МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ «ГУБЕРНСКИЙ КОЛЛЕДЖ Г. СЫЗРАНИ»

УТВЕРЖДЕНО

Приказ ГБПОУ «ГК г. Сызрани»
от « 30 » мая 2024 г. № 268-о

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

основной образовательной программы
по специальности:

10.02.05 Обеспечение информационной безопасности автоматизированных систем

ЭП

C=RU, OU=Директор, O="ГБПОУ ""ГК г. Сызрани""", CN=Павел Салугин, E=gk_szr@samara.edu.ru
00d644d85759a06e75
2024-06-15 11:32:11

Сызрань, 2024 г.

РАССМОТРЕНА	**СОГЛАСОВАНО**
Предметной (цикловой) комиссией	ИП Фирсов Е. В.
общепрофессиональных и	
профессиональных циклов	_____Е. В. Фирсов
председатель М.В. Киреева	
от « 23 » мая 2024г. протокол №9	от « 23 » мая 2024г. протокол №9

Составитель: М.В. Киреева, преподаватель строительного профиля ГБПОУ «ГК г. Сызрани»

Внутренняя экспертиза (техническая и содержательная):

И.Н. Ежкова, методист строительного профиля ГБПОУ «ГК г. Сызрани»

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденной приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553.

Рабочая программа разработана с учетом профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», 06.030, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25.11.2016 N 44449

Рабочая программа ориентирована на подготовку обучающихся к выполнению заданий, соответствующих требованиям регионального чемпионата «Молодые профессионалы» по компетенции Корпоративная защита от внутренних угроз информационной безопасности, требований демонстрационного экзамена по компетенции Корпоративная защита от внутренних угроз информационной безопасности.

Рабочая программа разработана в соответствии с требованиями к оформлению, установленными в ГБПОУ «ГК г. Сызрани».

Содержание программы реализуется в процессе освоения обучающимися программы подготовки специалистов среднего звена в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Рабочая программа профессионального модуля (далее программа – ПМ) является частью основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем углубленной подготовки, разработанной в ГБПОУ «ГК г. Сызрани».

Рабочая программа составляется для очной формы обучения.

1.2. Цель и задачи модуля – требования к результатам освоения модуля:

По результатам освоения ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами у обучающихся должны быть сформированы образовательные результаты в соответствии с ФГОС СПО:

В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установки, настройки программных средств защиты информации в автоматизированной системе; обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе.

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.

Вариативная часть:

По результатам освоения ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами у обучающихся должны быть сформированы вариативные образовательные результаты, ориентированные на выполнение профессионального стандарта.

С целью реализации требований профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации и квалификационных запросов предприятий/ регионального рынка труда, обучающийся должен*:*

иметь практический опыт:

- текущий, в том числе автоматизированный контроль функционирования СССЭ с установленными показателями;
- текущий, в том числе автоматизированный контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД;
- внесение изменений в настройки СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД без прерывания процесса их функционирования;
- восстановление процесса функционирования после сбоев и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД;
- восстановление значений показателей функционирования СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД.

уметь:

- проводить текущий контроль показателей и процесса функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД, предусмотренный регламентом их эксплуатации;
- выполнять предусмотренные в технической документации работы по изменению настроек СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД;
- проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД.

знать:

- Типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД;
- последовательность действий в целях изменения настроек СССЭ, а также средств и систем защиты СССЭ от НСД без прерывания процесса их функционирования;
- последовательность действий в целях восстановления процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД;
- организационные меры по защите информации;
- нормативные правовые акты в области связи, информатизации и защиты информации.

1.3. Количество часов на освоение программы профессионального модуля

Вид учебной деятельности	Объём часов
Объем образовательной программы (всего)	699
Нагрузка во взаимодействии с преподавателем	**659**
В том числе:	
Теоретическое обучение	66
Лабораторные работы и практические занятия	240
Консультации: По МДК 02.01 По МДК 02.02 По МДК 02.03	 6 6 6
Промежуточная аттестация По МДК 02.01 По МДК 02.02 По МДК 02.03	 6 6 6
Курсовая работа (проект) По МДК 02.01	 30
Учебная практика	108
Производственная практика	72
Промежуточная аттестация в форме	экзамена
Консультация к экзамену (квалификационному)	6
Экзамен (квалификационный)	6
Самостоятельная работа студента (всего) в том числе: *работа над курсовым проектом,* *оформление отчетов к практическим работам*	**29**

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

В результате изучения профессионального модуля обучающиеся должны освоить основной вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и овладеть соответствующими ему профессиональными компетенциями (ПК), указанными в ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, перечень профессиональных компетенций:

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

Результатом освоения профессионального модуля является овладение трудовой функцией профессионального стандарта:

- обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД.

В процессе освоения ПМ обучающиеся должны овладеть общими компетенциями (ОК):

Код	**Наименование видов деятельности и профессиональных компетенций**
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Тематический план профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Занятия во взаимодействии с преподавателем, час.							Квалификационный экзамен	Самостоятельная работа
			Обучение по МДК, в час.					Практики			
			Теоретическое обучение	Лабораторных и практических занятий	Курсовых работ (проектов)	Консультации	Промежуточная аттестация	Учебная	Производственная (если предусмотрена рассредоточенная практика)		
1	2	3	4	5	6			7	8		9
ПК 1.2	**Раздел 1.** Применение программных и программно-аппаратных средств защиты информации	**150**	28	72	*30*	*6*	*6*				8
ПК 1.1-1.3	**Раздел 2.** Применение криптографических средствзащиты информации	**465**	76	236		*12*	*12*	108			21
	Производственная практика	**72**							72		
	Экзамен (квалификационный) попрофессиональному модулю	**12**								*12*	
	Всего:	***699***	***104***	***308***	***30***	***18***	***18***	***108***	***72***	***12***	***29***

3.2 Содержание обучения по профессиональному модулю

Наименование разделовпрофессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия,самостоятельная работа обучающегося, курсовая работа (проект)	Объемчасов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	
Раздел 1. Применение программных и программно-аппаратных средств защиты информации			
МДК.02.01. Программные и программно-аппаратные средства защиты информации			
Тема 1. Основные принципы программной и программно-аппаратной защиты информации			ПК 2.1-2.6, ОК 01-11
Тема 1.1. Предмет изадачи программно-аппаратной защиты информации	**Содержание**	**2**	
	Предмет и задачи программно-аппаратной защиты информации		
	Основные понятия программно-аппаратной защиты информации		
	Классификация методов и средств программно-аппаратной защиты информации		
Тема 1.2. Стандартыбезопасности	**Содержание**	**2**	
	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, средствантивирусной защиты)		
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	**6**	
	1. Обзор нормативных правовых актов, нормативных методических документов по защи-		

		те информации,в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами		
	2.	Работа с содержанием нормативных правовых актов.		
	3.	Обзор стандартов. Работа с содержанием стандартов		
Тема 1.3. Защищеннаяавтоматизированная система	**Содержание**		**2**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**20**	
	4.	Учет, обработка, хранение и передача информации в АИС		
	5.	Ограничение доступа на вход в систему.		
	6.	Идентификация и аутентификация пользователей		
	7.	Разграничение доступа.		
	8.	Регистрация событий (аудит).		
	9.	Контроль целостности данных		
	10.	Уничтожение остаточной информации		
	11.	Управление политикой безопасности. Шаблоны безопасности		
	12.	Криптографическая защита. Обзор программ шифрования данных		
	13.	Управление политикой безопасности. Шаблоны безопасности		
Тема 1.4. Дестабилизирующее воздействие на объектызащиты	**Содержание**		**2**	
	Источники дестабилизирующего воздействия на объекты защиты			
	Способы воздействия на информацию			
	Причины и условия дестабилизирующего воздействия на информацию			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**4**	
	14	Распределение каналов в соответствии с источниками воздействия на информацию		

Тема 1.5. Принципы программно-аппаратнойзащиты информации от несанкционированного доступа	**Содержание**		**2**	
	Понятие несанкционированного доступа к информации			
	Основные подходы к защите информации от НСД			
	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.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**2**	
	15	Организация доступа к файлам		
	16	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		
Тема 2. Защита автономных автоматизированных систем				ПК 2.1-2.6, ОК 01-11
Тема 2.1. Основы защитыавтономных автоматизированных систем	**Содержание**		**2**	
	Работа автономной АС в защищенном режиме			
	Алгоритм загрузки ОС. Штатные средства замыкания среды			
	Расширение BIOS как средство замыкания программной среды			
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)			
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		Не предусмотрено	
Тема 2.2.Защита программ от изучения	**Содержание**		**2**	
	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.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		Не предусмотрено	

Тема 2.3. Вредоносное программное обеспечение	**Содержание**		**2**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**2**	
	17	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		
Тема 2.4. Защита программ и данных от несанкционированногокопирования	**Содержание**		**2**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**4**	
	18	Защита информации от несанкционированного копирования с использованием специализированных программных средств		
	19	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)		
Тема 2.5. Защита информации на машинных носителях	**Содержание**		**1**	
	Проблема защиты отчуждаемых компонентов ПЭВМ.			
	Методы защиты информации на отчуждаемых носителях. Шифрование.			
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**10**	
	20	Применение средства восстановления остаточной информации на примере Foremost или		

		аналога		
	21	Применение специализированного программно средства для восстановления удаленных файлов		
	22	Применение программ для безвозвратного удаления данных		
	23	Применение программ для шифрования данных на съемных носителях		
	24	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.		
	25	Безвозвратное удаление данных. Принципы и алгоритмы.		
Тема 2.6. Аппаратные средства идентификациии аутентификации пользователей	**Содержание**		**1**	
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ			
	Устройства Touch Memory			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		Не предусмотрено	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**		**1**	
	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.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**2**	
	26	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений		
Тема 3. Защита информации в локальных сетях				
Тема 3.1. Основы построения защищенныхсетей	**Содержание**		**1**	ПК 2.1-2.6, ОК 01-11
	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.			

	Лабораторные работы		Не предусмотрено	
	Практические занятия		Не предусмотрено	
Тема 3.2. Средстваорганизации VPN	**Содержание**		**1**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**2**	
	27	Развертывание VPN		
Тема 4. Защита информации в сетях общего доступа				ПК 2.1-2.6, ОК 01-11
Тема 4.1. Обеспечениебезопасности межсетевого взаимодействия	**Содержание**		**1**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**2**	
	28	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr		
	29	Изучение различных способов закрытия "опасных" портов		
Тема 5. Защита информации в базах данных				ПК 2.1-2.6, ОК 01-11
Тема 5.1. Защита информации в базахданных	**Содержание**		**1**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**2**	
	30	Изучение механизмов защиты СУБД MS Access		
	31	Изучение штатных средств защиты СУБД MSSQL Server		
Тема 6. Мониторинг систем защиты				ПК 2.1-2.6, ОК 01-11
Тема 6.1. Мониторингсистем защиты	**Содержание**		**1**	
	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.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**4**	
	32	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов		
	33	Проведение аудита ЛВС сетевым сканером		
Тема 6.2. Изучение мерзащиты информации в информационных системах	**Содержание**		**2**	
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**2**	
	34	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	**Содержание**		**-**	

современных программно-аппаратныхкомплексов.	**Лабораторные работы**		Не предусмотрено	
	Практические занятия		**10**	
	35	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов		
	36	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или другиханалогов		
	37	Изучение типовых решений для построения VPN на примере VipNet или других аналогов		
	38	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов		
	39	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов		
Курсовой проект			**30**	
Примерная тематика курсовых проектов 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 6. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам,главам учебных пособий, составленным преподавателем) 7. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление			**8**	

практическихработ, отчетов к их защите. 8. Работа над курсовым проектом (работой): планирование выполнения курсового проекта, определение задач работы,изучение литературных источников, проведение предпроектного исследования.			
Консультации		**6**	
Промежуточная аттестация по МДК.02.01 в виде экзамена		**6**	
Раздел 2. Применение криптографических средств защиты информации			
МДК.02.02. Криптографические средства защиты информации			
Введение	**Содержание**	**2**	
	Предмет и задачи криптографии. История криптографии. Основные термины		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	Не предусмотрено	
Тема 1. Математические основы защиты информации			ПК 2.4, ОК 01-11
Тема 1.1. Математические основы криптографии	**Содержание**	**5**	
	Элементы теории множеств. Группы, кольца, поля.		
	Делимость чисел. Признаки делимости. Простые и составные числа.		
	Основная теорема арифметики. Наибольший общий делитель. Взаимнопростые 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.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**18**	
	1	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений		
	2	Проверка чисел на простоту		
	3	Решение задач с элементами теории чисел.		
Тема 2. Классическая криптография				ПК 2.4, ОК 01-11
Тема 2.1. Методы криптографическогозащиты информации	**Содержание**		**3**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**16**	
	4	Применение классических шифров замены		
	5	Применение классических шифров перестановки		
	6	Применение метода гаммирования		
Тема 2.2. Криптоанализ	**Содержание**		**3**	
	Основные методы криптоанализа. Криптографические атаки.			
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса			
	Перспективные направления криптоанализа, квантовый криптоанализ.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**20**	
	7	Криптоанализ шифра простой замены методом анализа частотности символов		
	8	Криптоанализ классических шифров методом полного перебора ключей		
	9	Криптоанализ шифра Вижинера		
Тема 2.3. Поточные шифры и ге-	**Содержание учебного материала**		**3**	
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии			

нераторы псевдо-случайных чисел	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	10	Применение методов генерации ПСЧ		
Тема 3. Современная криптография				ПК 2.4, ОК 01-11
Тема 3.1. Кодирова-ниеинформации. Компьютеризация шифрования.	**Содержание учебного материала**		**3**	
	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 про-граммныхи аппаратных криптографических средств			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**18**	
	11	Кодирование информации		
	12	Программная реализация классических шифров		
	13	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.		
Тема 3.2. Симмет-ричныесистемы шифрования	**Содержание учебного материала**		**3**	
	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			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**10**	
	14	Изучение программной реализации современных симметричных шифров		
Тема 3.3. Асиммет-ричныесистемы шифрования	**Содержание учебного материала**		**3**	
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.			
	Элементы теории чисел в криптографии с открытым ключом.			
	Лабораторные работы		Не предусмотрено	

	Практические занятия		**16**	
	15	Применение различных асимметричных алгоритмов		
	16	Изучение программной реализации асимметричного алгоритма RSA		
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**		**3**	
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**16**	
	17	Применение различных функций хеширования, анализ особенностей хешей		
	18	Применение криптографических атак на хеш-функции		
	19	Изучение программно-аппаратных средств, реализующих основные функции ЭП		
Тема 3.5. Алгоритмыобмена ключей и протоколы аутентификации	**Содержание учебного материала**		**2**	
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**16**	
	20	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.		
	21	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos		
Тема 3.6. Криптозащитаинформации в сетях передачи данных	**Содержание учебного материала**		**3**	
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	22	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.		
Тема 3.7. Защита информации в электронных платежныхсистемах	**Содержание учебного материала**		**3**	
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.			
	Лабораторные работы		Не предусмотрено	

	Практические занятия		**12**	
	23	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей		
	24	Применение криптографических протоколов для обеспечения безопасности электронной коммерции		
Тема 3.8. Компьютернаястеганография	**Содержание учебного материала**		**2**	
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.			
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**10**	
	25	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ		
	26	Реализация простейших стеганографических алгоритмов		
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			**16**	
Консультации			**6**	
Промежуточная аттестация по МДК.02.02			**6**	
МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности				

Тема 1. Корпоративная защита от внутренних угроз информационной безопасности				ПК 2.4, ОК 01-11
Тема 1.1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты отвнутренних угроз	**Содержание учебного материала**		**20**	
	Сетевое окружение. Сетевые протоколы. Методы выявления и построения путей движения информации в организации; Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия. Типы сетевых устройств. Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонентсистем защиты от внутренних угроз; Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем; Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы; Этапы установки системы корпоративной защиты от внутренних угроз. Отличия различных версий систем корпоративной защиты от внутренних угроз; назначение различных компонент версий систем корпоративной защиты от внутренних угроз; технологии программной и аппаратной виртуализации.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**32**	
	1	Конфигурирование сетевой инфраструктуры		
	2	Установка и настройка системы корпоративной защиты		
	3	Имитация процесса утечки конфиденциальной информации		
	4	Подготовка отчета по оценке работоспособности системы		
Тема 1.2. Технологии агентского мониторинга	**Содержание учебного материала**		**18**	
	Функции агентского мониторинга; Общие настройки системы агентского мониторинга; Соединение с LDAP-сервером и синхронизация с Active Directory; Политики агентского мониторинга, особенности их настройки; Особенности настроек событий агентского мониторинга; Механизмы диагностики агента, подходы к защите агента.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**36**	
	5	Механизмы работы агентского мониторинга		
	6	Разработка и применение политик агентского мониторинга для работы с носителями и устройствами		
	7	Разработка и применение политик агентского мониторинга для работы с файлами		

	8	Работа с исключениями		
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.			**5**	
Консультации			**6**	
Промежуточная аттестация по МДК.02.03			**6**	
Учебная практика: − Применение программных и программно-аппаратных средств обеспечения информационной безопасности вавтоматизированных системах − Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационнойбезопасности − 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 − Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи			**108**	
Производственная практика по ПМ.02			**72**	

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 средствобеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности вструктурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационнойбезопасности программно-аппаратными средствами при выполнении задач практики.		
Экзамен (квалификационный) по профессиональному модулю	**12**	
Всего:	**699**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Требования к минимальному материально-техническому обеспечению

Реализация программы ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами требует наличия учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации».

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

Оборудование лаборатории «Информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

4.2 Информационное обеспечение обучения (перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы)

Основные источники

Для преподавателей

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

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

5. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

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

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

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

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

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

Для студентов

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

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

5. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

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

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

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

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

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

Дополнительные источники:

Для преподавателей

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 конфиденци-

альной 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

Для студентов

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

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

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

5. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

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

7. Информационно-справочная система по документам в области технической защитыинформации www.fstec.ru

8. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

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

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

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

12. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

13. Российский биометрический портал www.biometrics.ru

14. Федеральный портал «Информационно- коммуникационные технологии вобразовании» htpp\\:www.ict.edu.ru

15. Сайт Научной электронной библиотеки www.elibrary.ru

4.3 Общие требования к организации образовательного процесса

Освоение ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами производится в соответствии с учебным планом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и календарным графиком, утвержденным директором ОО.

График освоения ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами предполагает последовательное освоение МДК 02.01 Программные и программно-аппаратные средства защиты информации, МДК 02.02 Криптографические средства защиты информации МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности, включающих в себя как теоретические, так и лабораторно-практические занятия.

Освоению ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами предшествует обязательное изучение учебных дисциплин ОП.02 Организационно-правовое обеспечение информационной безопасности, ОП.03 Основы алгоритмизации и программирования.

В процессе освоения ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами предполагается проведение текущего контроля знаний, умений у обучающихся. Выполнение практических занятий работ является обязательной для всех обучающихся. Наличие оценок по практическим занятиям (ПЗ) является для каждого студента обязательным. В случае отсутствия оценок за ПЗ студент не допускается до сдачи квалификационного экзамена по ПМ.

С целью оказания помощи обучающимся при освоении теоретического и практического материала, выполнения самостоятельной работы разрабатываются учебно-методические комплексы для студентов (кейсы студентов).

С целью методического обеспечения прохождения учебной и/или производственной практики (далее - УП/ПП), выполнения курсового проекта разрабатываются методические рекомендации для студентов по выполнению КР/КП, прохождению УП/ПП.

При освоении ПМ консультации проводятся согласно графика проведения консультаций

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты (освоенные профессиональные и общие компетенции)	**Основные показатели оценки результата**	**Формы 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 практическихработ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации вавтоматизированных 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 практическихработ, 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 практическихработ, 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 ограниченногодоступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения практическихработ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 2.5. Уничтожать информацию и носители информации сиспользованием 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 практическихработ, 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 практическихработ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

6. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ,
ВНЕСЁННЫХ В РАБОЧУЮ ПРОГРАММУ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

№ п/п	Дата внесения изменения	Внесённые изменения	№ страницы

1. ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ
2.

Дата актуализации	Результаты актуализации	ФИО и подпись лица, ответственного за актуализацию

ПРИЛОЖЕНИЕ 1
к рабочей программе ПМ
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ПЛАНИРОВАНИЕ УЧЕБНЫХ ЗАНЯТИЙ С ИСПОЛЬЗОВАНИЕМ АКТИВНЫХ И ИНТЕРАКТИВНЫХ ФОРМ И МЕТОДОВ ОБУЧЕНИЯ

№ п/п	Тема учебного занятия	Активные и интерактивные формы и методы обучения	Код формируемыхкомпетенций
1.	Методы создания безопасных систем	Урок презентация	ПК 2.2
2.	Методы защиты информации на отчуждаемых носителях. Шифрование.	семинар	ОК 04, ОК 09, ПК 2.4
3.	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	Решение практической задачи	ОК 01, 02,03, 09, ПК 2.3
4.	Основные методы криптоанализа. Криптографические атаки.	Работа в м/группах	ОК 01, 02, 03, 04, 09, ПК 2.1
5.	Алгоритмы распределения ключей с применением симметричных и асимметричныхсхем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	Урок с элементами проблемного обучения	ОК 01, 02, 03, 04, 09, ПК 2.6

ПРИЛОЖЕНИЕ 2
к рабочей программе профессионального модуля основной части ФГОС СПО

Ведомость соотнесения требований профессионального стандарта по профессии 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации и ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Обобщенная трудовая функция (ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ)	**Вид профессиональной деятельности (ФГОС СПО)**
Формулировка ОТФ: Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД	Формулировка ВПД: Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Трудовые функции	ПК
Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД	ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6

Результаты, заявленные в профессиональном стандарте	**Образовательные результаты ФГОС СПО по ПМ**
Название ТФ Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД	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 по-

Результаты, заявленные в профессиональном стандарте	Образовательные результаты ФГОС СПО по ПМ		
	следствий компьютерных атак.		
Трудовые действия	**Практический опыт**	**Задания на практику**	**Самостоятельная работа**
Текущий, в том числе автоматизированный контроль функционирования СССЭ с установленными показателями	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 защитыинформации; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных крип-	Применение программных и программно-аппаратных средств обеспечения информационной безопасности вавтоматизированных 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 пра-	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 6. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 7. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. 8. Работа над курсовым проектом (работой): планирование выполнения курсового проекта, определение задач работы, изучение литературных

Результаты, заявленные в профессиональном стандарте	Образовательные результаты ФГОС СПО по ПМ		
	тографических 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.	вовых актов. Применение математических методов для оценки качества и выбора наилучшего программного средства – – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи – 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	источников, проведение предпроектного исследования 9. История развития криптографии 10. Программная реализация классических шифров 11. Оптимизация методов частотного анализа моноалфавитных шифров. 12. Программная реализация классических шифров 13. Методы механизации шифрования 14. Цифровое представление различных форм информации 15. Анализ современных симметричных криптоалгоритмов 16. Анализ современных асимметричных криптоалгоритмов 17. Программная реализация современных криптоалгоритмов 18. Сравнительный анализ функций хеширования 19. Аутентификация сообщений 20. Законодательство в области криптографической защиты информации 21. Перспективные направления криптографии 22. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам
Необходимые умения	**Умение**	**Практические задания**	

Результаты, заявленные в профессиональном стандарте	Образовательные результаты ФГОС СПО по ПМ		
Проводить текущий контроль показателей и процесса функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД, предусмотренный регламентом их эксплуатации Выполнять предусмотренные в технической документации работы по изменению настроек СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Проводить предусмотренные регламентом работы по восстановлению процесса и пара-	Применять программные устанавливать и настраивать средства антивирусной защиты в соответствии спредъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность итестировать 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	Криптографическая защита. Обзор программ шифрования данных Управление политикой безопасности. Шаблоны безопасности Распределение каналов в соответствии с источниками воздействия на информацию Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. Криптоанализ шифра Вижинера Применение криптографических атак на хеш-функции. Изучение программно-аппаратных средств, реализующих основные функции ЭП. Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	учебных пособий, составленным преподавателем). 23. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.

Результаты, заявленные в профессиональном стандарте	Образовательные результаты ФГОС СПО по ПМ		
метров функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД	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		
Необходимые знания	**Знание**	**Темы**	
Типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД Последовательность действий в целях изме-	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-	Принципы программно-аппаратной защиты информации от несанкционированного доступа Защита программ и данных от несанкционированногокопирования Защита информации на машинных носителях Системы обнаружения атак ивторжений Обеспечениебезопасности межсетевого взаимодействия Изучение мер защиты информации в информационных системах Методы криптографическогозащиты информа-	

Результаты, заявленные в профессиональном стандарте	Образовательные результаты ФГОС СПО по ПМ		
нения настроек СССЭ, а также средств и систем защиты СССЭ от НСД без прерывания процесса их функционирования Последовательность действий в целях восстановления процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД Организационные меры по защите информации Нормативные правовые акты в области связи, информатизации и защиты информации	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.	ции Аутентификация данных.Электронная подпись Технологии агентского мониторинга	