МИНОБРНАУКИ РОССИИ
Старооскольский геологоразведочный институт
(филиал) федерального государственного бюджетного образовательного учреждения высшего образования
«Российский государственный геологоразведочный университет имени Серго Орджоникидзе»
(СГИ МГРИ)

УТВЕРЖДАЮ
Директор СГИ-МГРИ
_____ С. И. Двоеглазов
«06» 03 2024 г.

СОГЛАСОВАНО
Заместитель директора по СПО
_____ Е. А. Мищенко
«06» 03 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

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

г. Старый Оскол
2024 г.

Рабочая программа профессионального модуля. **ПМ02. Защита информации в автоматизированных системах программными и программноаппаратными средствами** разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного Приказом Минпросвещения России от 9 декабря 2016 года № 1553.

Организация-разработчик: Старооскольский геологоразведочный институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный геологоразведочный университет имени Серго Орджоникидзе»

Разработчик:

преподаватель СГИ МГРИ

РАССМОТРЕНА И ОДОБРЕНА

Протокол № 2 от «28» февраля 2024 г.

На заседании учебно-методического отдела СГИ МГРИ

СОДЕРЖАНИЕ

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

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной образовательной программы в соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида профессиональной деятельности (ВПД): Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

1.2. Место дисциплины в структуре образовательной программы

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программноаппаратными средствами, входит в профессиональный учебный цикл.

Особое значение профессиональный модуль имеет при формировании и развитии общих компетенций (ОК 01 - 10), профессиональных компетенций (ПК 2.1 – 2.6).

1.3. Планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающихся должен освоить основной вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему общие компетенции, и профессиональные компетенции:

1.3.1. Перечень общих компетенций

Код	***Наименование общих компетенций***
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения

ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
ОК 09.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках

1.3.2. Перечень профессиональных компетенций

Код	*Наименование видов деятельности и профессиональных компетенций*
ВД 2	Осуществлять установку и настройку отдельных программных, программноаппаратных средств защиты информации
ПК 2.1.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.2.	Осуществлять тестирование функций отдельных программных и программноаппаратных средств защиты информации
ПК 2.3.	Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.4.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.5.	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
ПК 2.6.	Осуществлять установку и настройку отдельных программных, программноаппаратных средств защиты информации

1.3.4. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	-установка, настройка программных средств защиты информации в автоматизированной системе; -обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети; -тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации; -решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;

	-учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности; работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе
Уметь	-устанавливать, настраивать, применять программные и программноаппаратные средства защиты информации; -устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; -диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; -применять программные и программно-аппаратные средства для защиты информации в базах данных; -проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; -применять математический аппарат для выполнения криптографических преобразований; -использовать типовые программные криптографические средства, в том числе электронную подпись; -уметь работать со средствами электронной подписи; уметь производить установку и монтаж систем и средств защиты информации, в том числе СКЗИ, в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами; -производить настройку программных, программно-аппаратных средств применять средства гарантированного уничтожения информации; устанавливать, настраивать, применять программные и программноаппаратные 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; -уметь работать со средствами электронной подписи выбирать способы решения задач профессиональной деятельности осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации

Знать	-основные нормативно-правовые законы в области защиты информации и информационной безопасности; -особенности и способы применения программных и программноаппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; -методы тестирования функций отдельных программных и программноаппаратных 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; методологию работы со средствами криптографической защиты информации; особенности и способы применения программных и программноаппаратных средств гарантированного уничтожения информации; типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. Знать основные нормативно-правовые законы в области защиты информации и информационной безопасности Знать источники официальной нормативно-правовой информации по защите информации программно-аппаратными СЗИ, а также сайты производителей Знать особенности и способы применения программных и программноаппаратных средств защиты информации Знать требования к сертифицированным средствами защиты информации, порядок их применения Знать методологию работы со средствами криптографической защиты информации Знать основные нормативно-правовые законы в области защиты информации и информационной безопасности Знать источники официальной нормативно-правовой информации по защите информации программно-аппаратными СЗИ, а также сайты производителей Знать особенности и способы применения программных и программноаппаратных средств защиты информации Знать требования к сертифицированным средствами защиты информации, порядок их применения Знать методологию работы со средствами криптографической защиты информации

1.4. Количество часов, отводимое на освоение профессионального модуля

Объем часов**: 661 *ч.,***
в том числе в форме практической подготовки *568 ч.*
из них на освоение: - МДК ***211*** *ч.;*
практики:

- учебная практика *108 ч.;*
- производственная практика *324 ч.;*
- промежуточная аттестация, в форме *экзамена по модулю – 18 ч..*

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНОАППАРАТНЫМИ СРЕДСТВАМИ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций и личностных результатов, формированию которых способствует элемент программы	**Наименования разделов профессионального модуля**	Всего, час.	В том числе практич. подготовки	**Объем профессионального модуля, ак. час.**						
				Обучение по МДК					**Практики**	
					В том числе					
				Всего	**Лабораторных, и практических занятий**	**Курсовых работ (проектов)**	**Самостоятельная работа**	**Промежуточная аттестация**	**Учебная**	**Производственная**
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОК 1-10 ПК 2.1-2.6	МДК.02.01 Программные и программно-аппаратные средства защиты информации	112	86	112	50	36		Дз		
	МДК.02.02 Криптографические средства защиты информации	**99**	54	99	54		15	дз		
	Учебная практика	108	108						*108*	
	Производственная практика, часов	324	324							324

	Консультации	6								
	Промежуточная аттестация	18						18		
	Всего:	667	*568*	*661*	*104*	*36*	*15*	*18*	*108*	*324*

2.2. Тематический план и содержание профессионального модуля защита информации в автоматизированных системах программными и программно-аппаратными средствами

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, акад. ч / в том числе в форме практической подготовки, ак. ч
1		**3**
Раздел 1. ПМ2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		
МДК. 02.01 Программные и программно-аппаратные средства защиты информации		**112**
Раздел 1. Использование операционных систем специального назначения		
Тема 1.1 Предмет и задачи программноаппаратной защиты информации	**Содержание учебного материала**	**4**
	Основные понятия программно-аппаратной защиты информации *Предмет и задачи программно-аппаратной защиты информации*	2
	Стандарты безопасности *Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.*	2
Тема 1.2 Эксплуатация операционных систем в защищённом исполнении	**Содержание учебного материала**	**28**
	Понятие защищённой (доверенной) операционной системы *Архитектура, назначение и области применения ОССН*	2
	Основы пользовательской работы и администрирования в ОССН *Варианты загрузки, экраны входа и выхода из ОССН. Основные приемы работы с графической подсистемой fly. Основные задачи администрирования*	2
	Дискреционное управление доступом *Учетные записи пользователей и групп. Аутентификация пользователей с использованием механизма PAM. Файлы, каталоги и дискреционные права доступа к ним. Механизмы расширения дискреционного управления доступом «Киоск-2»*	2

	Мандатный контроль целостности *Общий подход к реализации мандатного контроля целостности. Администрирование параметров мандатного контроля целостности. Статистический контроль целостности (неизменности) файлов и замкнутая программная среда*	2
	Мандатное управление доступом	2
	Общий подход к реализации мандатного управления доступом. Администрирование параметров мандатного управления доступом учётных записей пользователей и процессов. Администрирование параметров мандатного управления доступом файлов и каталогов	
	Управление безопасностью операционной системы специального назначения *Мандатный контроль целостности. Мандатное управление доступом. Механизм замкнутой программной среды. Использование системных и графических киосков*	2
	В том числе лабораторных и практических занятий	
	Практическое занятие №1 *Управление учетными записями пользователей и групп*	2
	Практическое занятие №2 *Организация совместной работы с фалами и каталогами с помощью общей группы*	2
	Практическое занятие №3 *Организация совместной работы с файлами и каталогами с помощью списков управления доступом. Использование дополнительных атрибутов файловой системы и привилегий для ограничения производимых с файлами операций*	2
	Практическое занятие №4 *Использование механизмов «Киоск-2» и «Графический киоск» для расширения возможностей администрирования дискреционного управления доступом*	2
	Практическое занятие №5 *Использование мандатного контроля целостности для администрирования ОССН*	2
	Практическое занятие №6 *Организация файловой системы в рамках мандатного контроля целостности*	2
	Практическое занятие №7 *Использование мандатного и дискреционного управления доступом для организации совместной работы с файлами и каталогами*	2
	Практическое занятие №8 *Настройка ОССН для безопасной работы в соответствии с требованиями по защите информации Astra Red Book*	2
Раздел 2 Защита автоматизированных систем программными и программно-аппаратными средствами		**80**
Тема 2.1 Защита информации от несанкционированного доступа	**Содержание учебного материала**	**16**
	Средства защиты информации от несанкционированного доступа *Назначение и возможности. Разграничение доступа, , контроль целостности файловой системы, аудит действий пользователей* **Аппаратно-программные модули доверенной загрузки**	2
	В том числе лабораторных и практических занятий	

	Практическое занятие №9 *Установка СЗИ от НСД Secret Net Studio*	2
	Практическое занятие №10 *Настройка политик безопасности для Secret Net Studio*	2
	Практическое занятие №11 *Настройка аудита операционной системы и событий Secret Net Studio*	2
	Практическое занятие №12 *Работа с журналом событий Secret Net Studio*	2
	Практическое занятие №13 *Настройка механизма дискреционного управления доступом с помощью. Secret Net Studio*	2
	Практическое занятие №14 *Настройка механизма замкнутой программной среды в Secret Net Studio*	2
	Практическое занятие №15 *Ограничение трафика на переходы по определенным портам в Secret Net Studio*	2
Тема 2.2 Антивирусная защита	**Содержание учебного материала**	**6**
	Защита от вредоносных программ и спама *Классификация вредоносных программ. Основы работы антивирусных программ*	2
	В том числе лабораторных и практических занятий	
	Практическое занятие №16 *Установка и настройка антивирусного программного обеспечение*	2
	Практическое занятие № 17 *Применение средств исследования реестра Windows для нахождения следов активности вредоносного ПО*	2
Тема 2.3 Обеспечение безопасности межсетевого взаимодействия	**Содержание учебного материала**	**14**
	Методы защиты информации при работе в сетях общего доступа. *Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности*	2
	Нормативно-правовые требования к межсетевым экранам для защиты персональных данных *Применение МЭ в информационной системе персональных ПДн. Профили защиты межсетевых экранов для защиты персональных данных*	2
	В том числе лабораторных и практических занятий	
	Практическое занятие №18 *Установка межсетевого экрана. Развертывание виртуальной машины*	2
	Практическое занятие №19 *Первоначальная настройка МЭ. Подключение к веб-интерфейсу. Настройка подключения к интернет-провайдеру*	2
	Практическое занятие №20 *Настройка правила трафика. Контент-фильтр.*	2
	Практическое занятие №21 *Установка программно-аппаратного комплекса для построения виртуальных защищенных сетей*	2
	Практическое занятие № 22 *Методы анализа сетевого трафика с использованием WireShark*	2
Тема 2.4.	**Содержание учебного материала**	**6**
	В том числе лабораторных и практических занятий	

Средства анализа и контроля защищенности информации	**Практическое занятие № 23** *Установка сервера средства анализа защищенности в качестве виртуальной машины*	2
	Практическое занятие № 24 *Создание и управление проектами. Тестирование защищенности*	2
	Практическое занятие № 25 *Использование инструментария локальной версии. Локальный аудит паролей. Поиск остаточной информации. Гарантированное уничтожение информации*	2
Дифференцированный зачет		**2**
Курсовое проектирование	**Содержание учебного материала**	**36**
	1. Составление плана курсовой работы	2
	2. Выявление цели и задач курсовой работы	2
	3. Выявление предмета и объекта курсовой работы	2
	4. Выявление характеристики структуры курсовой работы	2
	5. Выявление обоснования актуальности темы	2
	6. Подбор нормативных источников по разделу курсовой работы	2
	7. Подбор методических источников по разделу курсовой работы	2
	8. Подбор материала для первого раздела курсовой работы	2
	9. Логичное распределение материала внутри раздела курсовой работы	2
	10. Подбор материала для второго раздела курсовой работы	2
	11. Логичное распределение материала внутри раздела курсовой работы	2
	12. Систематизация материала внутри раздела курсовой работы	2
	13. Формирование заключения курсовой работы	2
	14. Проверка оформления курсовой работы	2
	15. Проверка оформления списка используемых источников и приложения	2
	16. Оформление презентации к защите курсовой работы	2
	17. Подготовка речи к защите курсовой работы	2
	18. Проведение предзащиты курсовой работы	2
МДК.02.02. Криптографические средства защиты информации		**99**
Введение	Основные термины и определения в области криптографии. Предмет и задачи криптографии. История криптографии.	2
Тема 1.1. Математические основы криптографии	**Содержание учебного материала**	**32**
	Элементы теории множеств. Группы, кольца, поля.	1
	Делимость чисел. Признаки делимости. Простые и составные числа. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	1

	Отношения сравнимости. Свойства сравнений. Модулярная арифметика. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	2
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. Китайская теорема об остатках.	2
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена. Разложение числа на множители. Алгоритмы факторизации	2
	В том числе лабораторных и практических занятий	**24**
	Практическое занятие № 1 Решение задач с простыми и составными числами. Применение алгоритма Евклида для нахождения НОД.	2
	Практическое занятие № 2. Решение задач модулярной арифметики	6
	Практическое занятие № 3 Решение сравнений первой степени и линейных диофантовых уравнений.	4
	Практическое занятие № 4 Проверка чисел на простоту	4
	Практическое занятие № 5. Решение задач с элементами теории чисел	4
	Практическое занятие № 6 Программная реализация математических основ криптографии	4
	Содержание учебного материала	**8**
Тема 2.1. Методы криптографической защиты информации	Классификация основных методов криптографической защиты. Методы симметричного шифрования. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2
	Методы перестановки. Табличная перестановка, маршрутная перестановка. Гаммирование. Гаммирование с конечной и бесконечной гаммами	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 7. Применение классических шифров замены	2
	Практическое занятие № 8. Применение классических шифров перестановки. Применение метода гаммирования	2
Тема 2.2. Криптоанализ	**Содержание учебного материала**	**4**
	Основные методы криптоанализа. Криптографические атаки. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффсаю Перспективные направления криптоанализа, квантовый криптоанализ.	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 9. Криптоанализ шифра простой замены методом анализа частотности символов. Криптоанализ классических шифров методом полного перебора ключей. Криптоанализ шифра Вижинера	2
	Содержание учебного материала	**6**

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии. Методы получения псевдослучайных последовательностей (ПСП): ЛКГ, метод Фибоначчи, метод BBS, методы на основе теории динамического хаоса. Методы оценки свойств ПСП: тесты NIST, автокорреляционная функция, спектр, линейная сложность, показатель Херста, корреляционная энтропия	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 10. Применение методов генерации ПСП	2
	Практическое занятие № 11. Оценка свойств ПСП	2
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**6**
	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. Основы нормативно-правового обеспечения криптографической защиты информации в Российской Федерации	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 12. Программная реализация классических шифров. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	2
	Практическое занятие № 13 Изучение основ нормативно-правового обеспечения криптографической защиты информации в Российской Федерации	2
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	**8**
	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.	2
	Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 14. Изучение программной реализации современных симметричных шифров	2
	Практическое занятие № 15. Изучение программной реализации современных симметричных шифров	2
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**6**
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом.	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 16. Применение различных асимметричных алгоритмов.	2
	Практическое занятие № 17. Изучение программной реализации асимметричного алгоритма RSA	2
Тема 3.4.	**Содержание учебного материала**	**6**

Аутентификация данных. Электронная подпись	Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи.	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 18. Изучение программно-аппаратных средств, реализующих основные функции ЭП	2
	Практическое занятие № 19. Изучение программно-аппаратных средств, реализующих основные функции ЭП	2
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**6**
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем. Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	2
	В том числе лабораторных и практических занятий	
	Практическое занятие № 20. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2
	Практическое занятие № 21. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2
Самостоятельная работа: Изучение и работа со стандартами ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. **Подготовка к защите практических работ**		15
Дифференцированный зачет		2
УП. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	**Виды работ** 1. Инструктаж по технике безопасности 2. Установка ПО в соответствии с документацией. Проведение регламентных работ при установке ПО. Конфигурирование системного программного обеспечения 3. Разработка групповой политики безопасности. Конфигурирование автоматизированной системы. Текущий контроль, контроль целостности подсистем ОС. 4. Настройка аппаратных комплексов и подсистем защиты информации операционных систем 5. Установка обновления программного обеспечения. Установка виртуальных ОС для развертывания InfoWatch TM. 6. Установка ПО на виртуальных машинах. 7. Установка сетевых операционных систем. 8. Настройка сетевых операционных систем 9. Конфигурирование КС 10. Выполнение тестирование коммутации КС. Анализ настройки аппаратных компонентов 11. Тестирование аппаратных компонентов ЗИ 12. Тестирование параметров сетевых протоколов.	**108**

	13. Проведение диагностики ПАСЗИ 14. Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи конфиденциальной информации. 15. Использование специализированного ПО для обработки конфиденциальной информации 16. Аттестация систем хранения, обработки и передачи информации 17. Сертификация систем хранения, обработки и передачи информации 18. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем. Применение программных комплексов по уничтожению остаточной информации. 19. Применение аппаратных средств для уничтожения носителей информации 20. Организация учета носителей конфиденциальной информации 21. Составления регламентов обслуживания ИС 22. Определение работоспособности ПАСЗИ. 23. Выявление и устранение событий ИС средствами ПАСЗИ 24. Выявление и устранение последствий компьютерных атак ПАСЗИ	
ПП. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	**Виды работ** 1.Инструктаж по технике безопасности. 2.Разработка групповой политики безопасности. Конфигурирование автоматизированной системы. Текущий контроль, контроль целостности подсистем ОС. 3.Настройка аппаратных комплексов и подсистем защиты информации операционных систем. 4.Установка обновления программного обеспечения. Установка виртуальных ОС Установка ПО на виртуальных машинах. 5.Настройка сетевых операционных систем. 6.Конфигурирование КС. 7.Выполнение тестирование коммутации КС. 8.Тестирование аппаратных компонентов ЗИ 9.Проведение диагностики ПАСЗИ. 10.Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи конфиденциальной информации. Использование специализированного ПО для обработки конфиденциальной информации. 11.Аттестация систем хранения, обработки и передачи информации 12.Сертификация систем хранения, обработки и передачи информации.	**324**

	13.Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем. Применение программных комплексов по уничтожению остаточной информации.	
	Применение аппаратных средств для уничтожения носителей информации. 14.Организация учета носителей конфиденциальной информации Составления регламентов обслуживания ИС. 15.Определение работоспособности ПАСЗИ. 16.Выявление и устранение последствий компьютерных атак ПАСЗИ. 17.Выявление и устранение событий ИС средствами ПАСЗИ. 18.Тестирование параметров сетевых протоколов. 19.Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 20.Организация работ с удаленными хранилищами данных и базами данных. 21.Выполнение монтажа компьютерных сетей. установление и настройка параметров современных сетевых протоколов. 22.Работа в операционных системах с соблюдением действующих требований по защите информации 23.Установка обновления программного обеспечения. 24.Контроль целостность подсистем защиты информации операционных систем. 25.Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных. 26.Использование программных средств для архивирования информации. 27.Проведение аудита защищенности автоматизированной системы. 28.Применение нормативных правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 29.Применение технических средств для защиты информации в условиях применения мобильных устройств обработки и передачи данных. 30.Применение технических средств для криптографической защиты информации конфиденциального характера. 31.Применение технических средств для уничтожения информации и носителей информации. 32.Настройка сетевых операционных систем. 33.Конфигурирование КС. 34.Выполнение тестирование коммутации КС. 35.Тестирование аппаратных компонентов ЗИ	

	36.Проведение диагностики ПАСЗИ. 37.Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи конфиденциальной информации. Использование специализированного ПО для обработки конфиденциальной информации. 38.Аттестация систем хранения, обработки и передачи информации 39.Установка и настройка отдельных программных, программно-аппаратных средств защиты информации 40.Выявление и устранение событий ИС средствами ПАСЗИ. 41.Тестирование параметров сетевых протоколов. 42.Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 43.Организация работ с удаленными хранилищами данных и базами данных. 44.Выполнение монтажа компьютерных сетей. установление и настройка параметров современных сетевых протоколов. 45.Выявление и устранение событий ИС средствами ПАСЗИ. 46.Подготовка отчета о прохождении производственной практики 47.Дифференцированный зачет	
Объем часов по ПМ.02		**667**
Из них: теория		**56**
Практические занятия		**104**
Учебная практика		**108**
Производственная практика		**324**
Консультации		**6**
Самостоятельная работа		**15**
Промежуточная аттестация – экзамен по ПМ		**18**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Лаборатории программных и программно-аппаратных средств защиты информации. Рабочее место преподавателя, рабочие места по количеству обучающихся, компьютеры с лицензионным программным обеспечением, мультимедийное оборудование, интерактивная панель, комплект учебно-наглядных пособий, презентации, комплект видеофильмов.

Кабинет самостоятельной и воспитательной работы. Рабочее место преподавателя, рабочие места по количеству обучающихся, мультимедийное оборудование, комплект учебно-наглядных пособий, презентации, комплект видеофильмов, компьютер с лицензионным программным обеспечением, с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СГИ МГРИ: http://stud.sofmgri.ru:8081/

3.2. Информационное обеспечение реализации программы

3.2. Учебно-методическое и информационное обеспечение программы

а) нормативные акты:

№ п/п	Источник
1.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ .Об информации, информационных технологиях и о защите информации от 27 июля 2006 - docs.cntd.ru https://docs.cntd.ru/document/901990051
2.	Федеральный закон от 27 июля 2006 г. № 152-ФЗ О персональных данных от 27 июля 2006 - docs.cntd.ru https://docs.cntd.ru/document/901990046
3.	ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных

	технологий (с Поправкой) - docs.cntd.ru https://docs.cntd.ru/document/1200048398
4.	ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий - docs.cntd.ru https://docs.cntd.ru/document/1200051499
5.	ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер - docs.cntd.ru https://docs.cntd.ru/document/1200051500
6.	ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети - docs.cntd.ru https://docs.cntd.ru/document/1200048416
7.	ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология (ИТ). Практические правила управления информационной безопасностью - docs.cntd.ru https://docs.cntd.ru/document/1200044724
8.	ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель - docs.cntd.ru https://docs.cntd.ru/document/1200071694
9.	ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности - docs.cntd.ru https://docs.cntd.ru/document/1200069465
10.	ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности - docs.cntd.ru https://docs.cntd.ru/document/1200069464
11.	ГОСТ Р 34.10-2001 Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи - docs.cntd.ru https://docs.cntd.ru/document/1200026578
12.	ГОСТ Р 34.11-94 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (принят в качестве межгосударственного стандарта ГОСТ 34.311-95) - docs.cntd.ru https://docs.cntd.ru/document/1200004857

б) основная литература:

№ п/п	Источник
1.	Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511408

2.	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519364
3.	Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184.
4.	Советов, Б. Я. Базы данных : учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 403 с. — (Профессиональное образование). — ISBN 978-5-534-18784-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/545704
5.	Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511408.

в) дополнительная литература:

№ п/п	Источник
1.	Гниденко, И. Г. Технология разработки программного обеспечения : учебное пособие для среднего профессионального образования / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 248 с. — (Профессиональное образование). — ISBN 978-5-534-18131-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/534337 (дата обращения: 11.01.2024).
2.	Тенгайкин, Е. А. Эксплуатация объектов сетевого администрирования. Безопасность функционирования информационных систем. Лабораторные работы : учебное пособие для спо / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2022. — 80 с. — ISBN 978-5-8114-8692-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/197546 (дата обращения: 06.02.2024).
3.	Богатырев, В. А. Надежность информационных систем : учебное пособие для среднего профессионального образования / В. А. Богатырев. — Москва : Издательство Юрайт, 2023. — 318 с. — (Профессиональное образование). — ISBN 978-5-534-15205-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520442 (дата обращения: 06.02.2024).

г) периодические издания:

№ п/п	Источник
1.	Вопросы кибербезопасности : научный журнал / учредитель : Научно-производственное объединение Эшелон. – Москва : Научный центр правовой информации 2013 – . – выходит 6 раз в год . – ISBN печатной версии 2311-3456. – Текст : электронный // ЭБС elibrary [сайт]. — URL : https://www.elibrary.ru/title_about_new.asp?id=50036
2.	Безопасность информационных технология : научный журнал / учредитель : Национальный исследовательский ядерный университет МИФИ . – Москва : Национальный исследовательский ядерный университет МИФИ 1994 – . – выходит 4 раза в год . – ISBN печатной версии 2074-7128. – Текст : электронный // ЭБС elibrary [сайт]. — URL : https://www.elibrary.ru/title_about_new.asp?id=8429
3.	Программные продукты и системы : научный журнал / учредитель : Куприянов В. П.; Акционерное общество "Научно-исследовательский институт "Центрпрограммсистем". – Тверь : 1988 – . – Выходит 4 раза в год. – ISBN печатной версии 0236-235X. – Текст : электронный // ЭБС elibrary [сайт]. — URL: https://www.elibrary.ru/title_about_new.asp?id=9834

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения лабораторных, практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Итоговой формой контроля является: *экзамен по профессиональному модулю.*

Код и наименование профессиональных компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки результатов обучения**
ПК 2.1 Осуществлять установку и настройку	Осуществлять установку и настройку отдельных	тестирование, экзамен
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 программноаппаратных средств ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программноаппаратных средств обнаружения, предупреждения и ликвидации	программных, программноаппаратных средств защиты информации. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. Осуществлять обработку, хранение и передачу информации ограниченного доступа. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. 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. профессиональных компетенций (ПК)	квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

последствий компьютерных атак		
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданскопатриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	