

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ  
УНИВЕРСИТЕТ»

**ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»**



УТВЕРЖДАЮ

Заместитель директора по УМР

Е.Ю. Кузнецов

«21» марта 2025 г.

**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

## РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 8

«20» марта 2025 г.

Председатель ПЦК  /Л.И. Логинова/

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик:

Пекунов Андрей Ананьевич, преподаватель, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (внутренний)

Кузнецов Е.Ю., преподаватель с ученой степенью кандидата технических наук, заместитель директора по УМР Высшего колледжа ПГТУ «Политехник»

Рецензент (внешний)

Морохин Дмитрий Витальевич, преподаватель с ученой степенью кандидата технических наук, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (представитель работодателя)

Петухов О.В., начальник отдела информационной безопасности АО «Марийский машиностроительный завод»

## **СОДЕРЖАНИЕ**

1. АННОТАЦИЯ
2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 1. АННОТАЦИЯ

Профессиональный модуль ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами относится к обязательной части цикла профессиональной подготовки ППССЗ СПО, устанавливающей базовые знания по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Цель изучения профессионального модуля - формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документацией по обеспечению безопасности информации.

Общий объем учебной нагрузки по профессиональному модулю составляет 634 часа, нагрузка во взаимодействии с преподавателем составляет 354 часа, самостоятельной работы – 80 часов.

Содержание профессионального модуля включает:

- изучение разделов междисциплинарного курса МДК 02.01:

1. Основные принципы программной и программно-аппаратной защиты информации
2. Защита автономных автоматизированных систем
3. Защита информации в локальных сетях
4. Защита информации в сетях общего доступа
5. Защита информации в базах данных
6. Мониторинг систем защиты

- изучение разделов междисциплинарного курса МДК 02.02:

1. Математические основы защиты информации
2. Классическая криптография
3. Современная криптография

Текущий контроль проводится в форме оценки тестирования, экспертного наблюдения за выполнением лабораторных и практических работ, оценки процесса и результатов выполнения видов работ на практике.

Форма промежуточной аттестации – дифференцированный зачет, экзамен (квалификационный).

## 2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Место профессионального модуля в структуре программы подготовки специалистов среднего звена.

Профессиональный модуль ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами относится к профессиональному учебному циклу профессиональной подготовки программы подготовки специалистов среднего звена по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

### 2.2. Цель и планируемые результаты освоения профессионального модуля.

В результате освоения профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами обучающийся должен обладать предусмотренными ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем умениями, знаниями, которые формируют следующие **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.

Освоение профессионального модуля направлено на развитие **общих компетенций**:

Код	Наименование видов деятельности и общих компетенций
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

## Результаты обучения (знания, умения, практический опыт)

В результате освоения профессионального модуля обучающийся должен:

иметь практический опыт	<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>
уметь	<ul style="list-style-type: none"> <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>
знать	<ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> </ul>

	<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>
--	---

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

Всего часов – 634 часа, в том числе:

обязательной аудиторной учебной нагрузки обучающегося–354 часа;

самостоятельной работы обучающегося– 80 часов;

на практики: учебную – 72 часа

производственную –108 часов

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Тематический план ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Код профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)								Практика	
			Обязательная аудиторная учебная нагрузка обучающегося					Самостоятельная работа обучающегося, часов	консультации часов	Промежуточная аттестация	Учебная, часов	Производственная часов
			Всего, часов	теоретическое	практические занятия, часов	лабораторные занятия, часов	в т.ч., курсовая работа (проект), часов					
1	2	3	4		5		6	7	8		9	10
ПК 2.1 – ПК 2.6 ОК 01-ОК 09	Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации										72 (2 нед)	108 (3 нед)
	МДК.02.01. Программные и программно-аппаратные средства защиты информации	240	210	112	6	62	30	28	2	-		
ПК 2.4 ОК 01-ОК 09	Раздел 2 модуля. Применение криптографических средств защиты информации											
	МДК.02.02. Криптографические средства защиты информации	196	144	88	-	56	-	52	-	-		
	Учебная практика	72	-	-	-	-	-	-	-	-		
	Производственная практика	108	-	-	-	-	-	-	-	-		
Экзамен (квалификационный)		18	-	-	-	-	-	-	-	18		
Всего:		634	354	200	6	118	30	80	2	18	72	108



### 3.2. Тематический план и содержание обучения по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент учебной дисциплины
1	2	3	
РАЗДЕЛ 1 МОДУЛЯ. ПРИМЕНЕНИЕ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ			
МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ		240	
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации			
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание учебного материала	4	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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 учебного материала	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)		
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.		
	Лабораторные занятия	6	
	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		
Тема 1.3. Защищенная автоматизированная система	Содержание учебного материала	6	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Автоматизация процесса обработки информации		
	Понятие автоматизированной системы.		
	Особенности автоматизированных систем в защищенном исполнении.		
	Основные виды АС в защищенном исполнении.		

	Методы создания безопасных систем	10	
	Методология проектирования гарантированно защищенных КС		
	Дискреционные модели		
	Мандатные модели		
	Лабораторные занятия		
	Учет, обработка, хранение и передача информации в АИС		
	Ограничение доступа на вход в систему.		
	Идентификация и аутентификация пользователей		
	Разграничение доступа.		
	Регистрация событий (аудит).		
	Контроль целостности данных		
	Уничтожение остаточной информации.		
	Управление политикой безопасности. Шаблоны безопасности		
	Криптографическая защита. Обзор программ шифрования данных		
	Управление политикой безопасности. Шаблоны безопасности		
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	Содержание учебного материала	4	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Источники дестабилизирующего воздействия на объекты защиты		
	Способы воздействия на информацию		
	Причины и условия дестабилизирующего воздействия на информацию		
	Лабораторные занятия	4	
	Распределение каналов в соответствии с источниками воздействия на информацию		
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание учебного материала	8	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Понятие несанкционированного доступа к информации		
	Основные подходы к защите информации от НСД		
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам		
	Доступ к данным со стороны процесса		
	Особенности защиты данных от изменения. Шифрование.		
	Лабораторные занятия	4	
	Организация доступа к файлам		
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		
Раздел 2. Защита автономных автоматизированных систем			
Тема 2.1. Основы	Содержание учебного материала	6	

защиты автономных автоматизированных систем	Работа автономной АС в защищенном режиме		ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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	<b>Содержание учебного материала</b>	6	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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	<b>Содержание учебного материала</b>	8	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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-нет. 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>Лабораторные занятия</b>	2	
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		
Тема 2.4. Защита программ и данных от несанкционированного копирования	<b>Содержание учебного материала</b>	4	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Несанкционированное копирование программ как тип НСД		
	Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.		
	Привязка ПО к аппаратному окружению и носителям.		
	Защитные механизмы в современном программном обеспечении на примере MS Office		
	<b>Лабораторные занятия</b>	4	

	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	<b>Содержание учебного материала</b>	8	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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.		
	<b>Лабораторные занятия</b>	4	
	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	<b>Содержание учебного материала</b>	4	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ		
	Устройства Touch Memory		
Тема 2.7. Системы обнаружения атак и вторжений	<b>Содержание учебного материала</b>	8	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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.		
	<b>Лабораторные занятия</b>		
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2	
	<b>Раздел 3. Защита информации в локальных сетях</b>		
Тема 3.1. Основы построения защищенных сетей	<b>Содержание учебного материала</b>	6	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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.		
	<b>Практические занятия</b>	4	
	Аутентификация, основанная на IP-адресе. Нетехнические меры защиты от внутренних угроз		
Тема 3.2. Средства организации VPN	<b>Содержание учебного материала</b>	6	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Виртуальная частная сеть. Функции, назначение, принцип построения		
	Криптографические и некриптографические средства организации VPN		
	Устройства, образующие VPN. Криptomаршрутизатор и криптофильтр.		
	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки		
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки		
	<b>Лабораторные занятия</b>	2	
Развертывание VPN			
<b>Раздел 4. Защита информации в сетях общего доступа</b>			
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	<b>Содержание учебного материала</b>	10	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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. Проxy-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		
	<b>Лабораторные занятия</b>	4	
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.		
	Изучение различных способов закрытия "опасных" портов		
<b>Раздел 5. Защита информации в базах данных</b>			
Тема 5.1. Защита информации в базах данных	<b>Содержание учебного материала</b>	6	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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		
	<b>Лабораторные занятия</b>	4	

	Изучение механизмов защиты СУБД MS Access		
	Изучение штатных средств защиты СУБД MSSQL Server		
Раздел 6. Мониторинг систем защиты			
Тема 6.1. Мониторинг систем защиты	Содержание учебного материала	8	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации		
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25		
	Классификация отслеживаемых событий. Особенности построения систем мониторинга		
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.		
	Классификация сетевых мониторов		
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.		
	Лабораторные занятия		
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	4	
	Проведение аудита ЛВС сетевым сканером		
	Практические занятия	2	
	Классификация инструментальных средств анализа уязвимостей		
Тема 6.2. Изучение мер защиты информации в информационных системах	Содержание учебного материала	2	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.		
	Лабораторные занятия	6	
	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.	Содержание учебного материала	4	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
	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		
	Лабораторные занятия	6	
	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		
<b>Консультации</b>		<b>2</b>	ПК 2.1 – ПК 2.6 ОК 01-ОК 09
<b>Курсовая работа</b>		<b>30</b>	
<b>Примерная тематика курсовых работ</b>			
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			
<b>Примерная тематика самостоятельной работы при изучении МДК.02.01</b>			
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		<b>28</b>	
<b>Примерные виды самостоятельных работ при изучении раздела 1 модуля</b> Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.			

РАЗДЕЛ 2 МОДУЛЯ. ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ			
МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ		196	
Введение	Содержание учебного материала	2	ПК 2.4 ОК 01-ОК 09
	Предмет и задачи криптографии. История криптографии. Основные термины		
Раздел 1. Математические основы защиты информации			
Тема 1.1. Математические основы криптографии	Содержание учебного материала	26	
	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.		
	Лабораторные занятия		
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений		
Проверка чисел на простоту			
Решение задач с элементами теории чисел.			
Раздел 2. Классическая криптография			
Тема 2.1. Методы криптографического защиты информации	Содержание учебного материала	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		
	Лабораторные занятия	6	



	Применение классических шифров замены		
	Применение классических шифров перестановки		
	Применение метода гаммирования		
Тема 2.2. Криптоанализ	Содержание учебного материала	8	ПК 2.4 ОК 01-ОК 09
	Основные методы криптоанализа. Криптографические атаки.		
	Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхoffsа		
	Перспективные направления криптоанализа, квантовый криптоанализ.		
	Лабораторные занятия	10	
	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	ПК 2.4 ОК 01-ОК 09
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии		
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.		
	Лабораторные занятия	2	
	Применение методов генерации ПСЧ		
Раздел 3. Современная криптография			
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Содержание учебного материала	6	ПК 2.4 ОК 01-ОК 09
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII		
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств		
	Лабораторные занятия		
	Кодирование информации		
	Программная реализация классических шифров		
	Изучение реализации классических шифров замены и перестановки в программе СrupTool или аналоге.		
	Тема 3.2. Симметричные системы шифрования	Содержание учебного материала	
Общие сведения. Структурная схема симметричных криптографических систем			
Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4			
Лабораторные занятия		4	
Изучение программной реализации современных симметричных шифров			

Тема 3.3. Асимметричные системы шифрования	<b>Содержание учебного материала</b>	6	ПК 2.4 ОК 01-ОК 09
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.		
	Элементы теории чисел в криптографии с открытым ключом.		
	<b>Лабораторные занятия</b>	4	
	Применение различных асимметричных алгоритмов.		
	Изучение программной реализации асимметричного алгоритма RSA		
Тема 3.4. Аутентификация данных. Электронная подпись	<b>Содержание учебного материала</b>	4	ПК 2.4 ОК 01-ОК 09
	Аутентификация данных. Общие понятия. ЭП. MAC.		
	Однонаправленные хеш-функции. Алгоритмы цифровой подписи		
	<b>Лабораторные занятия</b>	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	<b>Содержание учебного материала</b>	4	ПК 2.4 ОК 01-ОК 09
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем		
	Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация		
	<b>Лабораторные занятия</b>	4	
	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	<b>Содержание учебного материала</b>	6	ПК 2.4 ОК 01-ОК 09
	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	<b>Содержание учебного материала</b>	4	ПК 2.4 ОК 01-ОК 09
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты.		
	Персональный идентификационный номер		
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	4	
	<b>Лабораторные занятия</b>		
Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей			

Тема 3.8. Компьютерная стеганография	Содержание учебного материала	6	ПК 2.4 ОК 01-ОК 09
	Скрытая передача информации в компьютерных системах.		
	Проблема аутентификации мультимедийной информации. Защита авторских прав.		
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	2	
	Лабораторные занятия		
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ		
Реализация простейших стеганографических алгоритмов			
Примерная тематика самостоятельной работы при изучении МДК.02.02		52	ПК 2.4 ОК 01-ОК 09
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			
Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)			
Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.			
Промежуточная аттестация ПМ.02		18	
Учебная практика по разделу 1 модуля		72	ПК 2.4 ОК 01-ОК 09
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			

<ul style="list-style-type: none"> <li>- Составление документации по учету, обработке, хранению и передаче конфиденциальной информации</li> <li>- Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации</li> <li>- Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.</li> <li>- Устранение замечаний по результатам проверки</li> <li>- Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.</li> </ul> <p>Применение математических методов для оценки качества и выбора наилучшего программного средства</p> <p><b>Учебная практика по разделу 2 модуля</b></p> <p><b>Виды работ:</b></p> <p>— Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи</p>		
<p><b>Производственная практика по ПМ.02</b></p> <p><b>Виды работ</b></p> <ul style="list-style-type: none"> <li>– Анализ принципов построения систем информационной защиты производственных подразделений.</li> <li>– Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.</li> <li>– Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;</li> <li>– Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении</li> <li>– Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации</li> <li>– Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.</li> </ul>	<b>108</b>	ПК 2.4 ОК 01-ОК 09
<b>Экзамен по профессиональному модулю</b>	<b>18</b>	
<b>Всего:</b>	<b>634</b>	

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

### **4.1. Материально-техническое обеспечение профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.**

Реализация профессионального модуля требует наличия учебных кабинетов:

#### **А) Кабинет информатики.**

Оснащенность учебного кабинета:

Комплект мебели для учебного процесса

Мультимедийное оборудование: персональные компьютеры – 12 шт.(подключенные к локальной вычислительной сети и сети «Интернет»); ПК 3 - ICL RAY S902.3, монитор ViewSonic VA2038W-LED; монитор 19" ViewSonic TFT 19" VA916; системный блок P-Athlon64 X2 6000/1024\*2M6/320 Gb/ клавиатура/мышь/коврик; сканер MUSTEK Bear Paw 2400; принтер Canon LBP-1120; проектор мультимедийный Hitachi; калькуляторы.

Средства обучения: учебная доска, справочные пособия и дидактический материал, медиатека (мультимедиа разработки и презентации к урокам), экран.

#### **Перечень лицензионного программного обеспечения:**

1С: Документооборот 8 КОРП (лицензия №75027601); 1С: Предприятие 8. Комплект для обучения. (лицензия №8922961); Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); КОМПАС-3D V19 (лицензия №Вг-20-00154); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); справочная правовая система «Консультант Плюс» (контракт №2025 СВ 2 от 04.12.2024г); МойОфис Образование (договор № 2350/2017).

#### **Б) Лаборатория программных и программно-аппаратных средств защиты информации**

Оснащенность лаборатории:

Комплект мебели для учебного процесса.

Мультимедийное оборудование: персональные компьютеры – 22 шт. (подключенные к локальной вычислительной сети и сети «Интернет»); мультимедийный проектор Hitachi CP-X1250, разветвитель видеосигнала; принтер HP LaserJet Professional P1102

Средства обучения: комплект наглядных пособий «Технические средства информатизации», техническая документация на технические средства информатизации, комплект презентаций; анализатор линейных коммуникаций ULAN-2; приёмник «Скорпион» поисковый, скоростной Ver 3.5; контрольное устройство ТЕСТ-031; многофункциональный поисковый прибор ST 031; нелинейный локатор SEL SP-61/М «Катран»; указатель проводки UP-7; аппаратный комплекс АККОРД -AMD3 - 5.5; аппаратный комплекс АККОРД -AMD3 - 5MX;

аппаратный комплекс АККОРД -AMD3 — 5.5 Е; аппаратный комплекс СЗИ НСД АККОРД –AMD; генератор шума ГШ-2500; комплекс защиты информации в составе PCI-плата, ПО SN-5, считыватель, 2 идентификатора; комплекс защиты информации Secret Net 5.0; комплекс защиты информации Secret Net 5.0; комплекс защиты информации Secret Disc 4.0; система вибро-акустической защиты «Соната-AB»; устройство защиты «Соната-PC2»; устройство защиты «Соната-P2»; виброизлучатель ВИ-45 – 5шт.; адаптер DWA-160-10 шт; DAP-2310 – 5шт.; DES-3200-28 – 8шт.; DES-3810-28 -2шт.; коммутатор D-Link DES-1005 – 5шт.; коммутатор D-Link DIR-615 – 5 шт.; коммутатор D-Link DES-1100-16 -5 шт.; кримпер NT-2008AR; кабельный тестер NCT-1; тестер кабельный TC-NT2; SMART-Card Алладин – 2шт; ASEDive IIIe V2C- 2 шт.; электронный ключ eToken – 8шт.; ПСКЗИ «Шипка 2.0» (диск + УСБ-устройство) -5шт; подсистема распределённого аудита и управления «Аккорд-РАУ» (2 CD + ТМ ключ DS-1996); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (3 CD); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (2 CD)- 3 шт; программно-аппаратный комплекс «Соболь» ( PCI- плата,CD-диск ПО, соединитель) – 3 шт., экран настенный 200\*200см Braun Roll Vision.

**Перечень лицензионного программного обеспечения:**

Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); антивирусный программный комплекс: Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); программные и программно-аппаратные средства обнаружения вторжений (Snort 2.9 (свободно распр. ПО), Nmap 7.8 (свободно распр. ПО)); средства уничтожения остаточной информации в запоминающих устройствах («СГУ–2» демоверсия (свободно распр. ПО)); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); справочная правовая система «Консультант Плюс» (контракт №2025 СВ 2 от 04.12.2024г); программные средства выявления уязвимостей в АС и СБТ (Tenable Nessus® vulnerability scanner (свободно распр. ПО), Metasploit Framework (свободно распр. ПО); программные средства криптографической защиты информации (КриптоПро CSP 5.0 (Лицензионный контракт №010/IO20-002792 от 28.08.20), VipNet CSP 4 (свободно-распространяемое); программные средства защиты среды виртуализации (VM Monitor (свободно распр. ПО), Zabbix (свободно распр. ПО).

**Договоры о практической подготовке:**

- АО «Марийский машиностроительный завод» Договор № 1/2021 от 01.02.2021 – бессрочный
- Филиал ПАО «Ростелеком» в Республике Марий Эл Договор № 83/2021 от 27.01.2021 - бессрочный

## 4.2. Информационное обеспечение профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

### Основная и дополнительная литература

№ п/п	Список используемой литературы (печатные издания, электронные издания за последние 5 лет)	Количество экземпляров, имеющихся в библиотеке, или ссылка на ЭБС
<b>ОСНОВНАЯ ЛИТЕРАТУРА</b>		
1.	<b>Краковский, Ю. М.</b> Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/156401">https://e.lanbook.com/book/156401</a>	Электронный ресурс
2.	<b>Прохорова, О. В.</b> Информационная безопасность и защита информации / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-47174-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/336200">https://e.lanbook.com/book/336200</a>	Электронный ресурс
3.	<b>Петров, А. А.</b> Компьютерная безопасность. Криптографические методы защиты : практическое руководство / А. А. Петров. - 2-е изд. - Москва : ДМК Пресс, 2023. - 451 с. - ISBN 978-5-89818-453-7. - Текст: электронный. - URL: <a href="https://znanium.com/catalog/product/2106222">https://znanium.com/catalog/product/2106222</a>	Электронный ресурс
<b>ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА</b>		
1.	<b>Душкин, А. В.</b> Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под. ред. А. В. Душкина. - Москва, 2022. - 248 с. - ISBN 978-5-9912-0470-5. - Текст: электронный. - URL: <a href="https://znanium.com/catalog/product/1911635">https://znanium.com/catalog/product/1911635</a>	Электронный ресурс
2.	<b>Крамаров, С.О.</b> Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: <a href="https://znanium.com/catalog/product/1899016">https://znanium.com/catalog/product/1899016</a>	Электронный ресурс

## **5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в форме текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по профессиональному модулю за период обучения. Форма промежуточной аттестации - дифференцированный зачет, экзамен, экзамен (квалификационный).

Текущий контроль успеваемости осуществляется в процессе проведения практических занятий и лабораторных работ, обеспечивает оценивание хода освоения модуля.

Формы текущего контроля успеваемости: тестирование, устный опрос, доклады, выполнение практических и лабораторных работ.



№	Наименование темы	Код формируемой компетенции	Результаты обучения по профессиональному модулю		Формы контроля
			уметь	знать	
МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ					
1.	Предмет и задачи программно-аппаратной защиты информации	ОК 01-ОК 09 ПК 2.1-ПК.2.3	–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	–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Тестирование
2.	Стандарты безопасности	ОК 01-ОК 09 ПК 2.1-ПК.2.3	–устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; –проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; –устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Тестирование Выполнение лабораторных работ.
3.	Защищенная автоматизированная система	ОК 01-ОК 09 ПК 2.1-ПК.2.4	–устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; –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; –устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	–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; –особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике

4.	Дестабилизирующее воздействие на объекты защиты	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <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>–проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>–устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> </ul>	<ul style="list-style-type: none"> <li>–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</li> </ul>	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
5.	Принципы программно-аппаратной защиты информации от несанкционированного доступа	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <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>–проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>–устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> </ul>	<ul style="list-style-type: none"> <li>–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты 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>	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
6.	Основы защиты автономных автоматизированных систем	ОК 01-ОК 09 ПК 2.1-ПК.2.6	<ul style="list-style-type: none"> <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> </ul>	<ul style="list-style-type: none"> <li>–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>–методы тестирования функций отдельных программных и</li> </ul>	Тестирование

			<ul style="list-style-type: none"> <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>	<ul style="list-style-type: none"> <li>программно-аппаратных средств защиты 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>	
7.	Защита программ от изучения	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <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>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации</li> </ul>	<ul style="list-style-type: none"> <li>–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты 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>	Тестирование
8.	Вредоносное программное обеспечение	ОК 01-ОК 09 ПК 2.1-ПК.2.6	<ul style="list-style-type: none"> <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>–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</li> </ul>	<ul style="list-style-type: none"> <li>–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации</li> </ul>	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике

			программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак		
9.	Защита программ и данных от несанкционированного копирования	ОК 01-ОК 09 ПК 2.1-ПК.2.6	<ul style="list-style-type: none"> <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>–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</li> </ul>	<ul style="list-style-type: none"> <li>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</li> <li>–особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации</li> </ul>	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
10.	Защита информации на машинных носителях	ОК 01-ОК 09 ПК 2.1-ПК.2.6	<ul style="list-style-type: none"> <li>–диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li> <li>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности 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>	<ul style="list-style-type: none"> <li>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</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> </ul>	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
11.	Аппаратные средства идентификации и аутентификации пользователей	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <li>–диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li> <li>– проверять выполнение требований по защите</li> </ul>	<ul style="list-style-type: none"> <li>–типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;</li> <li>–особенности и способы применения</li> </ul>	Тестирование

			информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; –устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	программных и программно-аппаратных средств гарантированного уничтожения информации	
12.	Системы обнаружения атак и вторжений	ОК 01-ОК 09 ПК 2.1-ПК.2.6	–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; –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	–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; –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	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
13.	Основы построения защищенных сетей	ОК 01-ОК 09 ПК 2.1-ПК.2.6	–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; –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	–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; –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	Тестирование, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

			средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	доступа	
14.	Средства организации VPN	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <li>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li> <li>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>– применять средства гарантированного уничтожения информации;</li> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> </ul>	<ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>– основные понятия криптографии и типовых криптографических методов и средств защиты 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>	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
15.	Обеспечение безопасности межсетевого взаимодействия	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <li>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li> <li>– применять средства гарантированного уничтожения информации;</li> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> </ul>	<ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>– основные понятия криптографии и типовых криптографических методов и средств защиты 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>	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
16.	Защита информации в базах данных	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <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</li> </ul>	<ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> </ul>	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения

			<p>требованиям безопасности информации;</p> <p>–применять средства гарантированного уничтожения информации</p>	<p>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</p> <p>–типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа</p>	<p>лабораторных работ, оценка процесса и результатов выполнения видов работ на практике</p>
17.	Мониторинг систем защиты	ОК 01-ОК 09 ПК 2.1-ПК.2.6	<p>–проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</p> <p>–устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</p> <p>–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</p>	<p>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</p> <p>–типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа</p>	<p>Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
18.	Изучение мер защиты информации в информационных системах	ОК 01-ОК 09 ПК 2.1-ПК.2.6	<p>–проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</p> <p>–применять средства гарантированного уничтожения информации;</p> <p>–устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</p> <p>–осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных</p>	<p>–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</p> <p>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации</p>	<p>Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике</p>

			средств обнаружения, предупреждения и ликвидации последствий компьютерных атак		
19.	Изучение современных программно-аппаратных комплексов.	ОК 01-ОК 09 ПК 2.1-ПК.2.4	<ul style="list-style-type: none"> <li>–проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>–применять средства гарантированного уничтожения информации;</li> <li>–устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> </ul>	<ul style="list-style-type: none"> <li>–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>–особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации</li> </ul>	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике



№	Наименование темы	Код формируемой компетенции	Результаты обучения по профессиональному модулю		Формы контроля
			уметь	знать	
МДК. 02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ					
1.	Математические основы криптографии	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства, в том числе электронную подпись	–основные понятия криптографии и типовых криптографических методов и средств защиты информации	Тестирование
2.	Методы криптографичес кого защиты информации	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства	–основные понятия криптографии и типовых криптографических методов и средств защиты информации	Тестирование Выполнение лабораторных работ.
3.	Криптоанализ	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства ликвидации последствий компьютерных атак	–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	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
4.	Поточные шифры и генераторы псевдослучайны х чисел	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	–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	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике

5.	Кодирование информации. Компьютеризация шифрования.	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства	–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	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
6.	Симметричные системы шифрования	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства ликвидации последствий компьютерных атак	–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	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
7.	Асимметричные системы шифрования	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства	–особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; –основные понятия криптографии и типовых криптографических методов и средств защиты информации	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
8.	Аутентификация данных. Электронная подпись	ОК 01-ОК 09 ПК 2.4	–применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства ликвидации	–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; –типовые модели управления доступом, средств, методов и протоколов	Тестирование, экзамен квалификационный, экспертное

			<p>последствий компьютерных атак</p> <p>–использовать типовые программные криптографические средства, в том числе электронную подпись;</p>	<p>идентификации и аутентификации;</p> <p>–основные понятия криптографии и типовых криптографических методов и средств защиты информации</p>	<p>наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике</p>
9.	Алгоритмы обмена ключей и протоколы аутентификации	ОК 01-ОК 09 ПК 2.4	<p>–применять математический аппарат для выполнения криптографических преобразований;</p> <p>–использовать типовые программные криптографические средства, в том числе электронную подпись;</p> <p>–применять средства гарантированного уничтожения информации</p>	<p>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</p> <p>–типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;</p> <p>–основные понятия криптографии и типовых криптографических методов и средств защиты информации</p>	<p>Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике</p>
10.	Криптозащита информации в сетях передачи данных	ОК 01-ОК 09 ПК 2.4	<p>–применять математический аппарат для выполнения криптографических преобразований;</p> <p>–использовать типовые программные криптографические средства, в том числе электронную подпись;</p> <p>–применять средства гарантированного уничтожения информации</p>	<p>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</p> <p>–основные понятия криптографии и типовых криптографических методов и средств защиты информации</p> <p>–типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа</p>	<p>Тестирование, экзамен квалификационный</p>
11.	Защита информации в электронных платежных	ОК 01-ОК 09 ПК 2.4	<p>–устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;</p> <p>–применять математический аппарат для выполнения криптографических</p>	<p>–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</p> <p>–основные понятия криптографии и типовых криптографических методов и средств</p>	<p>Тестирование, экзамен квалификационный, экспертное</p>

	системах		преобразований; –использовать типовые программные криптографические средства, в том числе электронную подпись; –применять средства гарантированного уничтожения информации	защиты информации –типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике
12.	Компьютерная стеганография	ОК 01-ОК 09 ПК 2.4	–устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; –применять математический аппарат для выполнения криптографических преобразований; –использовать типовые программные криптографические средства, в том числе электронную подпись; –применять средства гарантированного уничтожения информации	–методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; –основные понятия криптографии и типовых криптографических методов и средств защиты информации –типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практике

## **Критерии оценивания результатов обучения по профессиональному модулю, шкала оценивания.**

### Критерии оценивания:

- усвоение программного теоретического материала (объем знаний, глубина усвоения);
- умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания на практике.

### Шкала оценивания:

Результаты сдачи дифференцированного зачета, экзамена, экзамена (квалификационного) оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, который глубоко и прочно усвоил программный материал, проявляет знание основной и дополнительной литературы, грамотно, логически стройно и аргументировано излагает материал, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с практическими заданиями.

Оценка «хорошо» выставляется обучающемуся, твердо знающему программный материал, который излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, не испытывает затруднений с ответами на вопросы.

Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

## Дополнения и изменения к рабочей программе на учебный год

Дополнения и изменения к рабочей программе на \_\_\_\_\_ учебный год по профессиональному модулю \_\_\_\_\_

В рабочую программу внесены следующие изменения:

---

---

---

---

---

Дополнения и изменения в рабочей программе обсуждены на заседании ПЦК

\_\_\_\_\_

«\_\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г. (протокол № \_\_\_\_\_).

Председатель ПЦК \_\_\_\_\_ / \_\_\_\_\_ /