МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
СМОЛЕНСКИЙ КАЗАЧИЙ ИНСТИТУТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И БИЗНЕСА (ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»
(СКИПТБ (ФИЛИАЛ) ФГБОУ ВО «МГУТУ ИМ. К. Г. РАЗУМОВСКОГО (ПКУ)»)

УТВЕРЖДАЮ
Директор СКИПТБ (филиал) ФГБОУ ВО
«МГУТУ им. К.Г. Разумовского (ПКУ)
_____ Н.С. Коржикова
«28» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

профессионального учебного цикла
программы подготовки специалистов среднего звена

по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

уровень подготовки
базовый

Квалификация
Техник по защите информации

форма обучения
очная

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00B895E5D3E87E5E81C0F723DE8AC92877
Владелец: Коржикова Надежда Сергеевна
Действителен: с 06.08.2024 до 30.10.2025

Вязьма 2023

ОДОБРЕНА
предметной (цикловой) комиссией
общепрофессиональных дисциплин,
профессиональных модулей специальности
10.02.05 «Обеспечение информационной
безопасности автоматизированных систем»
Председатель ПЦК

_____А.А. Иванов

Протокол № 10 от «26» июня 2023 г.

СОГЛАСОВАНО

Заместитель директора

_____О.В. Комарова

«26» июня 2023 г.

Составитель (автор):
Преподаватель без
квалификационной категории _____А.И. Долотовский

Рабочая программа рекомендована к утверждению экспертами:
Генеральный директор
ООО «Споит» _____Н.В. Савин
(М.П.)

Специалист по защите
информации ФГКУ комбинат
«Прожектор» Росрезерва» _____Н.В. Готовщикова

Рабочая программа разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности **10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1553, и учебного плана программы подготовки специалистов среднего звена по специальности **10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

СОДЕРЖАНИЕ

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02	4
2	РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	5
3	СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
4	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	23
5	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)	29
6	ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	31

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами **и** соответствующие ему общие компетенции и профессиональные компетенции.

1.1.1. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
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. Перечень общих компетенций

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 обучающийся должен

Иметь практический опыт	- установки, настройки программных средств защиты информации в автоматизированной системе; - тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; - учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности.
уметь	- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; - 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.
знать	- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - 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

Вид учебной работы	Объем часов
Объем программы профессионального модуля	**625**
в том числе:	
теоретическое обучение (уроки, лекции)	146
практические занятия	310
лабораторные занятия	не предусмотрено
семинары	не предусмотрено
контрольные работы	не предусмотрено
курсовой проект/работа	30
консультации	не предусмотрено
самостоятельная работа	126
учебная практика	72
производственная практика	113
Промежуточная аттестация в форме экзамена, зачета с оценкой, экзамена по модулю	13

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов *(макс. учебная нагрузка и практики)*	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов *(если предусмотрена рассредоточенная практика)*
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6	**Раздел 1. МДК 02.01. Программные и программно-аппаратные средства защиты информации**	**235**	**225**	135	30	**10**	-	-	-
	Раздел 2. МДК 02.02. Криптографические средства защиты информации	**205**	**189**	103	-	**8**	-	-	-
	УП.02.01. Учебная практика	**72**	**72**	-	-	-	-	**72**	-
	ПП.02.01. Производственная практика	**113**	-	-	-	-	-	-	**113**
	Экзамен по модулю	-	-	-	-	-	-	-	-
	Всего:	**625**	**486**	**238**	**30**	**18**	-	**72**	**113**

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		
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**357**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации.	**Содержание**	**8**
	Предмет и задачи программно-аппаратной защиты информации	2
	Основные понятия программно-аппаратной защиты информации	2
	Классификация методов и средств программно-аппаратной защиты информации	2
	Тематика практических занятий и лабораторных работ	не предусмотрено
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 1.2. Стандарты безопасности.	**Содержание**	**10**
	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	**4**
	№ 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. Обзор стандартов. Работа с содержанием стандартов.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено

	Самостоятельная работа обучающихся	не предусмотрено
Тема 1.3. Защищенная автоматизированная система	**Содержание**	**20**
	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**
	№ 3. Учет, обработка, хранение и передача информации в АИС.	
	№ 4. Ограничение доступа на вход в систему.	
	№ 5. Идентификация и аутентификация пользователей.	
	№ 6. Разграничение доступа.	
	№ 7. Регистрация событий (аудит).	
	№ 8. Контроль целостности данных.	
	№ 9. Уничтожение остаточной информации.	
	№ 10. Управление политикой безопасности. Шаблоны безопасности.	
	№ 11. Криптографическая защита. Обзор программ шифрования данных.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**8**
	Источники дестабилизирующего воздействия на объекты защиты	
	Способы воздействия на информацию	
	Причины и условия дестабилизирующего воздействия на информацию	
	Тематика практических занятий и лабораторных работ	**2**
	Распределение каналов в соответствии с источниками воздействия на информацию	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 1.5. Принципы программно-аппаратной защиты информации от	**Содержание**	**16**
	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	
	Доступ к данным со стороны процесса	
	Особенности защиты данных от изменения. Шифрование.	
	Тематика практических занятий и лабораторных работ	**4**
	Организация доступа к файлам	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных автоматизированных систем.	**Содержание**	**16**
	Работа автономной АС в защищенном режиме.	
	Алгоритм загрузки ОС. Штатные средства замыкания среды.	
	Расширение BIOS как средство замыкания программной среы.	
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка).	
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	
	Тематика практических занятий и лабораторных работ	не предусмотрено
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 2.2.Защита программ от изучения.	**Содержание**	**16**
	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.	
	Тематика практических занятий и лабораторных работ	не предусмотрено
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено

Тема 2.3. Вредоносное программное обеспечение	**Содержание**	**30**
	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.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Промежуточная аттестация по МДК.02.01		**2**
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**	**14**
	Несанкционированное копирование программ как тип НСД	
	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты 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).	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 2.5. Защита информации на машинных носителях	**Содержание**	**16**
	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.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**8**
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ.	
	Устройства Touch Memory.	
	Тематика практических занятий и лабораторных работ	не предусмотрено
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 2.7. Системы обнаружения атак и вторжений.	**Содержание**	**12**
	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	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено

Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей.	**Содержание**	**10**
	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.	
	Тематика практических занятий и лабораторных работ	не предусмотрено
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.2. Средства организации VPN.	**Содержание**	**10**
	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.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**20**
	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. Proxy-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.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Раздел 5. Защита информации в базах данных.		
Тема 5.1. Защита информации в базах данных.	**Содержание**	**12**
	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	**2**
	Изучение механизмов защиты СУБД MS Access.	
	Изучение штатных средств защиты СУБД MSSQL Server.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Промежуточная аттестация по МДК.02.01.		**2**
Раздел 6. Мониторинг систем защиты.		
Тема 6.1. Мониторинг систем защиты.	**Содержание**	**20**
	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.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	**4**
	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.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Содержание**	не предусмотрено
	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.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Курсовая работа		**30**
Примерная тематика курсовых работ 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)		

4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах 6. Защита сред виртуализации	
Примерная тематика самостоятельной работы при изучении МДК.02.01 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты	**21**
Промежуточная аттестация по МДК.02.01	**2**
Примерные виды самостоятельных работ при изучении раздела 1 модуля 1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 2. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. 3. 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 **Виды работ:** − 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.	**78**
Раздел 2 модуля. Применение криптографических средств защиты информации	
МДК.02.02. Криптографические средства защиты информации	**192**

Введение.	**Содержание**	**2**
	Предмет и задачи криптографии. История криптографии. Основные термины	2
	Тематика практических занятий и лабораторных работ	не предусмотрено
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Раздел 1. Математические основы защиты информации.		
Тема 1.1. Математические основы криптографии	**Содержание**	**36**
	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**
	№ 1. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений.	
	№ 2. Проверка чисел на простоту.	
	№ 3. Решение задач с элементами теории чисел.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Раздел 2. Классическая криптография		
Тема 2.1. Методы	**Содержание**	**14**

криптографического защиты информации	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**
	№ 4. Применение классических шифров замены.	
	№ 5. Применение классических шифров перестановки.	
	№ 6. Применение метода гаммирования.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 2.2. Криптоанализ.	**Содержание**	**8**
	Основные методы криптоанализа. Криптографические атаки.	
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Тематика практических занятий и лабораторных работ	**10**
	№ 7. Криптоанализ шифра простой замены методом анализа частотности символов.	
	№ 8. Криптоанализ классических шифров методом полного перебора ключей.	
	№ 9. Криптоанализ шифра Вижинера.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Промежуточная аттестация по МДК.02.02.		**2**
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание**	**8**
	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**
	№ 10. Применение методов генерации ПСЧ.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено

Раздел 3. Современная криптография.		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание**	**8**
	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**
	№ 11. Кодирование информации.	
	№ 12. Программная реализация классических шифров.	
	№ 13. Изучение реализации классических шифров замены и перестановки в программе CrypTool.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.2. Симметричные системы шифрования	**Содержание**	**8**
	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**
	№ 14. Изучение программной реализации современных симметричных шифров.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.3. Асимметричные системы шифрования	**Содержание**	**8**
	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**
	№ 15. Применение различных асимметричных алгоритмов.	
	№ 16. Изучение программной реализации асимметричного алгоритма RSA.	

	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.4. Аутентификация данных. Электронная подпись.	**Содержание**	**8**
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Тематика практических занятий и лабораторных работ	**6**
	№ 17. Применение различных функций хеширования, анализ особенностей хешей.	
	№ 18. Применение криптографических атак на хеш-функции.	
	№ 19. Изучение программно-аппаратных средств, реализующих основные функции ЭП.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание**	**8**
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	
	Тематика практических занятий и лабораторных работ	**4**
	№ 20. Реализация протокола Диффи-Хеллмана для обмена ключами шифрования.	
	№ 21. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание**	**8**
	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.	
	Тематика практических занятий и лабораторных работ	не предусмотрено
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено

	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.7. Защита информации в электронных платежных системах	**Содержание**	**8**
	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	**2**
	№ 22. Применение аутентификации по одноразовым паролям. Реализация алгоритма создания одноразовых паролей.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Тема 3.8. Компьютерная стеганография.	**Содержание**	**8**
	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**
	№ 23. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ.	
	№ 24. Реализация простейших стеганографических алгоритмов.	
	Семинары	не предусмотрено
	Контрольные работы	не предусмотрено
	Самостоятельная работа обучающихся	не предусмотрено
Примерная тематика самостоятельной работы при изучении МДК.02.02 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		**8**

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**
Примерные виды самостоятельной работы при изучении раздела 2 модуля 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 раздела 2 модуля **Виды работ:** – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.	**30**
Производственная практика по ПМ.02 **Виды работ** – 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.	**180**
Экзамен по профессиональному модулю	
Всего:	**625**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к материально-техническому обеспечению

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

- Лаборатория программных и программно-аппаратных средств защиты информации для проведения дисциплин лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Рабочие места обучающихся; Рабочее место преподавателя оснащенное ПЭВМ; Доска интерактивная; Проектор; 10 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет, антивирусные программные комплексы; программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности; программные и программно-аппаратные средства обнаружения вторжений;средства уничтожения остаточной информации в запоминающих устройствах; программные средства выявления уязвимостей в АС и СВТ; программные средства криптографической защиты информации; программные средства защиты среды виртуализации.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации для использования в образовательном процессе должен иметь печатные и/или электронные образовательные и информационные ресурсы.

3.2.1. Печатные издания

Основные печатные источники

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования 2-е издание М.: Издательский центр «Академия», 2016.
2. Партыка Т.Л., Попов И.И. Информационная безопасность : учеб. пособие для студ. учреждений среднего проф. образования. [Электронный ресурс] - М.: ИД «ФОРУМ»: ИНФРА-М, 2018. Режим доступа: http://znanium.com/bookread2.php?book=915902.
3. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. [Электронный ресурс] - М: Форум, 2016. – Режим доступа: http://znanium.com/bookread2.php?book=945331

3.2.2. Дополнительные печатные источники:

1. 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.

2. 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.
3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.
4. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность и защита информации [Электронный ресурс] : Учебник. - М: РИОР, 2013. – Режим доступа: http://znanium.com/
5. Белов Е.Б. и др. Основы информационной безопасности : учеб. пособие для студентов вузов. - М: Горячая линия - Телеком, 2006.
6. Галатенко В.А. Стандарты информационной безопасности. - М: ИНТУИТ.РУ, 2006.
7. Гарнаев А.Ю. Самоучитель VBA. СПб.: БВХ, 2009.
8. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".
9. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования".
10. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
11. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
12. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
13. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
14. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
15. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
16. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
17. 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.
18. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

19. 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.
20. 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.
21. 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.
22. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
23. 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.
24. 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.
25. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.
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. 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.
30. Канцедал С.А. Алгоритмизация и программирование : учебное пособие. - М: ФОРУМ, 2010.
31. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации : учеб. пособие для студентов вузов / под ред. С.А. Клейменова. - М: Академия, 2008.
32. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
33. Методика определения актуальных угроз безопасности персональных

данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

34. 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.

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

36. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001г. № 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».

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

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

39. 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.

40. Саати Т. Принятие решений. - М.: «Радио и связь», 1993.

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

42. 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.

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

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

45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
46. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
47. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
48. 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».
49. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
50. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
51. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
52. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
53. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
54. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
55. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие (Профессиональное образование). - М: ФОРУМ: ИНФРА-М, 2009.

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

Результаты (освоенные профессиональные компетенции)	**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

Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			
3.			
4.			