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

Рабочая программа профессионального модуля

ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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 ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	9
4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	25
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ДЕЯТЕЛЬНОСТИ)	31

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля 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 и соответствующих профессиональных компетенций (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 ПМ – требования к результатам освоения профессионального модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы профессионального модуля должен:

иметь практический опыт в:

- установки, настройки программных средств защиты информации в автоматизированной системе;
- обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;

- решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

- применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

- учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

- работы с подсистемами регистрации событий;

- выявления событий и инцидентов безопасности в автоматизированной системе.

уметь:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

- применять программные и программно-аппаратные средства для защиты информации в базах данных;

- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

- применять математический аппарат для выполнения криптографических преобразований;

- использовать типовые программные криптографические средства, в том числе электронную подпись;

- применять средства гарантированного уничтожения информации;

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

- 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:

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

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

- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

- основные понятия криптографии и типовых криптографических методов и средств защиты информации;

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

- 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 профессионального модуля:

всего – 594 часов, в том числе:

максимальной учебной нагрузки обучающегося - 284 часа, из них в форме практической подготовки – 24 часа, в том числе:

практических занятий 104 часов,

теоретических занятий 190 часов;

курсовая работа – 30 часов; самостоятельной учебной работы обучающегося – 12 часов; консультации 24 часов; учебной практики – 108 часов; производственной практики – 108 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения рабочей программы профессионального модуля является овладение обучающимися видом деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами, в том числе 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 ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Объем профессионального модуля и виды учебной работы

Коды профессиональных компетенций, коды личностных результатов	Наименования разделов профессионального модуля*	Объем профессионального модуля, ак. час									
		Работа обучающихся во взаимодействии с преподавателем									Самостоятельная работа обучающегося
		Всего часов (макс. учебная нагрузка и практики)	В т.ч. в форме практ. подготовки	Обучение по МДК				Практика		Консультации	
				Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч. лабораторные работы и практические занятия в форме практической подготовки, часов	в т.ч., курсовая работа (проект), часов	Учебная, часов	Производственная, часов		
1	2	3	4	5	6	7	8	9	10	11	12
ПК 2.1 - ПК 2.6 ОК.01.-ОК.10 ЛР 4,7,9-11	Раздел I модуля. МДК 02.01. Программные и программно-аппаратные средства защиты информации	**210**	**6**	**180**	48	6	30	*	*	12	**12**
ПК 2.1 - ПК 2.6 ОК.01.-ОК.10 ЛР 4,7,9-11	Раздел I I модуля МДК 02.02 Криптографические средства защиты информации	**162**	**6**	**144**	56	6	*	*	*	**12**	*
ПК 2.1 - ПК 2.6 ОК.01.-ОК.10 ЛР 4,7,9-11	УП 02. Учебная практика	**108**	**6**	*	*	**6**	*	**108**	*	*	*
ПК 2.1 - ПК 2.6 ОК.01.-ОК.10 ЛР 4,7,9-11	ПП. 02. Производственная практика	**108**	**6**	*	*	**6**	*	*	**108**	*	*
Экзамен по модулю		**6**									
	Всего:	**594**	**24**	**594**	104	**24**	**30**	**108**	**108**	**24**	**12**

3.2. Содержание профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

1	2	3
Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	**Содержание учебного материала, лабораторные работы и Практические занятия, в том числе в форме практической подготовки, самостоятельная работа обучающихся, курсовая работа (проект)**	**Объем часов**
1	**2**	**3**
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		**210**
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**
	Предмет и задачи программно-аппаратной защиты информации	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	*
Тема 1.2. Стандарты безопасности	**Содержание учебного материала, в том числе в форме практической подготовки**	**10**
	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
	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
	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**
	Автоматизация процесса обработки информации	4
	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
	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**	
	Источники дестабилизирующего воздействия на объекты защиты	4
	Способы воздействия на информацию	
	Причины и условия дестабилизирующего воздействия на информацию	
	Лабораторные занятия	*
	Практические занятия, в том числе в форме практической подготовки	**4**
	1. Распределение каналов в соответствии с источниками воздействия	
	Контрольные работы	*
Тема 1.5. Принципы программно-аппаратной	**Содержание учебного материала, в том числе в форме практической подготовки**	
	Понятие несанкционированного доступа к информации	6

защиты информации от несанкционированного доступа	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**
	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**
	Работа автономной АС в защищенном режиме	6
	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
	Контрольные работы	*
Тема 2.2.Защита программ от изучения	**Содержание учебного материала, в том числе в форме практической подготовки**	**6**
	Изучение и обратное проектирование ПО	6
	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**
	Вредоносное программное обеспечение как особый вид разрушающих воздействий	4

	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**
	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**	
	Несанкционированное копирование программ как тип НСД	4
	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**
	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**	
	Проблема защиты отчуждаемых компонентов ПЭВМ.	6
	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

	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**
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	4
	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**
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	4
	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**
	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
	Сети, работающие по технологии коммутации пакетов	
	Стек протоколов TCP/IP. Особенности маршрутизации.	
	Штатные средства защиты информации стека протоколов TCP/IP.	
	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
	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
	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
	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
	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
	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

	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**
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	6
	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
	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**
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты	2
	Лабораторные занятия	
	Практические занятия, в том числе в форме практической подготовки	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**
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	8

	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** **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 Защита сред виртуализации	30
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 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)	12

	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.	
Консультации		**12**
Промежуточная аттестация	**Экзамен**	**6**
Всего по МДК 02.01:		**210**
МДК 02.02 Криптографические средства защиты информации		**162**
Раздел 1. Математические основы криптографии		
Тема 1.1. Математические основы криптографии	**Содержание учебного материала, в том числе в форме практической подготовки**	**32**
	1. Предмет и задачи криптографии. История криптографии. Основные термины	
	2. Элементы теории множеств. Группы, кольца, поля.	
	3. Делимость чисел. Признаки делимости. Простые и составные числа.	
	4. Основная теорема арифметики. Наибольший общий делитель. Взаимно	
	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		
	Содержание учебного материала, в том числе в форме практической подготовки	**14**

Тема 2.1. Методы криптографического защиты информации	1. Классификация основных методов криптографической защиты. Методы симметричного шифрования	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
	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**
	1. Основные методы криптоанализа. Криптографические атаки.	6
	2. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	
	3. Перспективные направления криптоанализа, квантовый криптоанализ.	
	Лабораторные занятия	*
	Практические занятия, в том числе в форме практической подготовки	8
	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**
	1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	4
	2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Лабораторные занятия	*
	Практические занятия, в том числе в форме практической подготовки	**4**
	2. Применение методов генерации ПСЧ	

	Контрольные работы	*
Раздел 3. Современная криптография		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала, в том числе в форме практической подготовки**	**12**
	1. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования.	6
	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**
	1. Кодирование информации	
	2. Программная реализация классических шифров	
	3. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
	Контрольные работы	*
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала, в том числе в форме практической подготовки**	**8**
	1. Общие сведения. Структурная схема симметричных криптографических систем	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
	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**
	1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	4
	2. Элементы теории чисел в криптографии с открытым ключом.	
	Лабораторные занятия	*
	Практические занятия, в том числе в форме практической подготовки	4

	1. Применение различных асимметричных алгоритмов.	
	2. Изучение программной реализации асимметричного алгоритма RSA	
	Контрольные работы	*
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала, в том числе в форме практической подготовки**	**10**
	1. Аутентификация данных. Общие понятия. ЭП. MAC.	4
	2. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Лабораторные занятия	*
	Практические занятия, в том числе в форме практической подготовки	**6**
	2. Применение различных функций хеширования, анализ особенностей хешей	
	3. Применение криптографических атак на хеш-функции.	
	4. Изучение программно-аппаратных средств, реализующих основные функции ЭП	
	Контрольные работы	*
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала, в том числе в форме практической подготовки**	**10**
	1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. аутентификация	4
	2. Взаимная аутентификация. Односторонняя	
	Лабораторные занятия	*
	Практические занятия, в том числе в форме практической подготовки	**6**
	1. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
	Контрольные работы	*
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала, в том числе в форме практической подготовки**	**4**
	1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	4
	2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
	Лабораторные занятия	*
	Практические занятия, в том числе в форме практической подготовки	*
	Контрольные работы	*
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала, в том числе в форме практической подготовки**	**10**
	1. Принципы функционирования электронных платежных систем.	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**
	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**
	1. Скрытая передача информации в компьютерных системах.	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**
	2. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	3. Реализация простейших стеганографических алгоритмов	
	Контрольные работы	*
Самостоятельная работа	Самостоятельная работа обучающихся 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии	*

	14. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 15. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	
Консультации		**12**
Промежуточная аттестация	***Ээкзамен***	**6**
Всего:		**162**
Учебная практика **Виды работ:** −Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах −Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности −Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности −Составление документации по учету, обработке, хранению и передаче конфиденциальной информации −Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации −Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. −Устранение замечаний по результатам проверки −Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. −Применение математических методов для оценки качества и выбора наилучшего программного средства – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи. – **Промежуточная аттестация** Дифференцированный зачет		**108** **2**

Производственная практика **Виды работ:** - Изучение инструкций по охране труда. Изучение инструкции по технике безопасности и пожароопасности, схем аварийных проходов и выходов. Изучение правил внутреннего распорядка, - правил и норм охраны труда, техники безопасности при работе с вычислительной техникой. - Знакомство со структурой и инфраструктурой организации, системой взаимоотношений между ее отдельными подразделениями, основными направлениями деятельности, отношениями с партнерами. - Анализ принципов построения систем информационной защиты производственных подразделений. - Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. - Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; - Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении - Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации - Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. - -Дифференцированный зачет..	**108** **2**
Экзамен по модулю	**6**
Всего	**594**

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению:

Реализация рабочей программы профессионального модуля предполагает наличие учебного кабинета лаборатории программных и программно – аппаратных средств защиты информации

Оборудование учебного кабинета:

доска; автоматизированные рабочие места на 14 обучающихся с наличием локальной и глобальной компьютерной сети на базе вычислительной техники, подключенные к локальной вычислительной сети и сети Интернет: 14 компьютерных столов, 14 стульев; 8 ученических столов; 16 стульев; автоматизированное рабочее место преподавателя (ПК – 1 шт., принтер – 1 шт.), мультимедийный проектор – 1 шт., интерактивная доска – 1 шт., маркерная доска – 1 шт., антивирусный программный комплекс, лабораторные учебные макеты.

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

Предусматриваются следующие виды практик, реализуемых в форме практической подготовки: учебная практика, производственная практика (по профилю специальности). Практики проводятся в рамках дуального обучения концентрировано. В последний день практики сдается дифференцированный зачет

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся – предприятиях на основе договоров, заключаемых между ОГАПОУ «Алексеевский колледж» и предприятиями.

Материально-техническая база должна соответствовать действующим санитарным и противопожарным нормам.

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.

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

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

Дополнительные источники:

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

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

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

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

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

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

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

23. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

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

25. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

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

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

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

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

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

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

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

33. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005.

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

35. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

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

37. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

38. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

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

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

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

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

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

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

45. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

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

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

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

Электронные издания (электронные ресурсы):

1. 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

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

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/

4.3. Общие требования к организации образовательного процесса

Освоение программы модуля базируется на изучении общепрофессиональных дисциплин Основы информационной безопасности, Организационно-правовое обеспечение информационной безопасности, Защита информационных процессов в компьютерных системах и профессионального модуля ПМ 01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках модуля является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля.

При освоении программ профессиональных модулей в последнем семестре изучения формой промежуточной аттестации по модулю является экзамен по модулю, который представляет собой форму независимой оценки результатов обучения с участием работодателей. Условием допуска к экзамену по модулю является успешное освоение обучающимися всех элементов программы профессионального модуля теоретической части модуля (МДК) и практик.

Экзамен по модулю проверяет готовность обучающегося к выполнению указанного вида профессиональной деятельности и сформированность у него профессиональных компетенций. Итогом проверки является однозначное решение: «вид деятельности освоен / не освоен». В зачетной книжке запись будет иметь вид: «ВД освоен» или «ВД не освоен». Данное решение подтверждается оценкой по пятибалльной системе.

4.4. Кадровое обеспечение образовательного процесса

Реализация рабочей программы профессионального модуля должна обеспечиваться педагогическими кадрами, имеющими высшее образование, соответствующее профилю модуля. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального цикла, эти преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ДЕЯТЕЛЬНОСТИ)

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	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты	— тестирование, — экзамен квалификационный, — экспертное наблюдение выполнения лабораторных работ,

защиты информации.	информации	– экспертное наблюдение выполнения практических работ, – оценка решения ситуационных задач, – оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	• тестирование, • экзамен квалификационный, • экспертное наблюдение выполнения лабораторных работ, • экспертное наблюдение выполнения практических работ, • оценка решения ситуационных задач, • оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и 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 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	• тестирование, • экзамен квалификационный, • экспертное наблюдение выполнения лабораторных работ, • экспертное наблюдение выполнения практических работ, • оценка решения ситуационных задач, • оценка процесса и результатов выполнения видов работ на практике

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