* *9. Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации;* *10. Выбор и обоснование критериев выбора эффективности функционирования защищенных автоматизированных систем;* *11. Проведение экспертизы состояния защищенности информации автоматизированных систем;* *12. Проведение предварительных испытаний системы защиты информации автоматизированной системы;* *13. Уточнение модели угроз безопасности информации автоматизированной системы;* *14. Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы.* ***Дифференцированный зачет***		3
Экзамен по ПМ.02		
Всего:	**644**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены следующие условия:

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

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные источники:

1. 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.

2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.

3. 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.

4. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

5. 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.

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

7. 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.

8. 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.

9. 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

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

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

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

25. 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

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

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

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

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

30. 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

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

32. 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

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

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

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» htpp\\: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 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
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; – адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам
ОК 02. Осуществлять поиск, анализ и интерпретацию	– использование различных источников, включая электронные	

информации, необходимой для выполнения задач профессиональной деятельности.	ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	– 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.	– 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 с учетом особенностей социального и культурного контекста.	– грамотность устной и письменной речи, – ясность формулирования и изложения мыслей	
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	– эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной	

процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	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.	