Приложение 5
к ППССЗ специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

Государственное бюджетное профессиональное образовательное учреждение
Республики Дагестан «Технический колледж имени Р.Н. Ашуралиева»

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

МДК.02.02. Криптографические средства защиты информации

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника: Техник по защите информации

Махачкала, 2024 г.

ОДОБРЕНО

предметной (цикловой) комиссией УГС 09.00.00. Информатика и вычислительная техника и 10.00.00 Информационная безопасность

Председатель П(Ц)К

__  Ш.М. Мусаева
Протокол №1 от «30» августа 2024 г

Рабочая программа учебной междисциплинарного курса МДК.02.02. Криптографические средства защиты информации разработана на основе:

- Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации № 1553 от 9 декабря 2016 г., (зарегистрирован Министерством юстиции РФ 26 декабря 2016 г. N 44938);

с учетом:

- Примерной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанной Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненным группам профессий и специальностей 10.00.00 Информационная безопасность (протокол № 1 от 28.03.2017)

в соответствии с рабочим учебным планом по специальности.

Разработчик:

- Полозкова Елена Николаевна, преподаватель ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО курса «МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

1.1. Место междисциплинарного курса в структуре основной профессиональной образовательной программы

Междисциплинарный курс МДК.02.02. Криптографические средства защиты информации, в составе профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, принадлежит общепрофессиональному циклу П.00 обязательной части ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Цель и планируемые результаты освоения междисциплинарного курса:

Освоение междисциплинарного курса должно способствовать формированию 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.

Освоение междисциплинарного курса должно способствовать овладению профессиональными компетенциями:

- ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В результате освоения междисциплинарного курса обучающийся должен получить практический опыт:

- 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;

В результате освоения междисциплинарного курса обучающийся должен **уметь:**

- 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;

В результате освоения междисциплинарного курса обучающийся должен **знать:**

- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации;

Общие компетенции:

Код компетенции	**Формулировка компетенции**	**Знания, умения**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности

ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
		Знания: номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в 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;	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
		Знания: психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе
		Знания: особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.
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;	**Умения:** описывать значимость своей специальности
		Знания: сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности

ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности
		Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
		Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Профессиональные компетенции:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	**Практический опыт:** 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.
	Умения: 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.
	Знания: Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных. Типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации. Основные понятия криптографии и типовых криптографических методов и средств защиты информации.

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

2.1. Объем учебной междисциплинарного курса и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы	186
в том числе:	
Урок	96
Лекция	-
Лабораторные занятия	38
Практические занятия	14
Консультация перед экзаменом	2
Промежуточная аттестация в форме экзамена	6
Самостоятельная работа	30

- Объем времени обязательной части ППССЗ 144 час.
- Объем времени вариативной части ППССЗ 42 час.

По сравнению с примерной программой в рабочей программе междисциплинарного курса количество часов увеличено на 46 часов. Вариативная часть используется на углубление подготовки по междисциплинарному курсу.

2.2. Тематический план и содержание междисциплинарного курса «МДК.02.02. Криптографические средства защиты информации»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
	5 семестр		
Тема 1. Математические основы криптографии	**Содержание учебного материала**	**26**	ОК 1 – ОК 09, ПК 2.4
	1. Предмет и задачи криптографии. История криптографии. Основные термины		
	2. Элементы теории множеств. Группы, кольца, поля		
	3. Делимость чисел. Признаки делимости. Простые и составные числа		
	4. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД		
	5. Отношения сравнимости. Свойства сравнений. Модулярная арифметика		
	6. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера		
	7. Алгоритм быстрого возведения в степень по модулю		
	8. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида		
	9. Китайская теорема об остатках		
	10. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена		
	11. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда		
	12. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра		
	13. Арифметические операции над большими числами. Эллиптические кривые и их приложения в криптографии		
	Практические занятия	8	
	14. Применение алгоритма Евклида для нахождения НОД		
	15. Решение линейных диофантовых уравнений		
	16. Проверка чисел на простоту.		
	17. Решение задач с элементами теории чисел		
Тема 2. Методы криптографического защиты информации	**Содержание учебного материала**	**8**	ОК 1 – ОК 09, ПК 2.4
	18. Классификация основных методов криптографической защиты		
	19. Методы симметричного шифрования		
	20. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр		

	21.	Методы перестановки. Табличная перестановка, маршрутная перестановка Гаммирование. Гаммирование с конечной и бесконечной гаммами		
	Практические занятия		6	
	22.	Применение классических шифров замены		
	23.	Применение классических шифров перестановки		
	24.	Применение метода гаммирования		
Тема 3. Криптоанализ	**Содержание учебного материала**		**8**	ОК 1 – ОК 09, ПК 2.4
	25.	Основные методы криптоанализа. Криптографические атаки		
	26.	Криптографическая стойкость. Абсолютно стойкие криптосистемы		
	27.	Принципы Киркхоффса		
	28.	Перспективные направления криптоанализа, квантовый криптоанализ		
	Лабораторные занятия		6	
	29.	Криптоанализ шифра простой замены методом анализа частотности символов		
	30.	Криптоанализ классических шифров методом полного перебора ключей		
	31.	Криптоанализ шифра Вижинера		
Тема 4. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**		**6**	ОК 1 – ОК 09, ПК 2.4
	32.	Основные принципы поточного шифрования		
	33.	Применение генераторов ПСЧ в криптографии		
	6 семестр			
	34.	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS		
	Лабораторные занятия		2	
	35.	Применение методов генерации ПСЧ		
Тема 5. Кодирование информации. Компьютеризация шифрования	**Содержание учебного материала**		**10**	ОК 1 – ОК 09, ПК 2.4
	36.	Кодирование информации. Символьное кодирование. Смысловое кодирование		
	37.	Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII		
	38.	Компьютеризация шифрования. Аппаратное и программное шифрование		
	39.	Стандартизация программно-аппаратных криптографических систем и средств.		
	40.	Изучение современных программных и аппаратных криптографических средств		
	Лабораторные занятия		8	
	41.	Кодирование информации		
	42.	Программная реализация классических шифров		
	43.	Изучение реализации классических шифров замены в программе CrypTool или аналоге		
	44.	Изучение реализации классических шифров перестановки в программе CrypTool или аналоге		
Тема 6. Симметричные системы шифрования	**Содержание учебного материала**		**8**	ОК 1 – ОК 09, ПК 2.4
	45.	Общие сведения о симметричных системах шифрования		
	46.	Структурная схема симметричных криптографических систем		
	47.	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015		

	48.	Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4		
	Лабораторные занятия		2	
	49.	Изучение программной реализации современных симметричных шифров		
Тема 7. Асимметричные системы шифрования	**Содержание учебного материала**		**4**	ОК 1 – ОК 09, ПК 2.4
	50.	Криптосистемы с открытым ключом. Необратимость систем.		
	51.	Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом		
	Лабораторные занятия		4	
	52.	Применение различных асимметричных алгоритмов		
	53.	Изучение программной реализации асимметричного алгоритма RSA		
Тема 8. Аутентификация данных. Электронная подпись	**Содержание учебного материала**		**6**	ОК 1 – ОК 09, ПК 2.4
	54.	Аутентификация данных. Общие понятия		
	55.	ЭП. MAC. Однонаправленные хеш-функции.		
	56.	Алгоритмы цифровой подписи		
	Лабораторные занятия		6	
	57.	Применение различных функций хеширования. Анализ особенностей хешей		
	58.	Применение криптографических атак на хеш-функции		
	59.	Изучение программно-аппаратных средств, реализующих основные функции ЭП		
Тема 9. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**		**4**	ОК 1 – ОК 09, ПК 2.4
	60.	Алгоритмы распределения ключей с применением симметричных и асимметричных схем		
	61.	Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация		
	Лабораторные занятия		4	
	62.	Применение протокола Диффи-Хеллмана для обмена ключами шифрования		
	63.	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos		
Тема 10. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**		**6**	ОК 1 – ОК 09, ПК 2.4
	64.	Абонентское шифрование. Пакетное шифрование		
	65.	Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр		
	66.	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP		
Тема 11. Защита информации в электронных платежных системах	**Содержание учебного материала**		**4**	ОК 1 – ОК 09, ПК 2.4
	67.	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер		
	68.	Применение криптографических протоколов для обеспечения безопасности электронной коммерции		
	Лабораторные занятия		2	
	69.	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей		
	Содержание учебного материала		**6**	ОК 1 – ОК 09, ПК 2.4
	70.	Скрытая передача информации в компьютерных системах.		

Тема 12. Компьютерная стеганография	71.	Проблема аутентификации мультимедийной информации. Защита авторских прав		
	72.	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ		
	Лабораторные занятия		4	
	73.	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ		
	74.	Изучение алгоритмов встраивания ЦВЗ. Реализация простейших стеганографических алгоритмов		
Консультации перед экзаменом			**2**	
Самостоятельная работа обучающихся:			**30**	
	Изучить теоретический материал и составить тезисы (краткий конспект): – История развития криптографии – Программная реализация классических шифров – Оптимизация методов частотного анализа моноалфавитных шифров – Программная реализация классических шифров – Методы механизации шифрования – Цифровое представление различных форм информации – Анализ современных симметричных криптоалгоритмов – Анализ современных асимметричных криптоалгоритмов – Программная реализация современных криптоалгоритмов – Сравнительный анализ функций хеширования – Аутентификация сообщений – Законодательство в области криптографической защиты информации – Перспективные направления криптографии			
	Промежуточная аттестация в форме экзамена		**6**	
	Всего		**186**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

3.1. Материально-техническое обеспечение

Для реализации программы междисциплинарного курса «МДК.02.02. Криптографические средства защиты информации» предусмотрены лаборатория «Программных и программно-аппаратных средств обеспечения информационной безопасности», оснащенная оборудованием и техническими средствами обучения:

Лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности»

- Рабочие места на 25 обучающихся;
- Автоматизированные рабочие места на 12 обучающихся, подключенные к локальной вычислительной сети и сети «Интернет»;
- Автоматизированное рабочее место преподавателя;
- Интерактивная доска, проектор, кронштейн;
- МФУ;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения;
- Антивирусные программные комплексы;
- Программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- Программные и программно-аппаратные средства обнаружения вторжений;
- Средства уничтожения остаточной информации в запоминающих устройствах;
- Программные средства выявления уязвимостей в АС и СВТ;
- Программные средства криптографической защиты информации;
- Программные средства защиты среды виртуализации.
- Комплект учебно-методической документации;
- Фонд оценочных средств по междисциплинарному курсу.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2023.
2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2020.- 412 с.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2021. – 214 с.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2021. – 185 с.
5. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2020. – 336с

6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2022.- 410 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
7. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2022. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности
8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 330с. – 2021
9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2022
10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2020. – 416 с.

3.2.2. Дополнительные печатные источники:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2021. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2021 г
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств

защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
16. от 30 августа 2002 г. № 282.
17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
19. от 31 августа 2010 г. № 416/489.
20. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
21. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
22. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
23. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.
24. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
25. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
26. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
27. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
28. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
29. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
30. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
31. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
32. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

33. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
34. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
35. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
37. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
38. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
39. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
40. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
41. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
42. Номенклатура показателей качества. Ростехрегулирование, 2005.
43. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
44. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
45. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
46. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
47. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
48. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
49. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
50. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
51. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
52. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

53. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
54. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
55. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
56. программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;
57. базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.3. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

3.3. Кадровое обеспечение образовательного процесса

Реализация программы МДК обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии (имеющих стаж работы в данной профессиональной области не менее 3 лет).

Квалификация педагогических работников должна отвечать квалификационным требованиям, указанным в квалификационных справочниках.

Требования к квалификации педагогических работников. Высшее профессиональное образование или среднее профессиональное образование по направлению подготовки "Образование и педагогика" или в области, соответствующей преподаваемой дисциплине, без предъявления требований к стажу работы, либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу работы.

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных занятий, экспертное наблюдение выполнения практических занятий, оценка решения ситуационных задач

Код компетенции	**Формулировка компетенции**	**Знания, умения**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение

	профессиональной деятельности	**Знания:** номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в 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;	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
		Знания: психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе
		Знания: особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.
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;	**Умения:** описывать значимость своей специальности
		Знания: сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности
ОК 07	Содействовать сохранению окружающей среды,	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности

	ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	**Знания:** правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
		Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности