

приложение 1.2  
к ОПОП по специальности  
10.02.05 Обеспечение информационной  
безопасности автоматизированных систем

**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ  
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ  
СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-  
АППАРАТНЫМИ СРЕДСТВАМИ**

## **СОДЕРЖАНИЕ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО  
МОДУЛЯ**

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**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
<b>ВД 2</b>	<b>Защита информации в автоматизированных системах программными и программно-аппаратными средствами</b>
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**

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в

чрезвычайных ситуациях;

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

<b>Иметь практический опыт</b>	<ul style="list-style-type: none"><li>– установки, настройки программных средств защиты информации в автоматизированной системе;</li><li>– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;</li><li>– тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;</li><li>– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;</li><li>– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;</li><li>– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;</li><li>– работы с подсистемами регистрации событий;</li><li>– выявления событий и инцидентов безопасности в автоматизированной системе.</li></ul>
<b>уметь</b>	<ul style="list-style-type: none"><li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</li><li>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;</li><li>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li><li>– применять программные и программно-аппаратные средства для защиты информации в базах данных;</li><li>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</li><li>– применять математический аппарат для выполнения криптографических преобразований;</li><li>– использовать типовые программные криптографические средства, в том числе электронную подпись;</li><li>– применять средства гарантированного уничтожения информации;</li><li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</li><li>– 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</li></ul>

<b>знать</b>	<ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных</li> </ul>
	<p>системах, компьютерных сетях, базах данных;</p> <ul style="list-style-type: none"> <li>– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</li> <li>– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;</li> <li>– основные понятия криптографии и типовых криптографических методов и средств защиты информации;</li> <li>– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;</li> <li>– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.</li> </ul>

## **1.2. Количество часов, отводимое на освоение профессионального модуля**

Всего 504 час, из них

на освоение МДК – 342 часов,

производственная практика – 144 час.,

экзамен по профессиональному модулю – 18 ч.

## 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 общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.				Практики	
			всего, часов	в том числе			учебная практика, часов	производственная практика, часов
лабораторных и практических занятий	курсовая работа (проект), часов	Сам. работа/консультации и						
ПК 2.1 – ПК 2.6 ОК 1-ОК 9	<b>Раздел 1 модуля.</b> Применение программных и программно-аппаратных средств защиты информации	<b>256</b>	<b>184</b>	54	30	27/27	-	72
ПК 2.4 ОК 1-ОК 9	<b>Раздел 2 модуля.</b> Применение криптографических средств защиты информации	<b>230</b>	<b>158</b>	60	–	13/13	-	72
	<b>Промежуточная аттестация</b>	-	-	–	–	-	–	–
	Экзамен по профессиональному модулю	<b>18</b>	-	–	–	-	–	–
	<b>Всего:</b>	<b>504</b>	<b>342</b>	104	30	40/40	-	<b>144</b>

## 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
<b>Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации</b>		
<b>МДК.02.01. Программные и программно-аппаратные средства защиты информации</b>		
<b>Раздел 1. Основные принципы программной и программно-аппаратной защиты информации</b>		
<b>Тема 1.1.</b> Предмет и задачи программно-аппаратной защиты информации	<b>Содержание</b> ТЗ.1 Предмет и задачи программно-аппаратной защиты информации ТЗ.2 Основные понятия программно-аппаратной защиты информации ТЗ.3 Классификация методов и средств программно-аппаратной защиты информации	2 2 2
<b>Тема 1.2.</b> Стандарты безопасности	<b>Содержание</b> ТЗ.4 Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты) ТЗ.5 Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. <b>Тематика практических занятий и лабораторных работ</b> ПЗ.1 Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. ПЗ.2 Работа с содержанием нормативных правовых актов. ПЗ.3 Обзор стандартов. Работа с содержанием стандартов	2 2 2
<b>Тема 1.3.</b> Защищенная	<b>Содержание</b>	
	ТЗ.6 Автоматизация процесса обработки информации	2

автоматизированная система	Понятие автоматизированной системы.	2
	Особенности автоматизированных систем в защищенном исполнении.	
	Основные виды АС в защищенном исполнении.	
	ТЗ.7 Методы создания безопасных систем	
	Методология проектирования гарантированно защищенных КС	
	Дискреционные модели	
	Мандатные модели	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.4 Учет, обработка, хранение и передача информации в АИС	2
	Ограничение доступа на вход в систему.	2
	Идентификация и аутентификация пользователей	2
	ПЗ.5 азграничение доступа.	
	Регистрация событий (аудит).	
	Контроль целостности данных	
	ПЗ.6 Уничтожение остаточной информации.	
Управление политикой безопасности. Шаблоны безопасности		
СР.1 Криптографическая защита. Обзор программ шифрования данных	2	
СР.2 Управление политикой безопасности. Шаблоны безопасности	2	
<b>Тема 1.4.</b>	<b>Содержание</b>	
Дестабилизирующее воздействие на объекты защиты	ТЗ.8 Источники дестабилизирующего воздействия на объекты защиты	2
	ТЗ.9 Способы воздействия на информацию	2
	СР.3 Причины и условия дестабилизирующего воздействия на информацию	1
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.7,8 Распределение каналов в соответствии с источниками воздействия на информацию	2
		2
<b>Тема 1.5. Принципы программно-аппаратной защиты информации от</b>	<b>Содержание</b>	
	ТЗ.10 Понятие несанкционированного доступа к информации	2
	К.1 Основные подходы к защите информации от НСД	2

несанкционированного доступа	ТЗ.11 Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	2
	ТЗ.12 Доступ к данным со стороны процесса	
	К.2 Особенности защиты данных от изменения. Шифрование.	2 2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.9 Организация доступа к файлам	2
	ПЗ.10 Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	2
	К.3	1
<b>Промежуточная аттестация в форме контрольной работы</b>		-
<b>Итого за семестр</b>		<b>54</b>
<b>Раздел 2. Защита автономных автоматизированных систем</b>		
<b>Тема 2.1.</b> Основы защиты автономных автоматизированных систем	<b>Содержание</b>	
	ТЗ.1 Работа автономной АС в защищенном режиме	2
	Алгоритм загрузки ОС. Штатные средства замыкания среды	2
	ТЗ.2 Расширение BIOS как средство замыкания программной среды	2
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	
ТЗ.3 Применение закладок, направленных на снижение эффективности средств, замыкающих среду.		
<b>Тема 2.2.</b> Защита программ от изучения	<b>Содержание</b>	
	ТЗ.4 Изучение и обратное проектирование ПО	2
	Способы изучения ПО: статическое и динамическое изучение	2
	ТЗ.5 Задачи защиты от изучения и способы их решения	2
	Защита от отладки.	
	ТЗ.6 Защита от дизассемблирования	
	Защита от трассировки по прерываниям.	
<b>Тема 2.3.</b> Вредоносное программное обеспечение	<b>Содержание</b>	
	ТЗ.7 Вредоносное программное обеспечение как особый вид разрушающих воздействий	2

	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	2
	ТЗ.8 Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие	
	информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	
	Бот-нетты. 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	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.1 Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2
<b>Тема 2.4.</b> Защита программ и данных от несанкционированного копирования	<b>Содержание</b>	
	ТЗ.9 Несанкционированное копирование программ как тип НСД	2
	Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.	2
	ТЗ.10 Привязка ПО к аппаратному окружению и носителям.	
	Защитные механизмы в современном программном обеспечении на примере MS Office	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.2 Защита информации от несанкционированного копирования с использованием специализированных программных средств	2
Защитные механизмы в приложениях (на примере MSWord, MSEXCEL, MSPowerPoint)		
<b>Тема 2.5.</b> Защита информации на машинных носителях	<b>Содержание</b>	
	ТЗ.11 Проблема защиты отчуждаемых компонентов ПЭВМ.	2
	Методы защиты информации на отчуждаемых носителях. Шифрование.	2
	К.1 Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2
	К.2 Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	
	Безвозвратное удаление данных. Принципы и алгоритмы.	

	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.3 Применение средства восстановления остаточной информации на примере Foremost или аналога	2
	ПЗ.4 Применение специализированного программно средства для восстановления удаленных файлов	2
	ПЗ.5 Применение программ для безвозвратного удаления данных	2
	ПЗ.6 Применение программ для шифрования данных на съемных носителях	2
<b>Тема 2.6.</b> Аппаратные средства идентификации и аутентификации пользователей	<b>Содержание</b>	
	К.3 Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2
	К.4 Устройства Touch Memory	2
<b>Тема 2.7.</b> Системы обнаружения атак и вторжений	<b>Содержание</b>	
	К.5 СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	2
	Использование сетевых снифферов в качестве СОВ	2
	Аппаратный компонент СОВ	
	Программный компонент СОВ	
	К.6 Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	<b>Тематика практических занятий и лабораторных работ</b>	
ПЗ.7 Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2	
<b>Раздел 3. Защита информации в локальных сетях</b>		
<b>Тема 3.1.</b> Основы построения защищенных сетей	<b>Содержание</b>	
	К.7 Сети, работающие по технологии коммутации пакетов	2
	Стек протоколов TCP/IP. Особенности маршрутизации.	2
	Штатные средства защиты информации стека протоколов TCP/IP.	
	К.8 Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
<b>Тема 3.2.</b> Средства организации VPN	<b>Содержание</b>	
	К.9 Виртуальная частная сеть. Функции, назначение, принцип построения	2
	Криптографические и некриптографические средства организации VPN	2
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	

	К.10 Крипторouter. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.8 Развертывание VPN	2
<b>Раздел 4. Защита информации в сетях общего доступа</b>		
<b>Тема 4.1.</b> Обеспечение безопасности межсетевое взаимодействия	<b>Содержание</b>	
	К.11 Методы защиты информации при работе в сетях общего доступа.	2
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности	2
	Основные типы firewall. Симметричные и несимметричные firewall.	2
	СР.1 Уровень 1. Пакетные фильтры	2
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	
	Уровень 3. Проxy-сервера прикладного уровня	
	СР.2 Однохостовые и мультихостовые firewall.	
	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	
	СР.3 Требования по сертификации межсетевых экранов	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.9 Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	2
ПЗ.10 Изучение различных способов закрытия "опасных" портов	2	
<b>Раздел 5. Защита информации в базах данных</b>		
<b>Тема 5.1.</b> Защита информации в базах данных	<b>Содержание</b>	
	СР.4 Основные типы угроз. Модель нарушителя	2
	Средства идентификации и аутентификации. Управление доступом	2
	СР.5 Средства контроля целостности информации в базах данных	2
	Средства аудита и контроля безопасности. Критерии защищенности баз данных	
	СР.6 Применение криптографических средств защиты информации в базах данных	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.11 Изучение механизмов защиты СУБД MS Access	2
	ПЗ.12 Изучение штатных средств защиты СУБД MSSQL Server	2
<b>Раздел 6. Мониторинг систем защиты</b>		

<b>Тема 6.1.</b> Мониторинг систем защиты	<b>Содержание</b>	
	СР.7 Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	2
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2
	СР.8 Классификация отслеживаемых событий. Особенности построения систем мониторинга	
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	
	СР.9 Классификация сетевых мониторов	
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.13 Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	2
	Проведение аудита ЛВС сетевым сканером	
<b>Тема 6.2.</b> Изучение мер защиты информации в информационных системах	<b>Содержание</b>	
	СР.10 Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	2
	<b>Тематика практических занятий и лабораторных работ</b>	
<b>Тема 6.3.</b> Изучение современных программно-аппаратных комплексов.	ПЗ.14 Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.15 Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	2
	ПЗ.16 Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других	2

	аналогов	
	ПЗ.17 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	
	СР.11 Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	
<b>Промежуточная аттестация в форме защиты курсовой работы</b>		<b>30</b>
<b>Примерная тематика курсовых работ</b>		
<ol style="list-style-type: none"> <li>1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)</li> <li>2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)</li> <li>3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)</li> <li>4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)</li> <li>5. Проблема защиты информации в облачных хранилищах данных и ЦОДах</li> <li>6. Защита сред виртуализации</li> </ol>		
Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.		
<b>Итого за семестр</b>		<b>130</b>
<b>Производственная практика по разделу 1 ПП.02.01</b>		<b>72</b>
<b>ВСЕГО ПО РАЗДЕЛУ 1</b>		<b>202</b>
<b>Раздел 2 модуля. Применение криптографических средств защиты информации</b>		
<b>МДК.02.02. Криптографические средства защиты информации</b>		
<b>Введение</b>	<b>Содержание</b>	
	ТЗ.1 Предмет и задачи криптографии. История криптографии. Основные термины	2
<b>Раздел 1. Математические основы защиты информации</b>		
<b>Тема 1.1.</b>	<b>Содержание</b>	

Математические основы криптографии	ТЗ.2 Элементы теории множеств. Группы, кольца, поля.	2
	ТЗ.3 Делимость чисел. Признаки делимости. Простые и составные числа.	2
	ТЗ.4 Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2
	ТЗ.5 Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2
	ТЗ.6 Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм	2
	быстрого возведения в степень по модулю.	2
	ТЗ.7 Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	2
	ТЗ.8 Китайская теорема об остатках.	2
	ТЗ.9 Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	2
	ТЗ.10 Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2
	ТЗ.11 Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2
	ТЗ.12 Арифметические операции над большими числами.	2
	К.1 Эллиптические кривые и их приложения в криптографии.	2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.1 Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	2
	ПЗ.2 Проверка чисел на простоту	2
	ПЗ.3 Решение задач с элементами теории чисел.	2
<b>Раздел 2. Классическая криптография</b>		
<b>Тема 2.1.</b> Методы криптографического защиты информации	<b>Содержание</b>	
	К.2 Классификация основных методов криптографической защиты. Методы симметричного шифрования	2
	СР.1 Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2
	СР.2 Методы перестановки. Табличная перестановка, маршрутная перестановка	2
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.4 Применение классических шифров замены	2

	ПЗ.5 Применение классических шифров перестановки	2
	ПЗ.6 Применение метода гаммирования	2
<b>Тема 2.2. Криптоанализ</b>	<b>Содержание</b>	
	К.3 Основные методы криптоанализа. Криптографические атаки.	1
	СР.3 Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффа	1
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.7 Криптоанализ шифра простой замены методом анализа частотности символов	2
	ПЗ.8,9 Криптоанализ классических шифров методом полного перебора ключей	2
	ПЗ.10 Криптоанализ шифра Вижинера	2
<b>Промежуточная аттестация в форме контрольной работы</b>		-
<b>Итого за семестр</b>		<b>54</b>
<b>Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел</b>	<b>Содержание учебного материала</b>	
	ТЗ.1 Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	2
	ТЗ.2 Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.1 Применение методов генерации ПСЧ	2
<b>Раздел 3. Современная криптография</b>		
<b>Тема 3.1. Кодирование информации. Компьютеризация шифрования.</b>	<b>Содержание учебного материала</b>	
	ТЗ.3 Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	2
	ТЗ.4 Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств.	2
	ТЗ.5 Изучение современных программных и аппаратных криптографических средств	2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.2 Кодирование информации	2
	ПЗ.3 Программная реализация классических шифров	2
	ПЗ.4,5 Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	2
	<b>Содержание учебного материала</b>	

<b>Тема 3.2.</b> Симметричные системы шифрования	ТЗ.6 Общие сведения. Структурная схема симметричных криптографических систем	2
	ТЗ.7 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	2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.6,7 Изучение программной реализации современных симметричных шифров	2 2
<b>Тема 3.3.</b> Асимметричные системы шифрования	<b>Содержание учебного материала</b>	
	ТЗ.8 Криптосистемы с открытым ключом. СР.1 Необратимость систем. СР.2 Структурная схема шифрования с открытым ключом.	2 2 2 2
	ТЗ.9 Элементы теории чисел в криптографии с открытым ключом.	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.8 Применение различных асимметричных алгоритмов.	2
	ПЗ.9 Изучение программной реализации асимметричного алгоритма RSA	2
<b>Тема 3.4.</b> Аутентификация данных. Электронная подпись	<b>Содержание учебного материала</b>	
	ТЗ.10 Аутентификация данных. Общие понятия. ЭП. MAC. СР.3 Однонаправленные хеш-функции. ТЗ.11 Алгоритмы цифровой подписи	2 2 2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.10 Применение различных функций хеширования, анализ особенностей хешей	2
	ПЗ.11 Применение криптографических атак на хеш-функции.	2
	ПЗ.12,13 Изучение программно-аппаратных средств, реализующих основные функции ЭП	2
<b>Тема 3.5.</b> Алгоритмы обмена ключей и протоколы аутентификации	<b>Содержание учебного материала</b>	
	ТЗ.12 Алгоритмы распределения ключей с применением симметричных и асимметричных схем ТЗ.13 Протоколы аутентификации.	2 2 2
	К.1 Взаимная аутентификация.	2
	СР.4 Односторонняя аутентификация	
	<b>Тематика практических занятий и лабораторных работ</b>	

	ПЗ.14 Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2
	ПЗ.15,16 Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2 2
<b>Тема 3.6. Криптозащита информации в сетях передачи данных</b>	<b>Содержание учебного материала</b>	
	ТЗ.14 Абонентское шифрование. Пакетное шифрование.	2
	ТЗ.15 Защита центра генерации ключей.	2
	ТЗ.16 Криптомаршрутизатор. Пакетный фильтр	2
	ТЗ.17 Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	2
<b>Тема 3.7. Защита информации в электронных платежных системах</b>	<b>Содержание учебного материала</b>	
	ТЗ.18 Принципы функционирования электронных платежных систем.	2
	ТЗ.19 Электронные пластиковые карты.	2
	ТЗ.20 Персональный идентификационный номер	2
	ТЗ.21 Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.17 Применение аутентификации по одноразовым паролям.	2
	ПЗ.18 Реализация алгоритмов создания одноразовых паролей	2
<b>Тема 3.8. Компьютерная стеганография</b>	<b>Содержание учебного материала</b>	
	ТЗ.22 Скрытая передача информации в компьютерных системах.	2
	ТЗ.23 Проблема аутентификации мультимедийной информации.	2
	ТЗ.24 Защита авторских прав.	2
	К.2 Методы компьютерной стеганографии.	2
	К.3 Цифровые водяные знаки.	2
	К.4 Алгоритмы встраивания ЦВЗ	
	<b>Тематика практических занятий и лабораторных работ</b>	
	ПЗ.19 Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	2
	ПЗ.20 Реализация простейших стеганографических алгоритмов	2
<b>Промежуточная аттестация в форме дифференцированного зачета</b>		-
<b>Итого за семестр</b>		<b>104</b>

<b>Производственная практика по разделу 2 ПП.02.02</b>	<b>72</b>
<b>ВСЕГО ПО РАЗДЕЛУ 2</b>	<b>176</b>
<b>Производственная практика по ПМ.02</b> <b>Виды работ</b> – 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.	
<b>Экзамен по профессиональному модулю</b>	<b>18</b>
<b>Всего:</b>	<b>504</b>

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

Лаборатория «Программных и программно-аппаратных средств обеспечения информационной безопасности», оснащенная в соответствии с ОПОП по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

#### **3.2. Информационное обеспечение обучения**

##### **3.2.1 Основные электронные издания:**

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340>.

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/580668>.

3. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561717>.

#### 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 по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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 по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения

		ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экзамен по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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	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 по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике

компьютерных атак.		
ОК 01.Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	<ul style="list-style-type: none"> <li>– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;</li> <li>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач</li> </ul>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p> <p>Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по производственной практике</p> <p>Экзамен по профессиональному модулю</p>
ОП 02.Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	<ul style="list-style-type: none"> <li>- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач</li> </ul>	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	<ul style="list-style-type: none"> <li>- демонстрация ответственности за принятые решения</li> <li>- обоснованность самоанализа и коррекция результатов собственной работы;</li> </ul>	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	<ul style="list-style-type: none"> <li>- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями производственной практики;</li> <li>- обоснованность анализа работы членов команды (подчиненных)</li> </ul>	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	<ul style="list-style-type: none"> <li>-грамотность устной и письменной речи,</li> <li>- ясность формулирования и изложения мыслей</li> </ul>	

<p>ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;</p>	<p>- соблюдение норм поведения во время учебных занятий и прохождения производственной практике</p>	
<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении производственной практике; - знание и использование ресурсосберегающих технологий в области телекоммуникаций</p>	
<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении производственной практике;</p>	
<p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p>	<p>- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.</p>	