МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова

Согласовано
Генеральный директор
ГАУ «Фарммедтехснаб» МЗ ЧР
_____ И.М. Халадов
«25» 01 2024г.

Первый проректор
ФГБОУ ВО «Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова»
_____ И.Г. Гайрабеков
«25» 01 2024г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация

Техник по защите информации

Грозный – 2024 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
«ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами обучающийся должен освоить основной вид деятельности техническое обслуживание и ремонт автомобильных двигателей и соответствующие ему общие компетенции и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для
ОК 09	Использовать информационные технологии в профессиональной деятельности

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 02	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1	Осуществлять установку и настройку отдельных программных, программноаппаратных 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 программноаппаратных средств защиты информации
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	установки, настройки программных средств защиты информации в автоматизированной систем.
	обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами
	тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программноаппаратных средств защиты информации

	решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации
	применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных
	учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности
	работы с подсистемами регистрации событий
	выявления событий и инцидентов безопасности в автоматизированной системе
Уметь	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
	устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями
	диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программноаппаратных средств защиты информации
	применять программные и программно-аппаратные средства для защиты информации в базах данных
	проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации
	применять математический аппарат для выполнения криптографических преобразований
	использовать типовые программные криптографические средства, в том числе электронную подпись
	применять средства гарантированного уничтожения информации
	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
	осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств 7 обнаружения, предупреждения и ликвидации последствий компьютерных атак
Знать	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 программно-аппаратных средств защиты информации;
	типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации
	основные понятия криптографии и типовых криптографических методов и средств защиты информации
	особенности и способы применения программных и 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

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего ОФО 652 часов
в том числе:
- на освоение МДК 354 часов;
- самостоятельная работа 56 часов;
- учебная практика 72 часов;
- производственная практика 144 часа;
- промежуточная аттестация 26.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	Объем профессионального модуля, ак. час.					
			Обучение по МДК				Практики	
			В том числе					
			Теоретических занятий	Практических занятий	Самостоя-тельная работа	Промежуточная аттестация	Учебная	Производственная
1	*2*	*3*	*6*	*7*	*8*	*9*	*10*	*11*
ПК 2.1 ПК 2.2 ОК 1, ОК 09	МДК.02.01.Программные и программно-аппаратные средства защиты информации	**276**	**116**	**116**	34	10	**-**	**-**
ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6 ОК 1, ОК 09	МДК.02.02.Криптографические средства защиты информации	**150**	**66**	**56**	22	6		
	УП.02. Учебная практика	**72**					**72**	**-**
	ПП.02.Производственная практика	**144**						**144**
	ПМ.02.Э.Промежуточная аттестация	**10**				10		
	Всего:	**652**	**182**	**172**	**56**	**26**	**72**	**144**

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад ч	Код ПК, ОК
1	2	3	4
Раздел 1. Программные и программно-аппаратные средства защиты информации		**276 /116**	
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**276 /116**	
Тема 1.1. Предмет и задачи программноаппаратной защиты информации	**Теоретические занятия**	***38***	
	1. Предмет и задачи программно-аппаратной защиты информации. Основные понятия программноаппаратной защиты информации.	4	ПК 2.1 ОК 02, ОК 09
	2. Классификация методов и средств, программно-аппаратной защиты информации.	6	ПК 2.1 ОК 02, ОК 09
	3. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	6	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	4. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).	6	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	5. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	6	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	6. Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall.	6	ПК 2.1, ПК 2.2 ОК 02, ОК 09

	7. Достоинства, недостатки, реализуемые политики безопасности	4	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	Практические занятия	**38**	
	1. Исследование дискреционной модели.	*4*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	2. Исследование мандатной модели.	*4*	ПК 1.2, ПК 1.3 ОК 02, ОК 09
	3.Технолигии защиты информации программно-аппаратными средствами.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	4. Исследование программ для шифрования данных	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	5.Изучение требований о защите информации, не составляющей государственную тайну.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	6. Изучение методических документов ФСТЭК по применению мер защиты.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	7. Установка и настройка программных средств оценки защищенности	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
Тема 1.2. Защищенная автоматизированная система	**Теоретические занятия**	***36***	
	1. Автоматизация процесса обработки информации. Понятие автоматизированной системы.	*6*	ПК 2.1, ПК 2.2, ОК 02, ОК 09
	2. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.	*6*	ПК 2.1, ПК 2.2, ОК 02, ОК 09
	3. Методы создания безопасных систем.	*6*	ПК 2.1 ОК 02, ОК 09
	4. Методология проектирования гарантированно защищенных КС.	*6*	ПК 2.1 ОК 02, ОК 09
	5. Дискреционные модели. Мандатные модели.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	6. Защитные механизмы в современном программном обеспечении на примере MS Office	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	Практические занятия	**42**	

	1. Исследование источников воздействия на объекты защиты.	*6*	ПК 2.2 ОК 02, ОК 09
	2. Исследование способов воздействия на информацию.	*6*	ПК 2.2 ОК 02, ОК 09
	3. Исследование методв создания безопасных систем	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	4. Исследование принципов, архитектуры, модели нарушителя, достоинства и не достатки.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	5. Исследование методов защиты информации при работе в сетях общего доступа.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	6.Исследование основных типов угроз, модель нарушителя.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	7.Исследование критериев защищенности баз данных	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
Тема 1.3. Дестабилизирующее воздействие на объекты защиты	**Теоретические занятия**	***42***	
	1. Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему.	*6*	ПК 2.1 ОК 02, ОК 09
	2. Идентификация и аутентификация пользователей. Разграничение доступа.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	3.Регистрация событий (аудит). Контроль целостности данных.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	4. Уничтожение остаточной информации. Управление политикой безопасности.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	5. Шаблоны безопасности. Криптографическая защита.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	6. Обзор программ шифрования данных. Управление политикой безопасности. Шаблоны безопасности.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	7. Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию.	*4*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	Практические занятия	**36**	
	1. Исследование несанкционированного доступа к информации.	*6*	ПК 2.1, ПК 2.2

			ОК 02, ОК 09
	2. Исследование контроля доступа	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	3. Исследование разграниченичного доступа.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	4. Исследование модели системы обнаружения вторжений, аномалий, сигнатур.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	5. Исследование вредоносного программного обеспечения.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
	6. Исследование защиты от вирусов в ручном режиме.	*6*	ПК 2.1, ПК 2.2 ОК 02, ОК 09
Примерная тематика самостоятельной учебной работы при изучении раздела 1 1. Составление алгоритма по защите информации программными и программно-аппаратными средствами. 2. Составление алгоритма по проектированию защищенных КС 3. Составление алгоритма дестабилизирующего воздействия на информацию. 4. Составление алгоритма защиты данных от изменения. 5. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов. 6. Обзор и анализ современных программно-аппаратных средств защиты информации. 7. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся данных. 8. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии. 9. Проблема защиты информации в облачных хранилищах данных. 10. Защита сред виртуализации.		***34***	
Промежуточная аттестация		***10***	

Раздел 2. Криптографические средства и методы защиты информации		**150/66**	
МДК 02.02. Криптографические средства и методы защиты информации		**150/66**	
Тема 2.1. Математические основы криптографии	**Теоретические занятия**	***26***	
	1. Элементы теории множеств. Группы, кольца, поля.	2	ПК 2.1, ОК 02, ОК 09
	2. Делимость чисел. Признаки делимости. Простые и составные числа.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	3. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	4. Эллиптические кривые и их приложения в криптографии.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	5. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	6. Классы. Полная и приведенная система вычетов.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	7. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	2	ПК 2.1, ОК 02, ОК 09
	8. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	9. Китайская теорема об остатках.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	10. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	2	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	11. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2	ПК 2.2 ОК 02, ОК 09
	12. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2	ПК 2.2 ОК 02, ОК 09
	13. Арифметические операции над большими числами.	2	ПК 2.2 ОК 02, ОК 09
	14. Эллиптические кривые и их приложения в криптографии.	2	ПК 2.2 ОК 02, ОК 09

	Практические занятия	**12**	
	1. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	*4*	ПК 2.2, ПК2.3 ОК 02, ОК 09
	2. Проверка чисел на простоту	*4*	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	3. Решение задач с элементами теории чисел.	*4*	ПК 22, ПК 2.3 ОК 02, ОК 10
Тема 2.2. Методы криптографическог о защиты информации	**Теоретические занятия**	***8***	
	1.Классификация основных методов криптографической защиты. Методы симметричного шифрования	*2*	ПК 2.1, ПК 2.2, ПК 2.3
	2. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	*2*	ПК 2.2 ОК 02, ОК 09
	3. Методы перестановки. Табличная перестановка, маршрутная перестановка	*2*	ПК 2.1 ОК 02, ОК 10
	4. Гаммирование. Гаммирование с конечной и бесконечной гаммами	*2*	ПК 2.2 ОК 02, ОК 09
	Практические занятия	**12**	
	1. Применение классических шифров замены	*4*	ПК 2.2 ОК 02, ОК 10
	2. Применение классических шифров перестановки	*4*	ПК 2.2 ОК 02, ОК 09
	3. Применение метода гаммирования	*4*	ПК 2.3 ОК 02, ОК 09
Тема 2.3. Криптоанализ	**Теоретические занятия**	***2***	
	1. Основные методы криптоанализа. Криптографические атаки. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	*2*	ПК 2.1 ОК 02, ОК 10
	Практические занятия	**12**	
	1. Криптоанализ шифра простой замены методом анализа частотности символов	*4*	ПК 2.1 ОК 02, ОК 09

	2. Криптоанализ классических шифров методом полного перебора ключей	*4*	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	3. Криптоанализ шифра Вижинера	*4*	ПК 2.3 ОК 02, ОК 09
Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	**Теоретические занятия**	***8***	
	1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	*4*	ПК 2.2 ОК 02, ОК 10
	2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	*4*	ПК 2.1 ОК 02, ОК 10
	Практические занятия	**2**	
	1. Применение методов генерации ПСЧ	*2*	ПК 2.2 ОК 02, ОК 10
Тема 2.5. Кодирование информации. Компьютеризация шифрования.	**Теоретические занятия**	***6***	
	1. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	*2*	ПК 2.3 ОК 02, ОК 09
	2. Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	*2*	ПК 2.3 ОК 02, ОК 09
	Практические занятия	***6***	
	1. Кодирование информации	*2*	ПК 2.3 ОК 02, ОК 09
	2. Программная реализация классических шифров	*2*	ПК 2.3 ОК 02, ОК 09
	3. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	*2*	ПК 2.2, ПК 2.3 ОК 02, ОК 09
Тема 2.6. Симметричные системы	**Теоретические занятия**	***4***	
	1. Общие сведения. Структурная схема симметричных криптографических систем	*2*	ПК 2.2, ПК 2.3 ОК 02, ОК 09

шифрования	2. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	*2*	ПК 2.1 ОК 02, ОК 10
	Практические занятия	***4***	
	1. Изучение программной реализации современных симметричных шифров	*4*	ПК 2.2, ПК 2.3 ОК 02, ОК 09
Тема 2.7. Асимметричные системы шифрования	**Теоретические занятия**	***4***	
	1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	*2*	ПК 2.1 ОК 02, ОК 10
	2. Элементы теории чисел в криптографии с открытым ключом.	*2*	ПК 2.1 ОК 02, ОК 10
	Практические занятия	***4***	
	1. Применение различных асимметричных алгоритмов.	*2*	ПК 2.2, ПК 2.3 ОК 02, ОК 09
	2. Изучение программной реализации асимметричного алгоритма RSA	*2*	ПК 2.2, ПК 2.3 ОК 02, ОК 09
Тема 2.8. Аутентификация данных. Электронная подпись	**Теоретические занятия**	***4***	
	1. Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	*4*	ПК 2.2 ОК 02, ОК 10
	Практические занятия	***2***	
	1. Применение различных функций хеширования, анализ особенностей хешей	***2***	ПК 2.2 ОК 02, ОК 10
Тема 2.9. Криптозащита информации в сетях передачи данных	**Теоретические занятия**	**4**	
	1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	*2*	ПК 2.2 ОК 02, ОК 10
	2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	*2*	ПК 2.2 ОК 02, ОК 10
Примерная тематика самостоятельной работы при изучении раздела 2 1. История развития криптографии		***22***	

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		
Промежуточная аттестация	***6***	
Учебная практика **Виды работ** 1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. 2. Диагностика, устрнение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности . 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации. 5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации. 6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 7. Устранение замечаний по результатам проверки . 8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программноаппаратными средствами, с учетом нормативных правовых актов. 9. Применение математических методов для оценки качества и выбора наилучшего программного средства .	***72***	

10. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.		
Производственная практика **Виды работ** 1. Анализ принципов построения систем информационной защиты производственных подразделений. 2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. 3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности. 4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении. 5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации. 6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	***144***	
Промежуточная аттестация	***10***	
Всего	***652***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория «Программных и программно-аппаратных средств защиты информации», оснащенная в соответствии с п. 6.1.2.3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с п 6.1.2.5 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет электронные образовательные и информационные ресурсы для использования в образовательном процессе.

3.2.1. Основные электронные издания

1. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. Учреждений сред. Проф. Образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлянский. - Москва : "Академия", 2020. - 288 с.

2. Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17926.html. — Режим доступа: для авторизир. пользователей

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, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997.

1. Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https://e.lanbook.com/book/161347. — Режим доступа: для авториз. пользователей.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
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 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств документации ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе	**Критерии оценивания рубежной аттестации:** **Аттестован** - выставляется обучающемуся, ответившему правильно на 6-20 вопросов. **Не аттестован** - выставляется обучающемуся, который ответил менее 5 вопроса. **Критерии оценивания зачета/экзамена:** **Зачтено** - выставляется обучающемуся, ответившему правильно на 11 вопросов. **Не зачтено** - выставляется обучающемуся, который ответил 10 и менее вопроса. **Отлично** - выставляется обучающемуся, ответившему на 31-40 вопросов. **Хорошо** - выставляется обучающемуся, ответившему на 21-30 вопросов. **Удовлетворительно** - выставляется обучающемуся, ответившему на 11 и более вопросов.	Рубежная аттестация Зачет Экзамен

с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. ОК 09. Использовать информационные технологии в профессиональной деятельности.		

Разработчик:

Преподаватель ФСПО _____ / А.У.Байдарова/
(подпись)

Согласовано:

Председатель ПЦК «Информационные технологии»

_____ / И.М.Дубаев/
(подпись)

Зам. декана по МР ФСПО _____ / И.В.Сулейманова/
(подпись)

Директор ДУМР _____ / М.А. Магомаева/
(подпись)