МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕ-НИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАБАРДИНО-БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Х.М. БЕРБЕКОВА»
КОЛЛЕДЖ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЭКОНОМИКИ

СОГЛАСОВАНО
Председатель КБНЦ РАН
_____/З.В. Нагоев/

«__»_____2020 г.

УТВЕРЖДАЮ
Директор колледжа информационных технологий и экономики
_____/З.Х. Этуева/
«__» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Программа подготовки специалистов среднего звена специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Среднее профессиональное образование

Квалификация выпускника

Техник по защите информации

Очная форма обучения

Нальчик, 2020г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее ФГОС) по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016г. № 1553, учебного плана по программе подготовки специалистов среднего звена

Разработчики: Л.Б. Бисчокова, преподаватель

З.С. Сижажева, преподаватель

Рецензент: _____Иванов Т.Х., директор Института информатики и проблем регионального управления КБНЦ РАН

Рабочая программа профессионального модуля обсуждена и одобрена на заседании ЦК программирования и информационной безопасности

Протокол № __ от « ___ » _____ 2020г

Председатель ЦК Е.К. Эдгулова

_____
(подпись)

Согласовано

Научная библиотека КБГУ,

отдел комплектования Н.А. Губжокова

_____
(подпись)

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Программа профессионального модуля (далее программа ПМ)-является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, в части освоения основного вида деятельности

1.2. Цели и задачи модуля, требования к результатам освоения модуля

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля 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.

Уметь:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- применять программные и программно-аппаратные средства для защиты информации в базах данных;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- применять математический аппарат для выполнения криптографических преобразований;
- использовать типовые программные криптографические средства, в том числе электронную подпись;

- применять средства гарантированного уничтожения информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

знать:

- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации;
- особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.3. Количество часов, отводимое на освоение профессионального модуля

объем образовательной программы учебной дисциплины – 611 часов,

- объем работы обучающихся с преподавателем по МДК– 425;
- самостоятельная работа – 6;
- консультации – 8;
- промежуточная аттестация – 14;
- учебной практики – 108;
- производственной практики – 72;
- курсовое проектирование – 30.

2.РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
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.
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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

3.1. Тематический план профессионального модуля

Коды ПК и ОК	Наименования разделов профессионального модуля	Всего часов	Объем профессионального модуля, час									
			Обучение по МДК								Практика	
			Объем образовательной программы	в том числе				Самостоятельная работа	Консультация	Промежуточная аттестация	УП	ПП
				теоретическое обучение	практические занятия	лабораторные работы	курсовая работа (проект)					
1	2	3	4	5	6	7	8	9	10	11	12	13
ПК 2.1.-2.6 ОК 1–10	**МДК 02.01** Программные и программно-аппаратных средства защиты информации	**363**	**255**	137	66	-	30	6	8	8	72	36
	МДК 02.02 Криптографические средства защиты информации	**242**	**170**	110	60	-	-				36	36
	Экзамен по модулю	**6**					-		-	6		
	Всего:	**611**	**425**	**247**	**126**	-	**30**	**6**	**8**	**14**	**108**	**72**

3.2. Содержание обучения по профессиональному модулю

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	Уровень освоения
1	2		3	
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации			**425**	
МДК.02.01. Программные и программно-аппаратные средства защиты информации			**247**	
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации			**52**	
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**		**6**	
	1	Предмет и задачи программно-аппаратной защиты информации	6	1,2
	2	Основные понятия программно-аппаратной защиты информации		1,2
	3	Классификация методов и средств программно-аппаратной защиты информации		1,2
Тема 1.2. Стандарты безопасности	**Содержание**		**10**	
	4	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	2
	5	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2	2
	Тематика практических занятий		**6**	**2,3**
	Практическая работа №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			
	Практическая работа №2-3. Работа с содержанием нормативных правовых актов Обзор стандартов. Работа с содержанием стандартов			
Тема 1.3. Защищенная автоматизированная система	**Содержание**		**16**	
	6	Автоматизация процесса обработки информации. Понятие автоматизированной системы.	2	1
	7	Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.	2	2
	8	Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС	2	2
	9	Дискреционные модели. Мандатные модели	2	2
	Тематика практических занятий		**8**	

	Практическая работа №4. Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей			
	Практическая работа №5. Разграничение доступа. Регистрация событий (аудит).			
	Практическая работа №6-7. Контроль целостности данных. Уничтожение остаточной информации.			
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**		**8**	
	10	Источники дестабилизирующего воздействия на объекты защиты	2	2
	11	Способы воздействия на информацию	2	2
	12	Причины и условия дестабилизирующего воздействия на информацию	2	2
	Тематика практических занятий		**2**	
	Практическая работа №8. Распределение каналов в соответствии с источниками воздействия на информацию			
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**		**12**	
	13	Понятие несанкционированного доступа к информации Основные подходы к защите информации от НСД	2	1
	14	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	2	2
	15	Доступ к данным со стороны процесса	2	2
	16	Особенности защиты данных от изменения. Шифрование	2	2
	Тематика практических занятий		**4**	
	Практическая работа №9. Организация доступа к файлам			
	Практическая работа №10. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД			
Рубежный контроль №1			2	
Самостоятельная работа 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. Тематика внеаудиторных самостоятельных работ: Написать реферат на тему «Новые технологии хранения информации»			1	
Раздел 2. Защита автономных автоматизированных систем			**74**	
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**		**10**	
	17	Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды	2	1,2
	18	Расширение BIOS как средство замыкания программной среды	2	2
	19	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды.	2	2

	20	Понятие АМДЗ (доверенная загрузка).Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	4	1
Тема 2.2.Защита программ от изучения	**Содержание**		**8**	
	21	Изучение и обратное проектирование ПО.	2	2
	22	Задачи защиты от изучения и способы их решения. Защита от отладки	2	2
	23	Защита от дизассемблирования	2	2
	24	Защита от трассировки по прерываниям	2	2
Тема 2.3. Вредоносное программное обеспечение	**Содержание**		**18**	
	25	Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения	2	2
	26	Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	2	2
	27	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	4	2
	28	Бот-неты. Принцип функционирования. Методы обнаружения	2	2
	29	Классификация антивирусных средств. Сигнатурный и эвристический анализ	2	2
	30	Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии	2	3
	Тематика практических занятий		**4**	
	Практическая работа №11-12. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО			
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**		**10**	
	31	Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования	2	1
	32	Привязка ПО к аппаратному окружению и носителям	2	2
	33	Защитные механизмы в современном программном обеспечении на примере MS Office	2	2
	Тематика практических занятий		**4**	**2,3**

	Практическая работа №13-14. Защита информации от несанкционированного копирования с использованием специализированных программных средств Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)			
Тема 2.5. Защита информации на машинных носителях	**Содержание**		**18**	
	34	Проблема защиты отчуждаемых компонентов ПЭВМ.	2	2
	35	Методы защиты информации на отчуждаемых носителях. Шифрование.	2	2
	36	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2	2
	37	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	2	2
	38	Безвозвратное удаление данных. Принципы и алгоритмы	2	2
	Тематика практических занятий		**8**	
	Практическая работа №15. Применение средства восстановления остаточной информации на примере Foremost или аналога			
	Практическая работа №16-17.Применение специализированного программного средства для восстановления удаленных файлов			
	Практическая работа №18. Применение программ для безвозвратного удаления данных			
	Практическая работа №19. Применение программ для шифрования данных на съемных носителях			
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**		**4**	
	39	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2	2
	40	Устройства Touch Memory	2	2
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**		**10**	
	41	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	4	2
	42	Использование сетевых снифферов в качестве СОВ		2
	43	Аппаратный компонент СОВ. Программный компонент СОВ	2	2
	44	Модели системы обнаружения вторжений. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений	2	2
	Тематика практических занятий		**2**	
	Практическая работа №20. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений			
Рубежный контроль №2			**2**	

Самостоятельная работа 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. Тематика внеаудиторных самостоятельных работ: 1. Подготовить презентацию на тему «Статистика и анализ крупных утечек информации за год»			2	
2 СЕМЕСТР ОБУЧЕНИЯ **Раздел 3. Защита информации в локальных сетях**			**17**	
Тема 3.1. Основы построения защищенных сетей	**Содержание**		**7**	
	45	Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации	5	1
	46	Штатные средства защиты информации стека протоколов TCP/IP		2
	47	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения	2	2
Тема 3.2. Средства организации VPN	**Содержание**		**10**	
	48	Виртуальная частная сеть. Функции, назначение, принцип построения	2	1
	49	Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр	2	2
	50	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2	2
	51	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2	2
	Тематика практических занятий		**2**	
	Практическая работа №21. Развертывание VPN			
Самостоятельная работа 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. Тематика внеаудиторных самостоятельных работ: Подготовить презентацию на тему «Поиск информации о новых видах атак на информационную систему»			**1**	
Раздел 4. Защита информации в сетях общего доступа			**18**	
Тема 4.1.Обеспечение безопасности межсетевого	**Содержание**		**18**	
	52	Методы защиты информации при работе в сетях общего доступа	2	1

взаимодействия	53	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall	2	2
	54	Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня	4	2
	55	Однохостовые и мультихостовые firewall	2	2
	56	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций.	2	2
	57	Требования по сертификации межсетевых экранов	2	2
	Тематика практических занятий и лабораторных работ		**4**	
	Практическая работа №22. Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr			
	Практическая работа №23. Изучение различных способов закрытия "опасных" портов			
Самостоятельная работа 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. Тематика внеаудиторных самостоятельных работ: Подготовить доклад по теме «Обзор современных программных и программно-аппаратных средств защиты»			**1**	
Раздел 5. Защита информации в базах данных			**14**	
Тема 5.1. Защита информации в базах данных	**Содержание**		**14**	
	58	Основные типы угроз. Модель нарушителя	**2**	**1**
	59	Средства идентификации и аутентификации. Управление доступом	**2**	**1**
	60	Средства контроля целостности информации в базах данных.Средства аудита и контроля безопасности. Критерии защищенности баз данных	2	2
	61	Применение криптографических средств защиты информации в базах данных	2	2
	Тематика практических занятий		**6**	
	Практическая работа №24-25. Изучение механизмов защиты СУБД MS Access			
	Практическая работа №26. Изучение штатных средств защиты СУБД MSSQL Server			
Рубежный контроль № 1			**2**	
Раздел 6. Мониторинг систем защиты			**22**	
Тема 6.1. Мониторинг систем защиты	**Содержание**		**10**	
	62	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	2	1

	63	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2	1
	64	Классификация отслеживаемых событий. Особенности построения систем мониторинга. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования	2	2
	65	Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке	2	2
	Тематика практических занятий		**2**	
	Практическая работа №27. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов			
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**		**6**	
	66	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты	4	1
	Тематика практических занятий		**2**	
	Практическая работа №28. Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке			
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Тематика практических занятий**		**8**	
	Практическая работа №29. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов			
	Практическая работа №30. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов			
	Практическая работа №31Изучение типовых решений для построения VPN на примере VipNet или других аналогов			
	Практическая работа №32. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов			
Рубежный контроль №2			2	
Самостоятельная работа 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. Тематика внеаудиторных самостоятельных работ: Подготовить реферат по теме «Сравнительный анализ современных программных и программно-аппаратных средств защиты»			**1**	
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		
Тематика самостоятельной работы при изучении МДК.02.01 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты		
Промежуточная аттестация по МДК.02.01 в виде экзамена	**6**	
Виды самостоятельных работ при изучении раздела 1 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 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.		
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	**72**	
Раздел 2 модуля. Применение криптографических средств защиты информации	**170**	

МДК.02.02. Криптографические средства защиты информации			**165**	
Введение	**Содержание**		**2**	
	1	Предмет и задачи криптографии. История криптографии. Основные термины		1
Раздел 1. Математические основы защиты информации				
Тема 1.1. Математические основы криптографии	**Содержание**		**40**	
	2	Элементы теории множеств. Группы, кольца, поля.	2	2
	3	Делимость чисел. Признаки делимости. Простые и составные числа.	2	2
	4	Основная теорема арифметики. Наибольший общий делитель.	2	2
	5	Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2	2
	6	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2	2
	7	Классы. Полная и приведенная система вычетов. Функция Эйлера.	2	2
	8	Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	2 2	2
	9	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида	2	2
	10	Китайская теорема об остатках.	2	2
	11	Проверка чисел на простоту. Алгоритмы генерации простых чисел.	2	3
	12	Метод пробных делений. Решето Эратосфена.	4	2
	13	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	3	3
	14	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2	3
	15	Арифметические операции над большими числами.	2	2
	16	Эллиптические кривые и их приложения в криптографии.	2	2
	Тематика практических занятий и лабораторных работ		**8**	
	Практическая работа №1-2. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений			
	Практическая работа №3. Проверка чисел на простоту			
	Практическая работа №4. Решение задач с элементами теории чисел. **Рубежный контроль № 1**			
Раздел 2. Классическая криптография				
Тема 2.1. Методы	**Содержание**		**14**	

криптографического защиты информации	17	Классификация основных методов криптографической защиты.	2	1
	18	Методы симметричного шифрования	2	1
	19	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2	2
	20	Методы перестановки. Табличная перестановка, маршрутная перестановка	2	2
	21	Гаммирование. Гаммирование с конечной и бесконечной гаммами	2	2
	Тематика практических занятий и лабораторных работ		**8**	
	Практическая работа №5-6. Применение классических шифров замены			
	Практическая работа №7. Применение классических шифров перестановки			
	Практическая работа №8. Применение метода гаммирования			
Тема 2.2. Криптоанализ	**Содержание**		**14**	
	22	Основные методы криптоанализа. Криптографические атаки.	2	1
	23	Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффа	2	1
	24	Перспективные направления криптоанализа, квантовый криптоанализ.	2	2
	Тематика практических занятий и лабораторных работ		**10**	
	Практическая работа №-9-10. Криптоанализ шифра простой замены методом анализа частотности символов			
	Практическая работа №11. Криптоанализ классических шифров методом полного перебора ключей			
	Практическая работа №12. Криптоанализ шифра Вижинера			
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**		**10**	
	25	Основные принципы поточного шифрования.	2	2
	26	Применение генераторов ПСЧ в криптографии	2	2
	27	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	2	2
	Тематика практических занятий и лабораторных работ		**4**	
	Практическая работа №13-14. Применение методов генерации ПСЧ **Рубежный контроль № 2**			
2 СЕМЕСТР ОБУЧЕНИЯ **Раздел 3. Современная криптография**			**20**	
Тема 3.1. Кодирование информации. Компьютеризация шифрования	28	Кодирование информации. Символьное кодирование.	2	2
	29	Смысловое кодирование. Механизация шифрования.	2	2
	30	Представление информации в двоичном коде. Таблица ASCII	2	2
	31	Компьютеризация шифрования. Аппаратное и программное шифрование	2	2

	32	Стандартизация программно-аппаратных криптографических систем и средств.	2	2
	33	Изучение современных программных и аппаратных криптографических средств	2	2
	Тематика практических занятий		**10**	
	Практическая работа №15. Кодирование информации			
	Практическая работа №16. Программная реализация классических шифров			
	Практическая работа №17-18.Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.			
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**		**9**	
	34	Общие сведения. Структурная схема симметричных криптографических систем	2	1
	35	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.	2	3
	36	Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	2	3
	Тематика практических занятий		**3**	
	Практическая работа №19.Изучение программной реализации современных симметричных шифров			
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**		**10**	
	37	Криптосистемы с открытым ключом. Необратимость систем	2	2
	38	Структурная схема шифрования с открытым ключом	2	2
	39	Элементы теории чисел в криптографии с открытым ключом	2	2
	Тематика практических занятий и лабораторных работ		**4**	
	Практическая работа №20. Применение различных асимметричных алгоритмов.			
	Практическая работа №21. Изучение программной реализации асимметричного алгоритма RSA			
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**		**12**	
	40	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции	2	2
	41	Алгоритмы цифровой подписи	2	2
	Тематика практических занятий и лабораторных работ		**8**	
	Практическая работа №22. Применение различных функций хеширования, анализ особенностей хешей			
	Практическая работа №23. Применение криптографических атак на хеш-функции.			
	Практическая работа №24. Изучение программно-аппаратных средств, реализующих основные функции ЭП			

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**		**8**	
	42	Алгоритмы распределения ключей с применением симметричных и асимметричных схем	2	2
	43	Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация **Рубежный контроль № 1**	2	2
	Тематика практических занятий и лабораторных работ		**4**	
	Практическая работа №25. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.			
	Практическая работа №26. 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**		**6**	
	44	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.	2	1
	45	Криптомаршрутизатор. Пакетный фильтр	2	2
	46	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	2	2
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**		**10**	
	47	Принципы функционирования электронных платежных систем. Электронные пластиковые карты.	2	2
	49	Персональный идентификационный номер	2	3
	50	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2	3
	Тематика практических занятий и лабораторных работ		**4**	
	Практическая работа №27-28**.** Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей			
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**		**12**	
	51	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	2	2
	52	Методы компьютерной стеганографии. Цифровые водяные знаки.	2	2
	53	Алгоритмы встраивания ЦВЗ	2	2
	Тематика практических занятий и лабораторных работ		**6**	
	Практическая работа №29 Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ			
	Практическая работа №30 Реализация простейших стеганографических алгоритмов **Рубежный контроль № 2**			
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 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 в виде дифференцированного зачета		
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	**36**	
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.	**36**	
Экзамен по профессиональному модулю	**6**	
Итого часов по модулю:	**611**	
Теоретическое обучение	**247**	
практически обучение	**126**	
Курсовое проектирование	**30**	
Учебная практика	**108**	

Производственная практика	**72**	
Самостоятельная работа	**6**	
Консультации	**8**	
Промежуточная аттестация	**14**	
Итого	**611**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1.Требования к материально-техническому обеспечению

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.

4.2. Информационное обеспечение обучения

4.2.1.Основные источники:

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М. : Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html

2. 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

Введение в защиту информации от внутренних ИТ-угроз : учебное пособие. — 2-е изд. — Москва : ИНТУИТ, 2016. — 39 с. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/100720 — Режим доступа: для авториз. пользователей.

3. Бондаренко, И.С. Методы и средства защиты информации : учебное пособие / И.С. Бондаренко, Ю.В. Демчишин. — Москва : МИСИС, 2018. — 32 с. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/115269 — Режим доступа: для авториз. пользователей.

4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб.

Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.

5. Бутакова, Н.Г. Криптографические методы защиты информации, учебное пособие : учебное пособие / Н.Г. Бутакова, Н.В. Федоров. — Санкт-Петербург : Интермедия, 2016. — 384 с. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/90270 — Режим доступа: для авториз. пользователей. 2 Бахаров, Л.Е. Информационная безопасность и защита информации (разделы криптография и стеганография) : учебное пособие / Л.Е. Бахаров. — Москва : МИСИС, 2019. — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/116907 . — Режим доступа: для авториз. пользователей.

6. Стеганографические и криптографические методы защиты информации : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/90963 . — Режим доступа: для авториз. пользователей.

7. Современные методы обеспечения защиты информации : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/90965 — Режим доступа: для авториз. пользователей.

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

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

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

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

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

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

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

30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

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

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

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

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

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

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

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

38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

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

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

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

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

43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных

технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

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

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

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

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

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

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

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

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

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

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

4.2.3. 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/

42.4. 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

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ(ВИДА ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные ПК)	Основные показатели оценки результата	Методы и методы контроля и 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

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
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 Экзамен квалификационный
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	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 Экзамен квалификационный
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
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;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

	- обоснованность анализа работы членов команды (подчиненных)	Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
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	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 Экзамен квалификационный
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,	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 Экзамен квалификационный
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	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 Экзамен квалификационный
ОК 08. Использовать средства физической культуры для сохранения и	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе

укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	производственной практик;	освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	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 Экзамен квалификационный