ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Рабочая программа междисциплинарного курса

МДК 02.02. Криптографические средства защиты информации

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Алексеевка
2021

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Одобрено
на заседании Педагогического совета
Протокол № 1 от 31 августа 2021 г.
Председатель
_____О.В. Афанасьева

Утверждаю:
Директор ОГАПОУ
«Алексеевский колледж»
_____О.В. Афанасьева
Приказ № 613
от 31 августа 2021 г.

Принято
предметно - цикловой комиссией
общепрофессиональных дисциплин и
профессиональных модулей
специальности 10.02.05 Обеспечение
информационной безопасности
автоматизированных систем и
профессии 09.01.01 Наладчик
аппаратного и программного
обеспечения
Протокол № 1 от 31 августа 2021 г.

Председатель _____ Зюбан Е.В.
подпись / ФИО

Разработчик: _____ А.В.Ляшенко, преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ МДК	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК	6
3. СТРУКТУРА И СОДЕРЖАНИЕ МДК	7
4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК	14
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК	20

1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

МДК 02.02 Криптографические средства защиты информации

1.1. Область применения рабочей программы междисциплинарного курса

Рабочая программа междисциплинарного курса является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД): Защита информации в автоматизированных системах программными и программно-аппаратными средствами(ПК):

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

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

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

уметь:

1. устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
2. устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

3. диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
4. применять программные и программно-аппаратные средства для защиты информации в базах данных;
5. проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
6. применять математический аппарат для выполнения криптографических преобразований;
7. использовать типовые программные криптографические средства, в том числе электронную подпись;
8. применять средства гарантированного уничтожения информации;
9. устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
10. 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.

знать:

1. особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
2. методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
3. типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
4. основные понятия криптографии и типовых криптографических методов и средств защиты информации;
5. особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
6. типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции Ворлдскиллс Корпоративная

защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

1) знать и понимать: скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню;

2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;

3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;

4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;

5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;

6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;

7) знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз.

1.3. Планируемые личностные результаты освоения рабочей программы

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.4. Количество часов на освоение рабочей программы МДК:

максимальной учебной нагрузки обучающегося –162 часа, в том числе: аудиторной учебной работы обучающегося - 144 часа, из них в форме практической подготовки – 6 часа; в том числе практических занятий –56 часов; самостоятельной учебной работы обучающегося – 0 часов; консультаций - 12 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК

Результатом освоения МДК является овладение обучающимися видом деятельности - Защита информации в автоматизированных системах программными и программно-аппаратными средствами, в том числе общие компетенции (ОК) и профессиональными компетенциями (ПК):

Код	Наименование результата обучения
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 поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3.2. Тематический план и содержание МДК 02.02 Криптографические средства защиты информации

Наименование разделов междисциплинарного курса (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная самостоятельная учебная работа обучающихся	Объем часов	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы
1	2	3	4
МДК 02.02 Криптографические средства защиты информации		**162/6**	
Раздел 1. Математические основы криптографии		**30/6**	
Тема 1.1. Математические основы	**Содержание учебного материала, в том числе в форме практической подготовки**	**24/0**	ОК1-5 ОК10 ПК 2.1-2.2
	1. Предмет и задачи криптографии. История криптографии. Основные термины		
	2. Элементы теории множеств. Группы, кольца, поля.		

криптографии	3. Делимость чисел. Признаки делимости. Простые и составные числа.		З1 З2 У1 У2 ЛР4 ЛР7 ЛР8-11
	4. Основная теорема арифметики. Наибольший общий делитель. Взаимно		
	5. простые числа. Алгоритм Евклида для нахождения НОД.		
	6. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.		
	7. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. 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.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки 1 Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений 2 Проверка чисел на простоту 3 Решение задач с элементами теории чисел	**6/6**	
	Контрольные работы	*	
Раздел 2. Классическая криптография		**34/0**	
Тема 2.1. Методы криптографического защиты информации	**Содержание учебного материала, в том числе в форме практической подготовки**	**14/0**	ОК1-5 ОК10 ПК 2.1-.2.2 З1 З2 У1 У2
	1. Классификация основных методов криптографической защиты. Методы симметричного шифрования	**8/0**	
	2. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр		
	3. Методы перестановки. Табличная перестановка, маршрутная перестановка		
	4. Гаммирование. Гаммирование с конечной и бесконечной гаммами		

	Лабораторные занятия	*	ЛР4 ЛР7 ЛР8-11
	Практические занятия, в том числе в форме практической подготовки	**6/0**	
	1. Применение классических шифров замены		
	2. Применение классических шифров перестановки		
	3. Применение метода гаммирования		
	Контрольные работы	*	
Тема 2.2. Криптоанализ	**Содержание учебного материала, в том числе в форме практической подготовки**	**14/0**	ОК1-5 ОК10 ПК 2.1-.2.2, 2.3 З1 З2 З3 З4 У1 У2 У3 У4 ЛР4 ЛР7 ЛР8-11
	1. Основные методы криптоанализа. Криптографические атаки.	6/0	
	2. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса		
	3. Перспективные направления криптоанализа, квантовый криптоанализ.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	8/0	
	1. Криптоанализ шифра простой замены методом анализа частотности символов		
	2. Криптоанализ классических шифров методом полного перебора ключей		
	3. Криптоанализ шифра Вижинера		
	4. Криптоанализ шифра Вижинера		
	Контрольные работы	*	
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/0**	ОК1-5 ОК10 ПК 2.1-2.3 З1-З4 У1-У4 ЛР4 ЛР7 ЛР8-11
	1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	4/0	
	2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**2/0**	
	1. Применение методов генерации ПСЧ		
	Контрольные работы	*	
Раздел 3.		**70/0**	

Современная криптография			
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/0**	ОК1-5 ОК10 ПК 2.1-2.3 З1-З4 У1-У4 ЛР4 ЛР7 ЛР8-11
	1. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования.		
	2. Представление информации в двоичном коде. Таблица ASCII. Компьютеризация шифрования. Аппаратное и программное шифрование	**6/0**	
	3. Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки		
	1. Кодирование информации		
	2. Программная реализация классических шифров	**6/0**	
	3. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.		
	Контрольные работы	*	
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала, в том числе в форме практической подготовки**	**8/0**	ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	1. Общие сведения. Структурная схема симметричных криптографических систем		
	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	4/0	
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	4/0	
	1.Изучение программной реализации симметричных шифров		
	2.Изучение программной реализации современных симметричных шифров		
	Контрольные работы	*	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала, в том числе в форме практической подготовки**	**8/0**	ОК1-7 ОК10 ПК 2.1-2.4
	1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	4/0	
	2. Элементы теории чисел в криптографии с открытым ключом.		

	Лабораторные занятия	*	З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	Практические занятия, в том числе в форме практической подготовки	4/0	
	1. Применение различных асимметричных алгоритмов.		
	2. Изучение программной реализации асимметричного алгоритма RSA		
	Контрольные работы	*	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/0**	ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	1. Аутентификация данных. Общие понятия. ЭП. МАС.	4/0	
	2. Однонаправленные хеш-функции. Алгоритмы цифровой подписи		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**6/0**	
	1. Применение различных функций хеширования, анализ особенностей хешей		
	2. Применение криптографических атак на хеш-функции.		
	3. Изучение программно-аппаратных средств, реализующих основные функции ЭП		
	Контрольные работы	*	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/0**	ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. аутентификация	4/0	
	2. Взаимная аутентификация. Односторонняя		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**6/0**	
	1. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.		
	2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.		
	Контрольные работы	*	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/0**	ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7
	1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	4/0	
	2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.		

			ЛР8-11
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	*	
	Контрольные работы	*	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/0**	ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	1. Принципы функционирования электронных платежных систем.	6/0	
	2. Электронные пластиковые карты. Персональный идентификационный номер		
	3. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**4/0**	
	1. Применение аутентификации по одноразовым паролям.		
	2. Реализация алгоритмов создания одноразовых паролей		
	Контрольные работы	*	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала, в том числе в форме практической подготовки**	**8/0**	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4 ЛР7 ЛР8-11
	1. Скрытая передача информации в компьютерных системах.	4/0	
	2. Проблема аутентификации мультимедийной информации. Защита авторских прав.		
	3. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**4/0**	
	1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ		
	2. Реализация простейших стеганографических алгоритмов		
	Контрольные работы	*	
Самостоятельная работа обучающихся		*	
Промежуточная аттестация ***экзамен***		**6/0**	
Консультации		**12/0**	
Всего:		**162**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК

4.1. Требования к минимальному материально-техническому обеспечению:

Реализация рабочей программы МДК предполагает наличие учебного кабинета лаборатория сетей и систем передачи информации.

Оборудование учебного кабинета:

Комплект учебно-методической документации. Специализированная учебная мебель: стол преподавателя, стул преподавателя, столы для студентов, стулья для студентов, классная доска.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение обучения

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н.Криптографическая защита информации в объектах информационной инфраструктуры, 1-е изд., ИЦ АКАДЕМИЯ ,2020 - 288 с.
2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.

Дополнительные источники:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 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

от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы.

Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. 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.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.

№ 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».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. 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

24. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

25. 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

26. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

27. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

28. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

29. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

30. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

31. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

32. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

33. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

34. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

35. 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.

36. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

37. 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.

38. 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.

39. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

40. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

41. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

42. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

44. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

45. Меры защиты информации в государственных

информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

46. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

47. программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

48. базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

Электронные издания (электронные ресурсы):

1. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 https://e.lanbook.com/book/82817

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, 2020. — 312 с. https://urait.ru/bcode/449548

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcode/456793

4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2020. — 325 с. https://urait.ru/bcode/451933

Цифровая образовательная среда СПО PROFобразование:

- Пащинская, Л. И. Социально-экономические аспекты современного общества : учебное пособие / Л. И. Пащинская. — Воронеж : Воронежский государственный университет инженерных технологий, 2018. — 208 с. — ISBN 978-5-00032-379-3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/88435 (дата обращения: 12.07.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPR BOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

Контроль и оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических занятий, экзамена.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	– тестирование, – экзамен квалификационный, – экспертное наблюдение выполнения лабораторных работ, – экспертное наблюдение выполнения практических работ, – оценка решения ситуационных задач, – оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	• тестирование, • экзамен квалификационный, • экспертное наблюдение выполнения лабораторных работ, • экспертное наблюдение выполнения практических работ, • оценка решения ситуационных задач, • оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	• тестирование, • экзамен квалификационный, • экспертное наблюдение выполнения лабораторных работ,

защиты информации.		• экспертное наблюдение выполнения практических работ, • оценка решения ситуационных задач, • оценка процесса и результатов выполнения видов работ на практике
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	• тестирование, • экзамен квалификационный, • экспертное наблюдение выполнения лабораторных работ, • экспертное наблюдение выполнения практических работ, • оценка решения ситуационных задач, • оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	• тестирование, • экзамен квалификационный, • экспертное наблюдение выполнения лабораторных работ, • экспертное наблюдение выполнения практических работ, • оценка решения ситуационных задач, • оценка процесса и результатов выполнения видов работ на практике
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	• тестирование, • экзамен квалификационный, • экспертное наблюдение выполнения лабораторных работ, • экспертное наблюдение выполнения практических работ, • оценка решения ситуационных задач, • оценка процесса и результатов выполнения видов работ на практике