

Приложение ППСЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2023-2024 уч.г.: Рабочая программа междисциплинарного курса МДК 02.02 Криптографические средства защиты информации

МИНИСТЕРСТВО 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
2023

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

Разработчик:

Гадяцкая И.Д., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ МДК
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МДК
3. СТРУКТУРА И СОДЕРЖАНИЕ МДК
- 4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК

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:

- У.1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- У.2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

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

- 3.1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- 3.2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
- 3.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- 3.4 основные понятия криптографии и типовых криптографических методов и средств защиты информации;
- 3.5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
- 3.6 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 чемпионатного движения по профессиональному мастерству «Профессионалы» компетенции Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении учебной дисциплины:

- 1) знать и понимать: типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- 2) знать и понимать: каналы передачи данных: определение и виды;
- 3) знать и понимать: технологии работы с политиками информационной безопасности;
- 4) уметь: создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты;
- 5) уметь: администрирование автоматизированных технических средства управления и контроля информации и информационных потоков;
- 6) уметь: создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты.

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 лично 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 – 162 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. СТРУКТУРА И СОДЕРЖАНИЕ

МДК 02.02 Криптографические средства защиты информации

3.1. Объем МДК и виды учебной работы

Вид учебной работы	Объем часов
1	2
Максимальная учебная нагрузка (всего)	162
Аудиторная учебная работа (обязательные учебные занятия) (всего)	144
из них в форме практической подготовки	162
в том числе:	
лекционные занятия	88
лабораторные работы	
практические занятия	56
Самостоятельная работа обучающегося (всего)	0
в том числе:	
Консультации	12
Промежуточная аттестация в форме <i>экзамена</i>	6

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		162/162	
Раздел 1. Математические основы криптографии			
Тема 1.1. Математические основы криптографии	Содержание учебного материала, в том числе в форме практической подготовки 1. Предмет и задачи криптографии. История криптографии. Основные термины 2. Элементы теории множеств. Группы, кольца, поля.	32/32	ОК1-5 ОК10 ПК 2.1-2.2

	3. Делимость чисел. Признаки делимости. Простые и составные числа.		31 32 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	*	
	Контрольные работы	*	
Раздел 2. Классическая криптография			
Тема 2.1. Методы криптографического защиты информации	Содержание учебного материала, в том числе в форме практической подготовки	14/14	ОК1-5 ОК10 ПК 2.1-.2.2 31 32 У1 У2 ЛР4 ЛР7 ЛР8-11
	1. Классификация основных методов криптографической защиты. Методы симметричного шифрования	8/8	
	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	*	
	Практические занятия, в том числе в форме практической подготовки	6/6	
	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	14/14	ОК1-5 ОК10 ПК 2.1- .2.2, 2.3 31 32 33 34 У1 У2 У3 У4 ЛР4 ЛР7 ЛР8-11
	1. Основные методы криптоанализа. Криптографические атаки.	6/6	
	2. Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхoffsа		
	3. Перспективные направления криптоанализа, квантовый криптоанализ.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	8/8	
	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	8/8	ОК1-5 ОК10 ПК 2.1- 2.3 31-34 У1-У4 ЛР4 ЛР7 ЛР8-11
	1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	4/4	
	2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод VBS.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	4/4	
	1. Применение методов генерации ПСЧ		
Контрольные работы	*		
Раздел 3. Современная криптография			
Тема 3.1. Кодирование информации.	Содержание учебного материала, в том числе в форме практической подготовки	12/12	ОК1-5 ОК10
	1. Кодирование информации. Символьное кодирование. Смысловое кодирование.	6/6	

Компьютеризация шифрования.		Механизация шифрования.		ПК 2.1-2.3 31-34 У1-У4 ЛР4 ЛР7 ЛР8-11
		2. Представление информации в двоичном коде. Таблица ASCII. Компьютеризация шифрования. Аппаратное и программное шифрование		
		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	6/6	
		1. Кодирование информации		
		2. Программная реализация классических шифров		
		3. Изучение реализации классических шифров замены и перестановки в программе СrupTool или аналоге.		
	Контрольные работы	*		
Тема 3.2. Симметричные системы шифрования		Содержание учебного материала, в том числе в форме практической подготовки	8/8	ОК1-7 ОК10 ПК 2.1-2.4 31-34 У1-У6 ЛР4 ЛР7 ЛР8-11
		1. Общие сведения. Структурная схема симметричных криптографических систем	4/4	
		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		
		Лабораторные занятия	*	
		Практические занятия, в том числе в форме практической подготовки	4/4	
		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	8/8	ОК1-7 ОК10 ПК 2.1-2.4 31-34 У1-У6 ЛР4 ЛР7
		1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	4/4	
		2. Элементы теории чисел в криптографии с открытым ключом.		
		Лабораторные занятия	*	
		Практические занятия, в том числе в форме практической подготовки	4/4	
		1. Применение различных асимметричных алгоритмов.		
	2. Изучение программной реализации асимметричного алгоритма RSA			

			ЛР8-11
	Контрольные работы	*	
Тема 3.4. Аутентификация данных. Электронная подпись	Содержание учебного материала, в том числе в форме практической подготовки	10/10	ОК1-7
	1. Аутентификация данных. Общие понятия. ЭП. MAC.	4/4	ОК10
	2. Однонаправленные хеш-функции. Алгоритмы цифровой подписи		ПК 2.1-2.4
	Лабораторные занятия	*	31-34
	Практические занятия, в том числе в форме практической подготовки	6/6	У1-У6
	1. Применение различных функций хеширования, анализ особенностей хешей		ЛР4
	2. Применение криптографических атак на хеш-функции.		ЛР7
3. Изучение программно-аппаратных средств, реализующих основные функции ЭП		ЛР8-11	
Контрольные работы	*		
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	Содержание учебного материала, в том числе в форме практической подготовки	10/10	ОК1-7
	1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. аутентификация	4/4	ОК10
	2. Взаимная аутентификация. Односторонняя		ПК 2.1-2.4
	Лабораторные занятия	*	31-34
	Практические занятия, в том числе в форме практической подготовки	6/6	У1-У6
	1. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.		ЛР4
	2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.		ЛР7
Контрольные работы	*	ЛР8-11	
Тема 3.6. Криптозащита информации в сетях передачи данных	Содержание учебного материала, в том числе в форме практической подготовки	4/4	ОК1-7
	1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	4/4	ОК10
	2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.		ПК 2.1-2.4
	Лабораторные занятия	*	31-34
	Практические занятия, в том числе в форме практической подготовки	*	У1-У6
	Контрольные работы	*	ЛР4
			ЛР7
			ЛР8-11

Тема 3.7. Защита информации в электронных платежных системах	Содержание учебного материала, в том числе в форме практической подготовки	10/10	ОК1-7 ОК10 ПК 2.1-2.4 31-34 У1-У6 ЛР4 ЛР7 ЛР8-11
	1. Принципы функционирования электронных платежных систем.	6/6	
	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	4/4	
	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	10/10	ОК1-7 ОК10 ПК 2.1-2.6 31-34 У1-У10 ЛР4 ЛР7 ЛР8-11
	1. Скрытая передача информации в компьютерных системах.	6/6	
	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	4/4	
	1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ		
2. Реализация простейших стеганографических алгоритмов			
Контрольные работы	*		
Самостоятельная работа обучающихся		*	
Промежуточная аттестация экзамен		6/6	
Консультации		12/12	
Всего:		162	

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ МДК

3.1. Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы МДК предполагает наличие учебной лаборатории Программных и программно-аппаратных средств обеспечения информационной безопасности.

Площадь кабинета (лаборатории) – 65,4м².

Оборудование учебного кабинета(лаборатории): доска, автоматизированные рабочие места на 13 обучающихся с наличием локальной и глобальной компьютерной сети (13 стульев, 13 столов), автоматизированное рабочее место преподавателя, принтер, аудиокolonки, интерактивная маркерная доска, 3D принтер, мультимедиапроектор, сервер в лаборатории.

Основное оборудование: стенд «Требования к результатам освоения профессиональной образовательной программы», «Компьютер и здоровье», «Области использования вычислительной техники», комплект учебно-методической документации, комплект учебников по количеству обучающихся.

Демонстрационные средства обучения: тематические папки дидактических материалов.

Программное обеспечение общего и профессионального назначения.

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. Криптографическая защита информации в объектах информационной инфраструктуры: учебник, 1-е изд./ Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - ИЦ Академия, 2020 -288 с.

2. 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. Белов В.В. Проектирование информационных систем: учебник для студ. учреждений высш. проф. образования / В. В. Белов, В. И. Чистякова; под ред. В. В. Белова – М.: Издательский центр «Академия», 2013.

2. Гвоздева В.А., Лаврентьева И.Ю., Основы построения автоматизированных информационных систем, Москва, ИД Форум – ИНФРА-М, 2009.

3. Гвоздева Т.В., Баллод Б.А., Проектирование информационных систем: учеб.пособие / Т.В. Гвоздева, Б.А. Баллод. – Ростов н/Д: Феникс, 2009. – 508 с.

4. Емельянова Н.З., Устройство и функционирование информационных систем: учеб.пособие для СПО / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – 2-е изд., перераб. и доп. – М.: Форум, 2015. – 448 с.

5. Избачков Ю.С., Информационные системы: учебник для вузов [Гриф УМО МО РФ]. 3-е изд. / Избачков Ю.С., Петров В.Н [и др.]. – СПб.: Питер, 2011. – 544 с.

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 PROФобразование:

- Абрамов, Г. В. Проектирование и разработка информационных систем : учебное пособие для СПО / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. — Саратов : Профобразование, 2020. — 169 с. — ISBN 978-5-4488-0730-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование : [сайт]. — URL: <https://profspo.ru/books/88888> (дата обращения: 07.09.2020). — Режим доступа: для авторизир. пользователей.

Электронно-библиотечная система:

IPRBOOKS - <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)	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	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ Экзамен
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	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ Экзамен
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ

		Экзамен
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ Экзамен
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	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ Экзамен
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	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ Экзамен