ДЕПАРТАМЕНТ 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
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	20
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК	25

1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ
МДК 02.01 Программные 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:

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 –210 часа, в том числе: аудиторной учебной работы обучающегося - 180 часов, из них в форме практической подготовки – 6 часа; в том числе практических занятий – 48 часов; курсовая работа – 30 часов; самостоятельной учебной работы обучающегося – 12 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 02.01 Программные и программно-аппаратные 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 02.01 Программные и программно-аппаратные средства защиты информации		**210/6**	
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**	**6/0**	ОК1-5 ОК10 ПК 2.1-2.2 З1 З2 У1 У2 ЛР4
	Предмет и задачи программно-аппаратной защиты информации	6/6	
	Основные понятия программно-аппаратной защиты информации		
	Классификация методов и средств программно-аппаратной защиты информации		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	*	

	Контрольные работы	*	ЛР7,8-11
Тема 1.2. Стандарты безопасности	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/6**	ОК1-5 ОК10 ПК 2.1-.2.2 З1 З2 У1 У2 ЛР4 ЛР7 ЛР8-11
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	4/4	
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	6/2	
	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. Работа с содержанием нормативных правовых актов.		
	Обзор стандартов. Работа с содержанием стандартов		
	Контрольные работы	*	
Тема 1.3. Защищенная автоматизированная система	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/0**	ОК1-5 ОК10 ПК 2.1-.2.2, 2.3 З1 З2 З3 З4 У1 У2 У3 У4 ЛР4 ЛР7 ЛР8-11
	Автоматизация процесса обработки информации	4/0	
	Понятие автоматизированной системы.		
	Особенности автоматизированных систем в защищенном исполнении.		
	Основные виды АС в защищенном исполнении.		
	Методы создания безопасных систем		
	Методология проектирования гарантированно защищенных КС		
	Дискреционные модели		
	Мандатные модели		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	6/0	
	Учет, обработка, хранение и передача информации в АИС		
	Ограничение доступа на вход в систему.		

	Идентификация и аутентификация пользователей		
	Разграничение доступа.		
	Регистрация событий (аудит).		
	Контроль целостности данных		
	Уничтожение остаточной информации.		
	Управление политикой безопасности. Шаблоны безопасности		
	Криптографическая защита. Обзор программ шифрования данных		
	Управление политикой безопасности. Шаблоны безопасности		
	Контрольные работы	*	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание учебного материала, в том числе в форме практической подготовки**		ОК1-5 ОК10 ПК 2.1-2.3 З1-З4 У1-У4 ЛР4 ЛР7,8-11
	Источники дестабилизирующего воздействия на объекты защиты	4/0	
	Способы воздействия на информацию		
	Причины и условия дестабилизирующего воздействия на информацию		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**4/0**	
	1. Распределение каналов в соответствии с источниками воздействия		
	Контрольные работы	*	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание учебного материала, в том числе в форме практической подготовки**		ОК1-5 ОК10 ПК 2.1-2.3 З1-З4 У1-У4 ЛР4 ЛР7 ЛР8-11
	Понятие несанкционированного доступа к информации	6/0	
	Основные подходы к защите информации от НСД		
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам		
	Доступ к данным со стороны процесса		
	Особенности защиты данных от изменения. Шифрование.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**4/0**	
	Организация доступа к файлам		
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		
	Контрольные работы	*	
Раздел 2. Защита автономных автоматизированных систем			

Тема 2.1. Основы защиты автономных автоматизированных систем	**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
	Работа автономной АС в защищенном режиме	6/0	
	Алгоритм загрузки ОС. Штатные средства замыкания среды		
	Расширение BIOS как средство замыкания программной среды		
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)		
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	4/0	
	Контрольные работы	*	
Тема 2.2.Защита программ от изучения	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/0**	ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	Изучение и обратное проектирование ПО	6/0	
	Способы изучения ПО: статическое и динамическое изучение		
	Задачи защиты от изучения и способы их решения		
	Защита от отладки.		
	Защита от дизассемблирования		
	Защита от трассировки по прерываниям.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	*	
	Контрольные работы	*	
Тема 2.3. Вредоносное программное обеспечение	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/0**	ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	Вредоносное программное обеспечение как особый вид разрушающих воздействий	4/0	
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения		
	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.		
	Бот-неты. Принцип функционирования. Методы обнаружения		
	Классификация антивирусных средств. Сигнатурный и эвристический анализ		

	Защита от вирусов в "ручном режиме"		
	Основные концепции построения систем антивирусной защиты на предприятии		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**2/0**	
	1. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		
	Контрольные работы	*	
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание учебного материала, в том числе в форме практической подготовки**		ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	Несанкционированное копирование программ как тип НСД	4/0	
	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.		
	Привязка ПО к аппаратному окружению и носителям.		
	Защитные механизмы в современном программном обеспечении на примере MS Office		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**2/0**	
	Защита информации от несанкционированного копирования с использованием специализированных программных средств		
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)		
	Контрольные работы	*	
Тема 2.5. Защита информации на машинных носителях	**Содержание учебного материала, в том числе в форме практической подготовки**		ОК1-7 ОК10 ПК 2.1-2.4 З1-З4 У1-У6 ЛР4 ЛР7 ЛР8-11
	Проблема защиты отчуждаемых компонентов ПЭВМ.	6/0	
	Методы защиты информации на отчуждаемых носителях. Шифрование.		
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.		
	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов		
	Безвозвратное удаление данных. Принципы и алгоритмы.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	8/0	
	Применение средства восстановления остаточной информации на примере Foremost или		

	аналога		
	Применение специализированного программно средства для восстановления удаленных файлов		
	Применение программ для безвозвратного удаления данных		
	Применение программ для шифрования данных на съемных носителях		
	Контрольные работы	*	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**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 ЛР7,8-11
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	4/0	
	Устройства Touch Memory		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	*****	
	Контрольные работы	*	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/0**	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4 ЛР7 ЛР8-11
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	4/0	
	Использование сетевых снифферов в качестве СОВ		
	Аппаратный компонент СОВ		
	Программный компонент СОВ		
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.		
	Лабораторные занятия	*	
	Практические занятия, в том числе в форме практической подготовки	**2/0**	
	1. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений		
	Контрольные работы	*	
Раздел 3. Защита информации в локальных сетях			
Тема 3.1. Основы построения защищенных сетей	**Содержание учебного материала, в том числе в форме практической подготовки**	4/0	ОК1-7 ОК10 ПК 2.1-
	Сети, работающие по технологии коммутации пакетов		
	Стек протоколов TCP/IP. Особенности маршрутизации.		

	Штатные средства защиты информации стека протоколов TCP/IP.		2.6 З1-З4 У1-У10 ЛР4 ЛР7 ЛР8-11
	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.		
	Лабораторные занятия		
	Практические занятия, в том числе в форме практической подготовки		
	Контрольные работы		
Тема 3.2. Средства организации VPN	**Содержание учебного материала, в том числе в форме практической подготовки**	4/0	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4 ЛР7 ЛР8-11
	Виртуальная частная сеть. Функции, назначение, принцип построения		
	Криптографические и некриптографические средства организации VPN		
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.		
	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки		
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки		
	Лабораторные занятия		
	Практические занятия, в том числе в форме практической подготовки	2/0	
	Развертывание VPN		
	Контрольные работы		
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**	14/0	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4 ЛР7 ЛР8-11
	Методы защиты информации при работе в сетях общего доступа.		
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности		
	Основные типы firewall. Симметричные и несимметричные firewall.		
	Уровень 1. Пакетные фильтры Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня		
	Однохостовые и мультихостовые firewall.		
	Основные типы архитектур мультихостовых firewall.		
	Требования к каждому хосту исходя из архитектуры и выполняемых функций Требования по сертификации межсетевых экранов		
	Лабораторные занятия		
	Практические занятия, в том числе в форме практической подготовки	4/0	

	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.		
	Изучение различных способов закрытия "опасных" портов		
	Контрольные работы		
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**	6/0	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4 ЛР7 ЛР8-11
	Основные типы угроз. Модель нарушителя		
	Средства идентификации и аутентификации. Управление доступом		
	Средства контроля целостности информации в базах данных		
	Средства аудита и контроля безопасности. Критерии защищенности баз данных		
	Применение криптографических средств защиты информации в базах данных		
	Лабораторные занятия		
	Практические занятия, в том числе в форме практической подготовки	4/0	
	Изучение механизмов защиты СУБД MS Access		
	Изучение штатных средств защиты СУБД MSSQL Server		
	Контрольные работы		
Раздел 6. Мониторинг систем защиты			
Тема 6.1. Мониторинг систем защиты	**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
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	6/0	
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25		
	Классификация отслеживаемых событий. Особенности построения систем мониторинга		
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.		
	Классификация сетевых мониторов		
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.		
	Лабораторные занятия		
	Практические занятия, в том числе в форме практической подготовки	2/0	
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере		

	RealSecure, SNORT, NFR или других аналогов		
	Проведение аудита ЛВС сетевым сканером		
	Контрольные работы		
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/0**	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4 ЛР7 ЛР8-11
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты	2/0	
	Лабораторные занятия		
	Практические занятия, в том числе в форме практической подготовки	2/2	
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке		
	Контрольные работы		
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**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
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	8/0	
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов		
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов		
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов		
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов		
	Лабораторные занятия		
	Практические занятия, в том числе в форме практической подготовки	*	
	Контрольные работы		
Курсовая работа	**Курсовая работа**	30/0	
Самостоятельная работа обучающихся	1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему	12/0	

	4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты 6. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 7. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. 8. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.		
Промежуточная аттестация ***экзамен***		**6/0**	
Консультации		**12/0**	
Всего:		**210/6**	

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. 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:

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	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных	• тестирование, • экзамен квалификационный, • экспертное

программно-аппаратных средств защиты информации.	средств защиты информации	наблюдение выполнения лабораторных работ, • 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	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

последствий компьютерных атак.		видов работ на практике