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

Рабочая программа профессионального модуля

ПМ. 02 Соадминистирирование баз данных и серверов

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Алексеевка
2022

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

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

СОДЕРЖАНИЕ

стр.

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:

- установка, настройка программных средств защиты информации в автоматизированной системе;
- обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- использование программных и программно-аппаратных средств для защиты информации в сети;

- тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации ;
- решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;
- применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;
- учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности;
- работа с подсистемами регистрации событий;
- выявление 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 Сетевое и системное администрирование, которые актуализируются при изучении междисциплинарного курса:

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

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

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

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

1.3. Планируемые личностные результаты освоения рабочей программы

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

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

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

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

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

1.4. Количество часов на освоение рабочей программы профессионального модуля:

Всего – 594 часов, в том числе:

максимальная учебная нагрузка обучающегося – 324 часа, из них в форме практической подготовки – 466 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 216 часа, в том числе практические занятия – 104часов;

консультаций – 24 часов;

самостоятельной работы – 12часов;

курсовой работы – 30 часов;

учебной практики – 108 часов; производственной практики – 108 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Код	Наименование результата обучения
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций, коды личностных результатов	Наименование 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 – 2.6 ЛР 4,7,10,11	МДК 02.01 Программные и программно-аппаратные средства защиты информации	210	**150**	**180**	48	48	30		*	12	12
ПК 2.1 – 2.6 ЛР 4,7,10,11	МДК 02.02 Криптографические средства защиты информации	162	**100**	**144**	56	56				12	
ПК 2.1 – 2.6 ЛР 4,7,10,11	УП 02 Учебная практика	108	**108**					**108**			
ПК 2.1 – 2.6 ЛР 4,7,10,11	ПП 02Производственная практика (по профилю специальности)	108	**108**						**108**		
ПК 2.1 – 2.6. ЛР 4,7,10,11	ЭК	6					-				

	Всего:	**594**	**466**	**324**	**104**	**104**	**30**	**108**	**108**	**24**	**12**

3.2. Содержание обучения по профессиональному модулю ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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	
МДК 02.01. Программные и программно-аппаратные средства защиты информации		210
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**
	1. Предмет и задачи программно-аппаратной защиты информации	6/6
	2. Основные понятия программно-аппаратной защиты информации	

1	2	
	3. Классификация методов и средств программно-аппаратной защиты информации	
Тема 1.2. Стандарты безопасности	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**
	1. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	4/4
	2. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	Практические занятия, в том числе в форме практической подготовки	6/6
	1. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	2. Работа с содержанием нормативных правовых актов.	
	3. Обзор стандартов. Работа с содержанием стандартов	
Тема 1.3. Защищенная автоматизированная система	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**
	1. Автоматизация процесса обработки информации. Понятие автоматизированной системы.	6/6
	2. Особенности автоматизированных систем в защищенном исполнении.	

1	2	
	3. Основные виды АС в защищенном исполнении.	
	Практические занятия, в том числе в форме практической подготовки	4/4
	1. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.	
	2. Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации.	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**
	1. Источники дестабилизирующего воздействия на объекты защиты	6/6
	2. Способы воздействия на информацию	
	3. Причины и условия дестабилизирующего воздействия на информацию	
	Практические занятия, в том числе в форме практической подготовки	**4/4**
	1. Распределение каналов в соответствии с источниками воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/8**
	2. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД	2/0
	3. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	

1	2	
	4. Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Шифрование.	
	Практические занятия, в том числе в форме практической подготовки	**2/2**
	1. Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	
	Самостоятельная работа	2
6Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/12**
	2. Работа автономной АС в защищенном режиме	6/6
	3. Алгоритм загрузки ОС. Штатные средства замыкания среды	
	4. Расширение BIOS как средство замыкания программной среды	
Тема 2.2.Защита программ от изучения	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**
	1. Изучение и обратное проектирование ПО	6/6
	2. Способы изучения ПО: статическое и динамическое изучение	
	3. Задачи защиты от изучения и способы их решения	
Тема 2.3. Вредоносное программное	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**
	1. Вредоносное программное обеспечение как особый вид разрушающих	4/4

1	2	
обеспечение	воздействий	
	2. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	
	Практические занятия, в том числе в форме практической подготовки	
	1. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	**2/2**
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**
	2. Несанкционированное копирование программ как тип НСД	4/4
	3. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	
	Практические занятия, в том числе в форме практической подготовки	
	1. Защита информации от несанкционированного копирования с использованием специализированных программных средств	**2/2**
Тема 2.5. Защита информации на машинных носителях	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/12**
	2. Проблема защиты отчуждаемых компонентов ПЭВМ	6/6
	3. Методы защиты информации на отчуждаемых носителях. Шифрование.	
	4. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	

1	2	
	Практические занятия, в том числе в форме практической подготовки	
	1. Применение средства восстановления остаточной информации на примере Foremost или аналога	**6/6**
	2. Применение специализированного программно средства для восстановления удаленных файлов	
	3. Применение программ для безвозвратного удаления данных	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/4**
	1. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	4/4
	2. Устройства Touch Memory	
	Практические занятия, в том числе в форме практической подготовки	*
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**
	1. Использование сетевых снифферов в качестве СОВ 2. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	6/6
	3. Аппаратный компонент СОВ ***4.*** Программный компонент СОВ	
	Практические занятия, в том числе в форме практической подготовки	**2/2**
	1. Моделирование проведения атаки. Изучение инструментальных средств	

1	2	
	обнаружения вторжений	
	Самостоятельная работа	2
Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/4**
	2. Стек протоколов TCP/IP. Особенности маршрутизации. Сети, работающие по технологии коммутации пакетов	4/4
	3. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
	Практические занятия, в том числе в форме практической подготовки	*
Тема 3.2. Средства организации VPN	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/4**
	1. Виртуальная частная сеть. Функции, назначение, принцип построения	4/4
	2. Криптографические и некриптографические средства организации VPN	
	Практические занятия, в том числе в форме практической подготовки	*
	Самостоятельная работа	2
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/12**
	1. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасностиМетоды защиты информации при работе в сетях общего доступа.	12/12

1	2	
	2. Основные типы firewall. Симметричные и несимметричные firewall. 3. Однохостовые и мультихостовые firewall.	
	4. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций.	
	5. Требования по сертификации межсетевых экранов	
	Практические занятия, в том числе в форме практической подготовки	**4/4**
	1. Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	
	2. Изучение различных способов закрытия "опасных" портов	
	Самостоятельная работа	2
Раздел 5. Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/10**
	1. Основные типы угроз. Модель нарушителя	6/6
	2. Средства идентификации и аутентификации. Управление доступом . Средства контроля целостности информации в базах данных	
	3. Средства аудита и контроля безопасности. Критерии защищенности баз данных 4. Применение криптографических средств защиты информации в базах данных	
	Практические занятия, в том числе в форме практической подготовки	4/4

1	2	
	1. Изучение механизмов защиты СУБД MS Access	2
	2. Изучение штатных средств защиты СУБД MSSQL Server	
	Самостоятельная работа	
Раздел 6. Мониторинг систем защиты		
Тема 6.1. Мониторинг систем защиты	**Содержание учебного материала, в том числе в форме практической подготовки**	8/2
	1. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	6/0
	2. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	
	3. Классификация отслеживаемых событий. Особенности построения систем мониторинга	
	Практические занятия, в том числе в форме практической подготовки	2/2
	1. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов.	
	2. Проведение аудита ЛВС сетевым сканером	
Тема 6.2. Изучение мер защиты информации в информационных	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/2**
	1. Изучение требований о защите информации, не составляющей государственную тайну.	**4/0**

1	2	
системах	2. Изучение методических документов ФСТЭК по применению мер защиты.	
	Практические занятия, в том числе в форме практической подготовки	**2/2**
	1. Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/0**
	2. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	**10/0**
	3. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	
	4. Изучение типовых решений для построения VPN на примере VipNet или других аналогов	
	5. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	
	Самостоятельная работа	**2**
Курсовая работа		**30/30**
Примерная тематика курсовых работ 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации		

1	2	
с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах *6.* Защита сред виртуализации		
Промежуточная аттестация ***экзамен***		**6**
Консультации		**12**
Всего:		**210**

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**	**26/26**
	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.	
	13. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	14. Арифметические операции над большими числами.	
Раздел 2. Классическая криптография		
Тема 2.1. Методы	**Содержание учебного материала, в том числе в форме практической подготовки**	**14/14**
	1. Классификация основных методов криптографической защиты. Методы	8/8

криптографического защиты информации	симметричного шифрования	
	2. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	
	3. Методы перестановки. Табличная перестановка, маршрутная перестановка	
	4. Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	Практические занятия, в том числе в форме практической подготовки	6/6
	1. Применение классических шифров замены	
	2. Применение классических шифров перестановки	
	3. Применение метода гаммирования	
Тема 2.2. Криптоанализ	**Содержание учебного материала, в том числе в форме практической подготовки**	**14/14**
	1. Основные методы криптоанализа. Криптографические атаки.	6/6
	2. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	
	3. Перспективные направления криптоанализа, квантовый криптоанализ.	
	Практические занятия, в том числе в форме практической подготовки	8/8
	1. Криптоанализ шифра простой замены методом анализа частотности символов	
	2. Криптоанализ классических шифров методом полного перебора ключей	
	3. Криптоанализ шифра Вижинера	
	4. Криптоанализ шифра Вижинера	

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала, в том числе в форме практической подготовки**	**6/6**
	1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	4/4
	2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Практические занятия, в том числе в форме практической подготовки	**2/2**
	5. Применение методов генерации ПСЧ	
Раздел 3. Современная криптография		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала, в том числе в форме практической подготовки**	**12/6**
	1. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования.	6/0
	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	
	Практические занятия, в том числе в форме практической подготовки	**6/6**
	1. Кодирование информации	
	2. Программная реализация классических шифров	
	3. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
Тема 3.2.	**Содержание учебного материала, в том числе в форме практической подготовки**	**8/4**

Симметричные системы шифрования	1. Общие сведения. Структурная схема симметричных криптографических систем	4/0
	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	
	Практические занятия, в том числе в форме практической подготовки	4/4
	1.Изучение программной реализации симметричных шифров	
	2.Изучение программной реализации современных симметричных шифров	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала, в том числе в форме практической подготовки**	**8/4**
	1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	4/0
	2. Элементы теории чисел в криптографии с открытым ключом.	
	Практические занятия, в том числе в форме практической подготовки	4/4
	1. Применение различных асимметричных алгоритмов.	
	2. Изучение программной реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/6**
	1. Аутентификация данных. Общие понятия. ЭП. MAC.	4/0
	2. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Практические занятия, в том числе в форме практической подготовки	**6/6**
	1. Применение различных функций хеширования, анализ особенностей хешей	
	2. Применение криптографических атак на хеш-функции.	
	3. Изучение программно-аппаратных средств, реализующих основные функции ЭП	

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/6**
	1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. аутентификация	4/0
	2. Взаимная аутентификация. Односторонняя	
	Практические занятия, в том числе в форме практической подготовки	**6/6**
	1. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала, в том числе в форме практической подготовки**	**4/0**
	1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	4/0
	2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/4**
	1. Принципы функционирования электронных платежных систем.	6/0
	2. Электронные пластиковые карты. Персональный идентификационный номер	
	3. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Практические занятия, в том числе в форме практической подготовки	**4/4**
	1. Применение аутентификации по одноразовым паролям.	

	2. Реализация алгоритмов создания одноразовых паролей	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала, в том числе в форме практической подготовки**	**10/4**
	1. Скрытая передача информации в компьютерных системах.	6/0
	2. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	3. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Практические занятия, в том числе в форме практической подготовки	**4/4**
	1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	2. Реализация простейших стеганографических алгоритмов	
Промежуточная аттестация ***экзамен***		**6**
Консультации		**12**
Всего:		**162**

Учебная практика в форме практической подготовки **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.	**108**

− 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 . Дифференцированный зачет.	
Производственная практика в форме практической подготовки **Виды работ** 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**
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 Лаборатория программирования и баз данных.

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.

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 - учреждениях сферы информационных технологий на основе договоров, заключаемых между ОГАПОУ «Алексеевский колледж» и организациями.

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.

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

2. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего

профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.

Дополнительные источники:

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

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

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

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

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

Электронные издания (электронные ресурсы):

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

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcode/449548

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

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

Цифровая образовательная среда СПО PROFобразование:

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

Электронно-библиотечная система:

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

Веб-система для организации дистанционного обучения и управления им:

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

4.3. Общие требования к организации образовательного процесса

Освоение программы модуля базируется на изучении общепрофессиональных дисциплин Защита информационных процессов в компьютерных системах, Основы информационной безопасности и профессионального модуля ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

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 и стандарта компетенции Ворлдскиллс**	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.3. Осуществлять тестирование функций отдельных программных и	Выполнение перечня работ по тестированию функций отдельных программных и	Защита отчетов по практическим

программно-аппаратных средств защиты информации.	программно-аппаратных средств защиты информации	и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением различных видов работ