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

Рабочая программа междисциплинарного курса

МДК 02.01 Программные и программно-аппаратные средства защиты информации

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Алексеевка
2022

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

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

СОДЕРЖАНИЕ

1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

МДК 02.01Программные и программно-аппаратные 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:

З.1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З.2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

З.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З.4 основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З.5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З.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 специфик ацией стандарта компетенции Ворлдскиллс Сетевое и системное администрирование, которые актуализируются при изучении междисциплинарного курса:

1) знать и понимать: как настраивать коммутацию уровня доступа, агрегации и ядра;

2) знать и понимать: как настраивать протоколы маршрутизации внутреннего и внешнего шлюза;

3) знать и понимать: как обеспечивать отказоустойчивость сети на уровне коммутации и маршрутизации;

4) знать и понимать: как применять базовые механизмы защиты от компрометации активного сетевого оборудования;

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 – 210 часа, в том числе: аудиторной учебной работы обучающегося - 180 часа, из них в форме практической подготовки – 150 часа; в том числе практических занятий – 48 часов; самостоятельной учебной работы обучающегося - 12 часов; консультаций - 12 часов, курсовая работа -30ч.

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 02.01Программные и программно-аппаратные средства защиты информации

3.1. Объем МДК и виды учебной работы

Вид учебной работы	Объем часов
1	2
Максимальная учебная нагрузка (всего)	**210**
Аудиторная учебная работа (обязательные учебные занятия) (всего)	**180**
из них в форме практической подготовки	**150**
в том числе:	
лекционные занятия	**102**
лабораторные работы	
практические занятия	**48**
курсовые работы	**30**
Самостоятельная работа обучающегося (всего) в том числе:	**12**
Консультации	12
Промежуточная аттестация в форме ***экзамена***	***6***

3.2. Тематический план и содержание МДК 02.01 Программные и программно-аппаратные средства защиты информации

1	2	3	4
	Всего:	**140**	

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 02.01. Программные и программно-аппаратные средства защиты информации		210	

Раздел 1. Основные принципы программной и программно-аппаратной защиты информации			
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**	ОК1-5 ОК10 ПК 2.1-2.2 З1 З2 У1 У2 ЛР4 ЛР7 ЛР8-11
	1. Предмет и задачи программно-аппаратной защиты информации	6/6	
	2. Основные понятия программно-аппаратной защиты информации		
	3. Классификация методов и средств программно-аппаратной защиты информации		
Тема 1.2. Стандарты безопасности	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**	ОК1-5 ОК10 ПК 2.1-.2.2 З1 З2 У1 У2
	1. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	4/4	
	2. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.		

	Практические занятия, в том числе в форме практической подготовки	6/6	ЛР4 ЛР7 ЛР8-11
	1. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.		
	2. Работа с содержанием нормативных правовых актов.		
	3. Обзор стандартов. Работа с содержанием стандартов		
Тема 1.3. Защищенная автоматизированная система	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**	ОК1-5 ОК10 ПК 2.1-.2.2, 2.3 З1 З2 З3 З4 У1 У2 У3 У4 ЛР4 ЛР7 ЛР8-11
	1. Автоматизация процесса обработки информации. Понятие автоматизированной системы.	6/6	
	2. Особенности автоматизированных систем в защищенном исполнении.		
	3. Основные виды АС в защищенном исполнении.		
	Практические занятия, в том числе в форме практической подготовки	4/4	
	1. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.		
	2. Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации.		
Тема 1.4. Дестабилизирующее воздействие на	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**	*ОК1-5* *ОК10* *ПК 2.1-*
	1. Источники дестабилизирующего воздействия на объекты защиты	6/6	
	2. Способы воздействия на информацию		

объекты защиты	3. Причины и условия дестабилизирующего воздействия на информацию		*2.3*
	Практические занятия, в том числе в форме практической подготовки		*З1-З4*
	1. Распределение каналов в соответствии с источниками воздействия на информацию	**4/4**	*У1-У4* *ЛР4* *ЛР7* *ЛР8-11*
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/8**	*ОК1-5* *ОК10* *ПК 2.1-2.3* *З1-З4* *У1-У4* *ЛР4* *ЛР7* *ЛР8-11*
	2. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД	2/0	
	3. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам		
	4. Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Шифрование.		
	Практические занятия, в том числе в форме практической подготовки	**2/2**	
	1. Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		
	Самостоятельная работа	2	
6Раздел 2. Защита автономных автоматизированных систем			
Тема 2.1. Основы защиты автономных автоматизированных	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/12**	*ОК1-7* *ОК10* *ПК 2.1-*
	2. Работа автономной АС в защищенном режиме	6/6	
	3. Алгоритм загрузки ОС. Штатные средства замыкания среды		

систем	4. Расширение BIOS как средство замыкания программной среды		*2.4* *З1-З4* *У1-У6* *ЛР4* *ЛР7* *ЛР8-11*
Тема 2.2.Защита программ от изучения	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**	*ОК1-7* *ОК10* *ПК 2.1-2.4* *З1-З4* *У1-У6* *ЛР4* *ЛР7* *ЛР8-11*
	1. Изучение и обратное проектирование ПО	6/6	
	2. Способы изучения ПО: статическое и динамическое изучение		
	3. Задачи защиты от изучения и способы их решения		
Тема 2.3. Вредоносное программное обеспечение	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**	*ОК1-7* *ОК10* *ПК 2.1-2.4* *З1-З4* *У1-У6* *ЛР4* *ЛР7*
	1. Вредоносное программное обеспечение как особый вид разрушающих воздействий	4/4	
	2. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения		
	Практические занятия, в том числе в форме практической подготовки	**2/2**	
	1. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		

			ЛР8-11
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**	*ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11*
	2. Несанкционированное копирование программ как тип НСД	4/4	
	3. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.		
	Практические занятия, в том числе в форме практической подготовки	**2/2**	
	1. Защита информации от несанкционированного копирования с использованием специализированных программных средств		
Тема 2.5. Защита информации на машинных носителях	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/12**	*ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11*
	2. Проблема защиты отчуждаемых компонентов ПЭВМ	6/6	
	3. Методы защиты информации на отчуждаемых носителях. Шифрование.		
	4. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.		
	Практические занятия, в том числе в форме практической подготовки	**6/6**	
	1. Применение средства восстановления остаточной информации на примере Foremost или аналога		
	2. Применение специализированного программно средства для восстановления удаленных файлов		
	3. Применение программ для безвозвратного удаления данных		
Тема 2.6. Аппаратные	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/4**	*ОК1-7*

средства идентификации и аутентификации пользователей	1. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	4/4	*ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11*
	2. Устройства Touch Memory		
	Практические занятия, в том числе в форме практической подготовки	*	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**	*ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11*
	1. Использование сетевых снифферов в качестве СОВ 2. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	6/6	
	3. Аппаратный компонент СОВ ***4.*** Программный компонент СОВ		
	Практические занятия, в том числе в форме практической подготовки	**2/2**	
	1. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений		
	Самостоятельная работа	2	
Раздел 3. Защита информации в локальных сетях			
Тема 3.1. Основы построения защищенных сетей	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/4**	*ОК1-9 ОК10 ПК 2.1-2.5*
	2. Стек протоколов TCP/IP. Особенности маршрутизации. Сети, работающие по технологии коммутации пакетов	4/4	
	3. Средства идентификации и аутентификации на разных уровнях протокола		

	TCP/IP, достоинства, недостатки, ограничения.		*З1-З6* *У1-У8* *ЛР4* *ЛР7* *ЛР8-11*
	Практические занятия, в том числе в форме практической подготовки	*	
Тема 3.2. Средства организации VPN	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/4**	*ОК1-9* *ОК10* *ПК 2.1-2.5* *З1-З6* *У1-У8* *ЛР4* *ЛР7* *ЛР8-11*
	1. Виртуальная частная сеть. Функции, назначение, принцип построения	4/4	
	2. Криптографические и некриптографические средства организации VPN		
	Практические занятия, в том числе в форме практической подготовки	*	
	Самостоятельная работа	2	
Раздел 4. Защита информации в сетях общего доступа			
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/12**	*ОК1-9* *ОК10* *ПК 2.1-2.5* *З1-З6* *У1-У8* *ЛР4* *ЛР7*
	1. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасностиМетоды защиты информации при работе в сетях общего доступа.	12/12	
	2. Основные типы firewall. Симметричные и несимметричные firewall. 3. Однохостовые и мультихостовые firewall.		
	4. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций.		

	5. Требования по сертификации межсетевых экранов		*ЛР8-11*
	Практические занятия, в том числе в форме практической подготовки	**4/4**	
	1. Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.		
	2. Изучение различных способов закрытия "опасных" портов		
	Самостоятельная работа	2	
Раздел 5. Защита информации в базах данных			
Тема 5.1. Защита информации в базах данных	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**	*ОК1-9 ОК10 ПК 2.1-2.5 З1-З6 У1-У8 ЛР4 ЛР7 ЛР8-11*
	1. Основные типы угроз. Модель нарушителя	6/6	
	2. Средства идентификации и аутентификации. Управление доступом . Средства контроля целостности информации в базах данных		
	3. Средства аудита и контроля безопасности. Критерии защищенности баз данных		
	4. Применение криптографических средств защиты информации в базах данных		
	Практические занятия, в том числе в форме практической подготовки	4/4	
	1. Изучение механизмов защиты СУБД MS Access		
	2. Изучение штатных средств защиты СУБД MSSQL Server	2	
	Самостоятельная работа		
Раздел 6. Мониторинг систем защиты			
Тема 6.1. Мониторинг систем защиты	**Содержание учебного материала, в том числе в форме практической подготовки**	8/2	*ОК1-9 ОК10 ПК 2.1-2.6 З1-З6*
	1. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	6/0	
	2. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25		

	3. Классификация отслеживаемых событий. Особенности построения систем мониторинга		*У1-У10 ЛР4 ЛР7 ЛР8-11*
	Практические занятия, в том числе в форме практической подготовки	2/2	
	1. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов. **2.** Проведение аудита ЛВС сетевым сканером		
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/2**	ОК1-9 ОК10 ПК 2.1-2.6 З1-З6 У1-У10 ЛР4 ЛР7 ЛР8-11
	1. Изучение требований о защите информации, не составляющей государственную тайну.	**4/0**	
	2. Изучение методических документов ФСТЭК по применению мер защиты.		
	Практические занятия, в том числе в форме практической подготовки	**2/2**	
	1. Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.		
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/0**	ОК1-9 ОК10 ПК 2.1-2.6 З1-З6 У1-У10 ЛР4 ЛР7
	2. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	**10/0**	
	3. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов		
	4. Изучение типовых решений для построения VPN на примере VipNet или других аналогов		

	5. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов		ЛР8-11
	Самостоятельная работа	**2**	
Курсовая работа		**30/30**	
Примерная тематика курсовых работ 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах *6.* Защита сред виртуализации			
Промежуточная аттестация ***экзамен***		**6**	
Консультации		**12**	
Всего:		**210**	

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) – 65,4м^2.

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, аудиоколонки, 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. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с

2. 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.

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 PROFобразование:

- 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 PROFобразование : [сайт]. — URL: https://profspo.ru/books/88888 (дата обращения: 07.09.2020). — 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

Контрольи оценка результатов освоения МДК осуществляется преподавателем в процессе проведения теоретических и практических занятий, дифференцированный зачет.

Результаты **(освоенные профессиональные компетенции) с учетом личностных результатов 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	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
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
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
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
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
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