государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»

Одобрено на заседании ПЦК
Информационных технологий и
программирования
Протокол № 9 от 13.06.2018

УТВЕРЖДАЮ
Заместитель директора
_____ О.В.Князева

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

для специальности

10.02.05 Обеспечение информационной безопасности
автоматизированных систем

2018

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённым приказом Министерства образования и науки Российской Федерации 09 декабря 2016 № 1553.

Составители:

Зиннурова Юлия Владимировна, преподаватель

Жигалова Елена Александровна, преподаватель высшей квалификационной категории

Соковнина Елена Алексеевна, преподаватель высшей квалификационной категории

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля (далее – рабочая программа) – является частью основной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области информатики и вычислительной техники при наличии основного общего и среднего (полного) общего образования.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля

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

иметь практический опыт в:

- установке и настройке программных средств защиты информации;
- тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;
- учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

уметь:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- использовать типовые программные криптографические средства, в том числе

электронную подпись;

- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- 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;
- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации.

1.3. Количество часов на освоение программы профессионального модуля

Вид учебной деятельности	Объем часов
Всего объем образовательной нагрузки	628
в том числе:	
Во взаимодействии с преподавателем	596
всего по дисциплинам и МДК	312
учебная практика	72
производственная практика	144
курсовое проектирование	30
консультации	18
промежуточная аттестация	20
Самостоятельная работа студента (в том числе):	32
Промежуточная аттестация в форме	Экзамен квалификационный

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами, в том числе профессиональными (ПК), указанными в ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем:

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

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

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

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 профессиональных компетенций	Наименования разделов профессионального модуля	Всего объем образовательной нагрузки	Работа обучающихся во взаимодействии с преподавателем								Самостоятельная работа обучающегося	
			Объем времени, отведенный на освоение междисциплинарного курса (курсов)				Практика		Консультации, час	Промежуточная аттестация, час	Всего, часов	в т.ч., курсовая работа (проект), часов
			Всего, часов	*в т.ч. теоретическое обучение, часов*	в т.ч. лабораторные работы и практические занятия, часов	курсовая работа (проект), часов	Учебная, часов	Производственная (по профилю специальности)				
1	2	3	4		5	6	7	8			9	10
ПК 2.1, ПК 2.2, ПК 2.3, ОК 01-ОК 07, ОК 09-ОК 10	Раздел 1. Программные и программно-аппаратные средства защиты информации	**200**	172	104	68				6	8	**14**	
ПК 2.4, ПК 2.5, ПК 2.6, ОК 01-ОК 07, ОК 09-ОК 10	Раздел 2. Криптографические средства и методы защиты информации	**196**	140	90	50	30			6	2	**18**	16
ПК 2.1-ПК 2.6	Учебная практика	**76**					72		2	2		
ПК 2.1-ПК 2.6, ОК 01-ОК 07, ОК 09-ОК 10	Практика производственная	**150**						144	4	2		
	Экзамен квалификационный	**6**								6		
	Всего:	**628**	**312**	**194**	**118**	**30**	**72**	**144**	**18**	**20**	**32**	**16**

3.2. Содержание обучения по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов			Уровень освоения
		л	пр	сам	
1	2	3	4	5	6
Раздел 1. Программные и программно-аппаратные средства защиты информации					
МДК 02.01 Программные и программно-аппаратные средства защиты информации					
Подраздел 1. Основные принципы программной и программно-аппаратной защиты информации					
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**				
	Предмет и задачи программно-аппаратной защиты информации	2			1
	Основные понятия программно-аппаратной защиты информации	2			
	Классификация методов и средств программно-аппаратной защиты информации	2			
Тема 1.2. Стандарты безопасности	**Содержание**				
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	2			2
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2			
	Тематика практических занятий и лабораторных работ				
	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.		4		
	Обзор стандартов. Работа с содержанием стандартов		2		
Тема 1.3. Защищенная автоматизированная система	**Содержание**				
	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в	2			2

	защищенном исполнении.				
	Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели	2			
	Тематика практических занятий и лабораторных работ				
	Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.		2		
	Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации.		2		
	Управление политикой безопасности. Шаблоны безопасности. Криптографическая защита. Обзор программ шифрования данных. Управление политикой безопасности. Шаблоны безопасности		2		
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**				
	Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию	2			2
	Причины и условия дестабилизирующего воздействия на информацию	2			
	Тематика практических занятий и лабораторных работ				
	Распределение каналов в соответствии с источниками воздействия на информацию		4		
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**				
	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД	2			2
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса	2			
	Особенности защиты данных от изменения. Шифрование.	2			
	Тематика практических занятий и лабораторных работ				
	Организация доступа к файлам		2		
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		2		
Подраздел 2. Защита автономных автоматизированных систем					
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**				
	Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды	2			2
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	2			
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	2			

Тема 2.2.Защита программ от изучения	**Содержание**				1
	Изучение и обратное проектирование ПО	1			
	Способы изучения ПО: статическое и динамическое изучение	1			
	Задачи защиты от изучения и способы их решения	1			
	Защита от отладки.	1			
	Защита от дизассемблирования	1			
	Защита от трассировки по прерываниям.	1			
Тема 2.3. Вредоносное программное обеспечение	**Содержание**				
	Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	1			**2**
	Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии	1			
	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	2			
	Тематика практических занятий и лабораторных работ				
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		2		
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**				
	Несанкционированное копирование программ как тип НСД	1			2
	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	1			
	Привязка ПО к аппаратному окружению и носителям.	1			
	Защитные механизмы в современном программном обеспечении на примере MS Office	1			
	Тематика практических занятий и лабораторных работ				
	Защита информации от несанкционированного копирования с использованием специализированных программных средств		1		
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)		1		
Тема 2.5. Защита информации на машинных носителях	**Содержание**				
	Проблема защиты отчуждаемых компонентов ПЭВМ.	1			2
	Методы защиты информации на отчуждаемых носителях. Шифрование.	1			
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	1			
	Применение средств восстановления остаточной информации в судебных криминалистических	1			

	экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов				
	Безвозвратное удаление данных. Принципы и алгоритмы.	2			
	Тематика практических занятий и лабораторных работ				
	Применение средства восстановления остаточной информации на примере Foremost или аналога		2		
	Применение специализированного программно средства для восстановления удаленных файлов		2		
	Применение программ для безвозвратного удаления данных		2		
	Применение программ для шифрования данных на съемных носителях		2		
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**				
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2			1
	Устройства Touch Memory	2			
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**				
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	1			2
	Использование сетевых снифферов в качестве СОВ	1			
	Аппаратный компонент СОВ. Программный компонент СОВ	1			
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	1			
	Тематика практических занятий и лабораторных работ				
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений		2		
Подраздел 3. Защита информации в локальных сетях					
Тема 3.1. Основы построения защищенных сетей	**Содержание**				
	Сети, работающие по технологии коммутации пакетов	1			1
	Стек протоколов TCP/IP. Особенности маршрутизации.	1			
	Штатные средства защиты информации стека протоколов TCP/IP.	1			
	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	1			
Тема 3.2. Средства организации VPN	**Содержание**				
	Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN	1			2
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	1			
	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	1			
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	1			
	Тематика практических занятий и лабораторных работ				
	Развертывание VPN		2		

Подраздел 4. Защита информации в сетях общего доступа					
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**				
	Методы защиты информации при работе в сетях общего доступа.	1			2
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall.	1			
	Уровень 1. Пакетные фильтры	1			
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	1			
	Уровень 3. Proxy-сервера прикладного уровня	1			
	Однохостовые и мультихостовые firewall.	1			
	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	1			
	Требования по сертификации межсетевых экранов	1			
	Тематика практических занятий и лабораторных работ				
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.		2		
	Изучение различных способов закрытия "опасных" портов		2		
Подраздел 5. Защита информации в базах данных					
Тема 5.1. Защита информации в базах данных	**Содержание**				
	Основные типы угроз. Модель нарушителя	1			2
	Средства идентификации и аутентификации. Управление доступом	1			
	Средства контроля целостности информации в базах данных	1			
	Средства аудита и контроля безопасности. Критерии защищенности баз данных	1			
	Применение криптографических средств защиты информации в базах данных	2			
	Тематика практических занятий и лабораторных работ				
	Изучение механизмов защиты СУБД MS Access		2		
	Изучение штатных средств защиты СУБД MSSQL Server		2		
Раздел 6. Мониторинг систем защиты					
Тема 6.1. Мониторинг систем защиты	**Содержание**				
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	1			2
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	1			

	Классификация отслеживаемых событий. Особенности построения систем мониторинга	1			
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	1			
	Классификация сетевых мониторов	1			
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	1			
	Тематика практических занятий и лабораторных работ				
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов		1		
	Проведение аудита ЛВС сетевым сканером		1		
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**				
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	2			2
	Тематика практических занятий и лабораторных работ				
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.		2		
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Тематика практических занятий и лабораторных работ**				
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов		1		2
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов		1		
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов		2		
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов		2		
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов		2		
	Самостоятельная работа при изучении раздела Изучение рекомендованной литературы. Подготовка к практическим занятиям. Оформление в виде конспекта основных положений МДК Подготовка реферативных докладов. • Создание отказоустойчивых информационных систем • Случайные угрозы • Составление схемы подсистемы защиты от несанкционированного доступа. Основные			14	

	признаки несанкционированного доступа к информации. • Оптимизация взаимодействия пользователей и обслуживающего персонала • Минимизация ущерба от аварий и стихийных бедствий • Дублирование информации • Модель защиты информации • Значение информационной безопасности для субъектов информационных отношений • Изучение принципа написания вредоносного программного кода. • Изучение алгоритма электронной цифровой подписи Эль-Гамаля. • Изучение принципа создания виртуальной машины. • Изучение принципов построения штриховых кодов. • Воздействия программных закладок на компьютеры • Защита от программных закладок • Классификация и общая характеристика программно-аппаратных средств защиты информации • Разработка схемы Парольной аутентификации.				
	Консультации	6			
	Промежуточная аттестация	8			
Раздел 2. Криптографические средства и методы защиты информации		90	50	18	
МДК 02.02 Криптографические средства защиты информации					
Введение	**Содержание**				
	Предмет и задачи криптографии. История криптографии. Основные термины	2			1
	Тематика самостоятельной работы				
	Проверочная работа по вводной лекции			2	
Подраздел 1. Математические основы защиты информации	**Содержание**				
Тема 1.1. Математические основы криптографии	Элементы теории множеств. Группы, кольца, поля.	2			2
	Делимость чисел. Признаки делимости. Простые и составные числа.	2			
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2			
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2			
	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	4			
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	2			

	Китайская теорема об остатках.	2			
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	2			
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2			
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2			
	Арифметические операции над большими числами.	2			
	Эллиптические кривые и их приложения в криптографии.	2			
	Тематика практических занятий и лабораторных работ				
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений		2		
	Проверка чисел на простоту		2		
	Решение задач с элементами теории чисел.		2		
	Тематика самостоятельной работы				
	Подготовка к проверочной работе по сравнениям			2	
	Подготовка к проверочной работе по полям			2	
Подраздел 2. Классическая криптография					
Тема 2.1. Методы криптографического защиты информации	**Содержание**				
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	**2**			2
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2			
	Методы перестановки. Табличная перестановка, маршрутная перестановка	2			
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	**2**			
	Тематика практических занятий и лабораторных работ				
	Применение классических шифров замены		2		
	Применение классических шифров перестановки		2		
	Тематика самостоятельной работы				
	Подготовка к проверочной работе по симметричному шифрованию			2	
Тема 2.2. Криптоанализ	**Содержание**				
	Основные методы криптоанализа. Криптографические атаки.	**2**			
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	**2**			
	Перспективные направления криптоанализа, квантовый криптоанализ.	2			
	Тематика практических занятий и лабораторных работ				
	Криптоанализ шифра простой замены методом анализа частотности символов		4		

	Криптоанализ классических шифров методом полного перебора ключей		4		
	Криптоанализ шифра Вижинера		2		
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**				
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	2			2
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	4			
	Тематика практических занятий и лабораторных работ				
	Применение методов генерации ПСЧ		2		
	Тематика самостоятельной работы				
	Подготовка к проверочной работе по поточному шифрованию			2	
Подраздел 3. Современная криптография	**Содержание учебного материала**				
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	2			2
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	4			
	Тематика практических занятий и лабораторных работ				
	Программная реализация классических шифров		8		
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**				
	Общие сведения. Структурная схема симметричных криптографических систем	4			2
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	4			
	Тематика самостоятельной работы			6	
	Подготовка к проверочной работе по симметричным системам шифрования				
	Подготовка к проверочной работе по стандарту шифрования DES				
	Подготовка к проверочной работе по стандарту шифрования AES				
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**				
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	2			2
	Элементы теории чисел в криптографии с открытым ключом.	2			
	Тематика практических занятий и лабораторных работ				
	Применение различных асимметричных алгоритмов.		2		
	Изучение программной реализации асимметричного алгоритма RSA		2		
	Тематика самостоятельной работы				
	Подготовка к проверочной работе по ассимметричным системам шифрования			2	

Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**				
	Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	4			2
	Тематика практических занятий и лабораторных работ				
	Применение различных функций хеширования, анализ особенностей хешей		4		
	Изучение программно-аппаратных средств, реализующих основные функции ЭП		2		
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**				
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем	2			2
	Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	4			
	Тематика практических занятий и лабораторных работ				
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.		4		
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**				
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	4			2
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	2			
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**				
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	2			2
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2			
	Тематика практических занятий и лабораторных работ				
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей		4		
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**				
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	2			2
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	2			
	Тематика практических занятий и лабораторных работ				
	Реализация простейших стеганографических алгоритмов		2		
Консультации		**6**			
Промежуточная аттестация		**2**			
Учебная практика **Виды работ**			72		

– 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 – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи				
Консультации		2		
Промежуточная аттестация		2		
Производственная практика		144		
– Знакомство с предприятием. Прохождение инструктажей по ТБ. – 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.				
Консультации		4		
Промежуточная аттестация		2		
Итого		628		

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами требует наличия кабинета информатики, лаборатории программных и программно-аппаратных средств защиты информации.

Кабинет Информатики

1. Стол преподавателя - 1 шт.
2. Столы ученические – 15 шт.
3. Стул преподавателя – 1 шт.
4. Стулья ученические - 30 шт.
5. Доска магнитная классная -1шт.
6. Персональный компьютер – 1 шт..
7. Звуковые колонки – 2 шт.
8. Проектор – 1 шт.
9. Интерактивная доска – 1 шт.
10. Экран-1шт.

Лаборатория программных и программно-аппаратных средств защиты информации:

1. Стол – рабочее место преподавателя – 1 шт.
2. Стул преподавателя (п/мягкий) – 1 шт.
3. Стол - рабочее место обучающегося для работы за
4. компьютером – 15 шт.
5. Стул п/мягкий - 15 шт.
6. Шкаф для хранения сумок, пакетов студентов -1 шт.
7. Жалюзи - 2 шт.
8. Проектор – 1 шт.
9. Экран – 1 шт.
10. Огнетушители – 1 шт.
11. Персональный компьютер – рабочее место
12. преподавателя – 1 шт.
13. Персональный компьютер – рабочее место
14. обучающегося – 15 шт.
15. Локальная сеть – есть
16. Учебный стенд "Программные средства криптографии", SCRYPTO – 1 шт

Программное обеспечение
ОС Windows 10, Visual Management Studio, Microsoft Visio, Архиватор WinRAR, Приложения MS Office 2016, Adobe Reader X, Notepad++, Google Chrome,

Консультант Плюс, MS SQL-Server, Oracle VM Virtual Box, CrypTool, ItMan, Snort и Suricata, Wireshark, Nmap Free Security Scanner, ОС Linux: Lubuntu и Kali, Linux, Cisco

Реализация рабочей программы ПМ предполагает производственную практику, которую рекомендуется проводить концентрировано.

4.2. Информационное обеспечение обучения

Основные источники

1. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для студентов высших учебных заведений / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В., Славнов. – М.: Горячая линия – Телеком, 2018г.
2. Сагдеев К.М. Физические основы защиты информации Бакалавриат: учебное пособие / Сагдеев К.М., Петренко В.И., Чипига А.Ф. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 394 с. — URL: https://book.ru/book/928736. — Текст: электронный.
3. Баранова Е.К. Криптографические методы защиты информации. Лабораторный практикум +CD: учебное пособие / Баранова Е.К., Бабаш А.В. — Москва: КноРус, 2017. — 196 с. — (для бакалавров). — ISBN 978-5-406-03802-4. — URL: https://book.ru/book/920017. — Текст: электронный.
4. Баричев С.Г. Основы современной криптографии: учебный курс для студентов высших учебных заведений / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия-Телеком, 2017г.
5. Криптографические методы защиты информации: лабораторный: практикум / сост. Калмыков И.А., Науменко Д.О., Гиш Т.А. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — URL: https://book.ru/book/928786. — Текст: электронный.

Дополнительные источники:

1. Нестандартные методы защиты информации: лабораторный: практикум / сост. Пашинцев В.П., Ляхов А.В. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 196 с. — URL: https://book.ru/book/928802. — Текст: электронный.
2. Тараскин М.М. Комплексная защита информации в организации: монография / Тараскин М.М., и др. — Москва: Русайнс, 2017. — 353 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/922538. — Текст: электронный.
3. Царегородцев А.В. Методы и средства защиты информации в государственном управлении: учебное пособие / Царегородцев А.В., Тараскин М.М. — Москва: Проспект, 2017. — 205 с. — ISBN 978-5-392-20353-6. — URL: https://book.ru/book/922352. — Текст: электронный.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студентов СПО. - М.: ИД "ФОРУМ": ИНФРА-М,

2016г
5. Мельников В.П. Информационная безопасность: учебное пособие для студентов средних профессиональных учебных заведений. - М.: Издательский центр "Академия", 2010г

Интернет- 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 htppW: /db/portal/sites/portal_page.html
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» www.law.edu.ru
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Социально-гуманитарное и политологическое образование» www.humanities.edu.ru
10. Федеральный портал «Информационно- коммуникационные технологии в образовании» htppWwww.ict.edu.ru
11. 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 учебном планом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и календарным графиком.

Образовательный процесс организуется строго по расписанию занятий, утвержденному заместителем директора. График освоения ПМ предполагает параллельное освоение МДК 02.01 Программные и программно-аппаратные средства защиты информации, МДК 02.02 Криптографические средства защиты информации, включающих в себя как теоретические, так и практические занятия.

Освоению ПМ предшествует обязательное изучение учебных дисциплин «ОП.01 основы информационной безопасности», «ОП.03 Основы алгоритмизации и программирования», «ОП.07 Технические средства информатизации».

Изучение теоретического материала может проводиться как в каждой группе, так и для нескольких групп (при наличии нескольких групп на специальности).

При проведении практических занятий проводится деление группы обучающихся на подгруппы, численностью не более 13 чел.

В процессе освоения ПМ предполагается проведение текущего и промежуточного контроля знаний, умений у студентов. Промежуточная аттестация по междисциплинарным курсам модуля является обязательной для всех обучающихся. Формой промежуточной аттестации по МДК 02.01 Программные и программно-аппаратные средства защиты информации, является дифференцированный зачет в 6 семестре, и экзамен в 7 семестре, по МДК 02.02 Криптографические средства защиты информации– дифференцированный зачет в 6 семестре. Результатом освоения ПМ выступают профессиональные компетенции, оценка которых представляет собой создание и сбор свидетельств деятельности на основе заранее определенных критериев.

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

При освоении ПМ каждым преподавателем устанавливаются часы дополнительных занятий, в рамках которых для всех желающих проводятся консультации.

Текущий учет результатов освоения ПМ производится в журнале успеваемости.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по МДК:

наличие высшего профессионального образования, соответствующего профилю специальности, стажировка по профилю специальности не реже 1 раза в 3 года.

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих проведение практических работ:

наличие высшего профессионального образования, соответствующего профилю специальности, стажировка по профилю специальности не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

наличие высшего профессионального образования, соответствующего профилю специальности, стажировка по профилю специальности не реже 1 раза в 3 года.

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

Коды проверяемых компетенций	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	**Действия** - установка и настройка программных средств защиты информации;	Практические работы
	Умения - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;	Практические работы, внеаудиторная самостоятельная работа
	Знания - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	Тестирование, устный и письменный опрос, внеаудиторная самостоятельная работа
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	**Действия** - установка и настройка программных средств защиты информации;	Практические работы
	Умения - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;	Практические работы, внеаудиторная самостоятельная работа
	Знания - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;	Тестирование, устный и письменный опрос, внеаудиторная самостоятельная работа

	– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; – основные понятия криптографии и типовых криптографических методов и средств защиты информации.	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	**Действия** – тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;	Практические работы
	Умения – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	Практические работы, внеаудиторная самостоятельная работа
	Знания – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	Тестирование, устный и письменный опрос, внеаудиторная самостоятельная работа
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	**Действия** – учет, обработка, хранение и передача информации, для которой установлен режим конфиденциальности.	Практические работы
	Умения – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – использовать типовые программные криптографические средства, в том числе электронную подпись;	Практические работы, внеаудиторная самостоятельная работа
	Знания – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – типовые модели управления	Тестирование, устный и письменный опрос, внеаудиторная самостоятельная работа

	доступом, средств, методов и протоколов идентификации и аутентификации;	
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	**Действия** - установка и настройка программных средств защиты информации;	Практические работы
	Умения - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	Практические работы, внеаудиторная самостоятельная работа
	Знания - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	Тестирование, устный и письменный опрос, внеаудиторная самостоятельная работа
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	**Действия** - установка и настройка программных средств защиты информации; - учет, обработка, хранение и передача информации, для которой установлен режим конфиденциальности.	Практические работы
	Умения - 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.	Практические работы, внеаудиторная самостоятельная работа
	Знания - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - типовые модели управления доступом, средств, методов и протоколов идентификации и	Тестирование, устный и письменный опрос, внеаудиторная самостоятельная работа

	аутентификации; - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;	

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.

Коды проверяемых компетенций	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- Распознает сложные проблемы в знакомых ситуациях. - Выделяет сложные составные части проблемы и описывает её причины и ресурсы, необходимые для её решения в целом. - Определяет потребность в информации и предпринимает усилия для её поиска. - Выделяет главные и альтернативные источники нужных ресурсов. - Разрабатывает детальный план действий и придерживается его. - Оценивает результат своей работы, выделяет в нём сильные и слабые стороны. - Качество результата решения ситуационной задачи, в целом, соответствует требованиям.	Экспертная оценка материалов учебной и производственной практик. Наблюдение за обучающимся во время теоретического, практического обучения и прохождения учебной практики. Экспертная оценка результатов решения производственной (ситуационной) задачи
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- Планирует информационный поиск из широкого набора источников, необходимого для выполнения профессиональных задач. - Проводит анализ полученной информации, выделяет в ней главные аспекты. - Структурирует отобранную информацию в соответствии с параметрами поиска. - Интерпретирует полученную информацию в контексте профессиональной деятельности.	Экспертная оценка материалов учебной и производственной практик. Экспертная оценка выполнения самостоятельной внеаудиторной работы. Наблюдение за обучающимся во время теоретического и практического обучения, прохождения учебной практики

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	– Использует актуальную нормативно-правовую документацию по специальности. – Применяет современную научно профессиональную терминологию. – Определяет траекторию профессионального развития и самообразования.	Оценка портфолио. Экспертная оценка материалов учебной и производственной практик.
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	– Участвует в деловом общении для эффективного решения деловых задач. – Планирует профессиональную деятельность.	Экспертная оценка материалов учебной и производственной практик. Наблюдение за обучающимся во время теоретического и практического обучения, прохождения учебной практики
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	– Грамотно устно и письменно излагает свои мысли по профессиональной тематике на государственном языке. – Проявляет толерантность в рабочем коллективе.	Экспертная оценка материалов учебной и производственной практик.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	– соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; – понимать значимость своей специальности; – демонстрирует поведение на основе общечеловеческих ценностей	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка документов по учебной и производственной практике
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	– эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; – использует ресурсосберегающие технологии в профессиональной деятельности, на рабочем месте	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка документов по учебной и производственной практике
ОК 9. Использовать информационные технологии в профессиональной деятельности.	– Применяет средства информатизации и информационных технологий для реализации профессиональной деятельности.	Наблюдение за обучающимся во время теоретического и практического обучения, прохождения учебной и

		производственной практики Экспертная оценка материалов учебной и производственной практик, защита индивидуального задания
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	– Применяет в профессиональной деятельности инструкции на государственном и иностранном языке. – Ведет общение на профессиональные темы. – Понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые).	Экспертная оценка материалов учебной и производственной практик