Министерство образования, науки и молодежной политики

Нижегородской области

Государственное бюджетное профессиональное образовательное учреждение

«Нижегородский радиотехнический колледж»

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

КВАЛИФИКАЦИЯ : ТЕХНИК ПО ЗАЩИТЕ ИНФОРМАЦИИ

2019г.

Рабочая программа (далее — программа) профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее - ФГОС) по специальности среднего профессионального образования ***10.02.05 Обеспечение информационной безопасности автоматизированных систем***

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение «Нижегородский радиотехнический колледж» (ГБПОУ «НРТК»)

Разработчик: _____Калентьева Е.В., преподаватель общепрофессиональных дисциплин

Рассмотрена на заседании ПЦК специальности ИТ

Протокол № 1 от 29 августа 2017 г.

Председатель ПЦК _____Калентьева Е.В.

Рекомендована Экспертным советом Государственного бюджетного профессионального образовательного учреждения «Нижегородский радиотехнический колледж».

Заключение Экспертного совета №1 от 30 августа 2017г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1.1. Цель и планируемые результаты освоения профессионального модуля

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

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

1.1.2. Общие компетенции

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	• установки, настройки программных средств защиты информации в автоматизированной системе; • обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; • тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ; • решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; • применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; • учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; • работы с подсистемами регистрации событий; • выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	• устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; • устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; • диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; • применять программные и программно-аппаратные средства для защиты информации в базах данных; • проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; • применять математический аппарат для выполнения криптографических преобразований; • использовать типовые программные криптографические средства, в том числе электронную подпись; • применять средства гарантированного уничтожения информации; • устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; • осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
знать	• особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; • методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; • типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; • основные понятия криптографии и типовых криптографических методов и средств защиты информации; • особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; • типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.2. Количество часов, отводимое на освоение профессионального модуля
Всего 586 час, из них
на освоение МДК – 370 часов, в том числе

на практики – 216 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.						Консультации
			Обучение по МДК, в час.			Практики		Самостоятельная работа	
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов		
				лабораторных и практических занятий	курсовая работа (проект), часов				
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	**Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации**	**298**	**212**	48	30	**72**	–	**10**	**4**
ПК 2.4 ОК 1-ОК 10	**Раздел 2 модуля. Применение криптографических средств защиты информации**	**180**	**134**	56	–	**36**	–	**10**	
Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)		**108**					**108**	**–**	
Промежуточная аттестация				–	–	–	–	–	
Экзамен по профессиональному модулю		–	–	–	–	–	–	–	
	Всего:	**586**	**346**	104	30	**108**	**108**	**20**	

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)**	**Объем часов**
1	2	3
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		**298**
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**186**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		42
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**	**6**
	Предмет и задачи программно-аппаратной защиты информации.	
	Основные понятия программно-аппаратной защиты информации.	
	Классификация методов и средств программно-аппаратной защиты информации.	
Тема 1.2. Стандарты безопасности	**Содержание**	**6**
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).	
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	Тематика практических занятий и лабораторных работ	**2**
	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. Обзор стандартов. Работа с содержанием стандартов.	
	Содержание	**6**
	Автоматизация процесса обработки информации. Понятие автоматизированной системы.	

Тема 1.3. Защищенная автоматизированная система	Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.	
	Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС.	
	Дискреционные модели. Мандатные модели.	
	Тематика практических занятий и лабораторных работ	**4**
	Учет, обработка, хранение и передача информации в АИС. Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации.	
	Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа. Управление политикой безопасности. Шаблоны безопасности.	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**4**
	Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию.	
	Причины и условия дестабилизирующего воздействия на информацию.	
	Тематика практических занятий и лабораторных работ	**2**
	Распределение каналов в соответствии с источниками воздействия на информацию.	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	**8**
	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.	
	Тематика практических занятий и лабораторных работ	**4**
	Организация доступа к файлам.	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД.	
Раздел 2. Защита автономных автоматизированных систем		66
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**	**8**
	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.	

Тема 2.2.Защита программ от изучения	**Содержание**	**10**
	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.	
Тема 2.3. Вредоносное программное обеспечение	**Содержание**	**10**
	Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.	
	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	
	Бот-неты. Принцип функционирования. Методы обнаружения.	
	Классификация антивирусных средств. Сигнатурный и эвристический анализ.Защита от вирусов в "ручном режиме".	
	Основные концепции построения систем антивирусной защиты на предприятии.	
	Тематика практических занятий и лабораторных работ	**2**
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО.	
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**	**6**
	Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	
	Привязка ПО к аппаратному окружению и носителям.	
	Защитные механизмы в современном программном обеспечении на примере MS Office.	
	Тематика практических занятий и лабораторных работ	**2**
	Защита информации от несанкционированного копирования с использованием специализированных программных средств. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint).	
Тема 2.5. Защита информации на машинных носителях	**Содержание**	**8**
	Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование.	
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	

	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.	
	Безвозвратное удаление данных. Принципы и алгоритмы.	
	Тематика практических занятий и лабораторных работ	**8**
	Применение средства восстановления остаточной информации на примере Foremost или аналога.	
	Применение специализированного программно средства для восстановления удаленных файлов.	
	Применение программ для безвозвратного удаления данных.	
	Применение программ для шифрования данных на съемных носителях.	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**4**
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ.	
	Устройства Touch Memory.	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**	**6**
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ.	
	Аппаратный компонент СОВ. Программный компонент СОВ.	
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	Тематика практических занятий и лабораторных работ	**2**
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений.	
Раздел 3. Защита информации в локальных сетях		18
Тема 3.1. Основы построения защищенных сетей	**Содержание**	**6**
	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.	
Тема 3.2. Средства организации VPN	**Содержание**	**10**
	Виртуальная частная сеть. Функции, назначение, принцип построения.	
	Криптографические и некриптографические средства организации VPN.	
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	

	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	
	Тематика практических занятий и лабораторных работ	**2**
	Развертывание VPN.	
Раздел 4. Защита информации в сетях общего доступа		22
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**18**
	Методы защиты информации при работе в сетях общего доступа.	
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.	
	Основные типы firewall. Симметричные и несимметричные firewall.	
	Уровень 1. Пакетные фильтры.	
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	
	Уровень 3. Proxy-сервера прикладного уровня.	
	Однохостовые и мультихостовые firewall.	
	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций.	
	Требования по сертификации межсетевых экранов.	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	
	Изучение различных способов закрытия "опасных" портов.	
Раздел 5. Защита информации в базах данных		12
Тема 5.1. Защита информации в базах данных	**Содержание**	**10**
	Основные типы угроз. Модель нарушителя.	
	Средства идентификации и аутентификации. Управление доступом.	
	Средства контроля целостности информации в базах данных.	
	Средства аудита и контроля безопасности. Критерии защищенности баз данных.	
	Применение криптографических средств защиты информации в базах данных.	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение штатных средств защиты СУБД MSSQL Server.	
Раздел 6. Мониторинг систем защиты		26
Тема 6.1. Мониторинг	**Содержание**	**10**

систем защиты	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.	
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25.	
	Классификация отслеживаемых событий. Особенности построения систем мониторинга.	
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов.	
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	Тематика практических занятий и лабораторных работ	**2**
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов. Проведение аудита ЛВС сетевым сканером.	
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	**2**
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	
	Тематика практических занятий и лабораторных работ	**2**
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Тематика практических занятий и лабораторных работ**	**10**
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов.	
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов.	
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов.	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов.	
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов.	
Курсовая работа		**30**
Примерная тематика курсовых работ		

1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах 6. Защита сред виртуализации	
Примерная тематика самостоятельной работы при изучении МДК.02.01 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты **Примерные виды самостоятельных работ при изучении раздела 1 модуля** 1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 2. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. 3. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.	**10**
Учебная практика по разделу 1 модуля **Виды работ:** • Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах • Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности • Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности • Составление документации по учету, обработке, хранению и передаче конфиденциальной информации • Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	**72**

• 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		
Раздел 2 модуля. Применение криптографических средств защиты информации		**180**
МДК.02.02. Криптографические средства защиты информации		**130**
Введение	**Содержание**	**2**
	Предмет и задачи криптографии. История криптографии. Основные термины.	
Раздел 1. Математические основы защиты информации		26
Тема 1.1. Математические основы криптографии	**Содержание**	**20**
	Элементы теории множеств. Группы, кольца, поля.	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	Китайская теорема об остатках.	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	Арифметические операции над большими числами.	
	Эллиптические кривые и их приложения в криптографии.	
	Тематика практических занятий и лабораторных работ	**6**
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений.	

	Проверка чисел на простоту.	
	Решение задач с элементами теории чисел.	
Раздел 2. Классическая криптография		32
Тема 2.1. Методы криптографического защиты информации	**Содержание**	**8**
	Классификация основных методов криптографической защиты. Методы симметричного шифрования.	
	Шифры замены. Простая замена.	
	Многоалфавитная подстановка, пропорциональный шифр.	
	Методы перестановки. Табличная перестановка, маршрутная перестановка	
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	Тематика практических занятий и лабораторных работ	**6**
	Применение классических шифров замены.	
	Применение классических шифров перестановки.	
	Применение метода гаммирования.	
Тема 2.2. Криптоанализ	**Содержание**	**6**
	Основные методы криптоанализа. Криптографические атаки.	
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса.	
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Тематика практических занятий и лабораторных работ	**6**
	Криптоанализ шифра простой замены методом анализа частотности символов.	
	Криптоанализ классических шифров методом полного перебора ключей.	
	Криптоанализ шифра Вижинера.	
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**4**
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии.	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Тематика практических занятий и лабораторных работ	**2**
	Применение методов генерации ПСЧ.	
Раздел 3. Современная криптография		70
Тема 3.1. Кодирование информации.	**Содержание учебного материала**	**6**
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.	

Компьютеризация шифрования.	Компьютеризация шифрования. Аппаратное и программное шифрование.	
	Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств.	
	Тематика практических занятий и лабораторных работ	**6**
	Кодирование информации.	
	Программная реализация классических шифров.	
	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	**4**
	Общие сведения. Структурная схема симметричных криптографических систем.	
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4.	
	Тематика практических занятий и лабораторных работ	**4**
	Изучение программной реализации современных симметричных шифров.	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**4**
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	
	Элементы теории чисел в криптографии с открытым ключом.	
	Тематика практических занятий и лабораторных работ	**4**
	Применение различных асимметричных алгоритмов.	
	Изучение программной реализации асимметричного алгоритма RSA.	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**4**
	Аутентификация данных. Общие понятия. ЭП. MAC.	
	Однонаправленные хеш-функции. Алгоритмы цифровой подписи.	
	Тематика практических занятий и лабораторных работ	**8**
	Применение различных функций хеширования, анализ особенностей хешей.	
	Применение криптографических атак на хеш-функции.	

	Изучение программно-аппаратных средств, реализующих основные функции ЭП.	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**4**
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации.	
	Взаимная аутентификация. Односторонняя аутентификация.	
	Тематика практических занятий и лабораторных работ	**6**
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	**4**
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**	**4**
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Тематика практических занятий и лабораторных работ	**4**
	Применение аутентификации по одноразовым паролям.	
	Реализация алгоритмов создания одноразовых паролей	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	**4**
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Тематика практических занятий и лабораторных работ	**4**
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ.	
	Реализация простейших стеганографических алгоритмов.	

Консультации	**4**
Примерная тематика самостоятельной работы при изучении МДК.02.02 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии **Примерные виды самостоятельной работы при изучении раздела 2 модуля** 1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 2. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	**10**
Учебная практика раздела 2 модуля **Виды работ:** • Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	**36**
Производственная практика по ПМ.02 **Виды работ** – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	**108**

– 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.	
Всего:	**586**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Лекционная аудитория, Лаборатория программных и программно-аппаратных средств защиты информации № 152, Автоматизированное рабочее место преподавателя (компьютер, проектор). Стол, стул.
автоматизированные рабочие места обучающихся (объединенные в локальную сеть с выходом в интернет), маркерная доска
Комплект ученической мебели (ученический стол, ученический стул)
Программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности, обнаружения вторжений в составе:
Учебно-лабораторный стенд «Сетевая Безопасность», Учебно-лабораторный стенд "Системы контроля доступа", Учебно-лабораторный стенд "Криптографические системы", Универсальная приемно-передающая платформа (переносная). Средство уничтожения информации в запоминающих устройствах – шредер.

3.2. Информационное обеспечение обучения

1. Бубнов А.А. Основы информационной безопасности: учебное пособие для СПО — М,: «Академия», 2016,
2. ЭОР elib.nntc.nnov.ru: Бубнов А.А. Основы информационной безопасности: учебное пособие для СПО — М,: «Академия», 2016
3. Рудаков А.В.Технология разработки программных продуктов:практикум.:учеб пособие д/студ. учреждений СПО./А.В.Рудаков, Г.Н.Федорова. - 5-еизд, стер. - М.:Изд.центр"Академия", 2014. – 192 с.,
4. ЭОР elib.nntc.nnov.ru: Рудаков А.В.Технология разработки программных продуктов:практикум.:учеб пособие д/студ. учреждений СПО./А.В.Рудаков, Г.Н.Федорова. - 5-еизд, стер. - М.:Изд.центр"Академия", 2014. – 192 с.
5. Фуфаев Э.В..Базы данных: учебное пособие для СПО — М,: «Академия», 2015, ЭОР elib.nntc.nnov.ru: Фуфаев Э.В..Базы данных: учебное пособие для СПО — М,: «Академия», 2015
6. Батаев А.В. Операционные системы и среды: учебник для системы СПО -М: «Академия», 2017
7. Федорова Г.Н. Основы проектирования баз данных : учебник для системы СПО -.М,: «Академия», 2017
8. Федорова Г.Н. Разработка модулей программного обеспечения: учебник для системы СПО -М: «Академия», 2017
9. ЭОР: elib.nntc.nnov.ru:
10. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.
11. 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
12. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью: Учебное пособие для

вузов. – 2-е изд. . испр.- М. – 2014.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации.	Тестирование. Экзамен квалификационный. Экспертное наблюдение выполнения лабораторных работ. Экспертное наблюдение выполнения практических работ. Оценка решения ситуационных задач. Оценка процесса и результатов выполнения видов работ на практике.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	
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.	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа.	
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств.	
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.	

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на лабораторно -
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен квалификационный.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- грамотность устной и письменной речи; - ясность формулирования и изложения мыслей;	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик;	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций;	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	