МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательноеучреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Колледж

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММАМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

по программе подготовки специалистов среднего звена (ППССЗ)среднего профессионального образования

Специальность:	*10.02.05. Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовки*
Уровень образования, на базе которого осваиваетсяППССЗ:	*основное общее образование*
Квалификация:	*техник по защите информации*
Форма обучения:	*очная*

Махачкала - 2021

2

Рабочая программа профессионального модуля «ПМ.02 Защита информации в автоматизированных системах программами и программно-аппаратными средствами» разработана на основе ФГОС СПО по специальности по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем от 9 декабря 2016 г. № 1553 утвержденного приказом Министерства образования и науки с учетом примерной основной образовательной программы.

Организация-разработчик: Колледж федерального государственного бюджетного образовательного учреждения высшего образования «Дагестанский государственный университет»

Автор-разработчик:
Шахбанова З.И. – преподаватель кафедры общепрофессиональных дисциплин Колледжа ДГУ
Шахбанова М.И. - преподаватель кафедры естественнонаучных и гуманитарных дисциплин Колледжа ДГУ ВО «Дагестанский государственный университет»

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин колледжа ДГУ

Протокол № 7 от «27» 02 2021г.

Зав. кафедрой _____ /Магомедова А.М./

Рабочая программа профессионального модуля согласована с учебно-методическим управлением
«16» 03 2021 г. _____
(подпись)

Программа профессионального модуля согласована с представителем работодателя
Нач. отдела информационной безопасности Минцифры РД
(полное наименование организации и должности руководителя)
Шестимов Артур Тагирович _____ (подпись)
ФИО
М.П.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММАМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»

1. Область применения программы

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программами и программно-аппаратными средствами является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.05.Обеспечение информационной безопасности автоматизированных систем для очного обучения студентов, имеющих основное общее образование, по программе базовой подготовки.

Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровья, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждаются в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Профессиональный модуль «Защита информации в автоматизированных системах программами и программно-аппаратными средствами» относится к профессиональному циклу ПССЗ.

1.3. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности: иметь практический опыт по защите информации в автоматизированных системах программными и программно-аппаратными средствами и осуществлению полномочий оператора электронно-вычислительных и вычислительных машин и соответствующие ему общие компетенции и профессиональные компетенции:

Общие компетенции

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной[5] документацией на государственном и иностранном языке.

Профессиональные компетенции

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.

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

Иметь практический опыт	– применения программно-аппаратных средств обеспечения информационной безопасности; – диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности; – мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности; – решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов; – обеспечение учета, обработки, хранения и передачи конфиденциальной информации; – применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности аппаратно-программных средств.
Уметь	– применять программно-аппаратные средства обеспечения информационной безопасности; – диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности; – оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности; – участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;

	– решать частные технические задачи, возникающих при аттестации объектов; – применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности аппаратно-программных средств.
Знать	– методы и формы применения применение программно-аппаратных средств обеспечения информационной безопасности; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, баз данных; – типовые модели управления доступом; – типовые средства , методы и протоколы идентификации, аутентификации и авторизации; – типовые средства и методы ведения аудита и обнаружения вторжений; – типовые средства обеспечения информационной безопасности в локальных и глобальных вычислительных сетях; – основные понятия криптографии и типовые криптографические методы защиты информации.

1.1. Количество часов, отводимое на освоение профессионального модуля

Всего часов 331

Из них на освоение МДК 259

на практики, в том числе производственную 72

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Код профессиональных компетенций	Наименование разделов профессионального модуля	Всего, часов	Объем времени, отведенный на освоение междисциплинарного курса(курсов)					Практика	
			Обязательная аудиторная учебная нагрузкаобучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	В т.ч. лабораторные работы и практические занятия, часов (в т.ч. практическая подготовка)	В т.ч. курсовая работа (проект), часов	Всего, часов	В т.ч. курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 2.1. ПК 2.4. ПК 2.5.	**МДК.02.01. Программные и программно-аппаратные средства обеспечения информационной безопасности**	**95**	**95**	48		-	-		-
ПК 2.1. ПК 2.2. ПК 2.5.	**МДК.02.02. Криптографические средства и методы защиты информации**	**95**	**95**	48		-	-		
ПК 2.1. ПК 2.2. ПК 2.6.	**МДК.02.03. Корпоративная защита внутренних угроз информационной безопасности**	**69**	**69**	36					
ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6	**Производственная практика, часов**	**72**							**72**
Всего:		**331**	**259**	**132**	**-**		**-**		**72**

2.2. Тематический план и содержание профессионального модуля «ПМ.02 Защита информации в автоматизированных системах программами и программно-аппаратными средствами»

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия,самостоятельная работа обучающихся, курсовая работ (проект) (если предусмотрены)	Объем часов
1	**2**	**3**
МДК.02.01. Программные и программно-аппаратные средства обеспечения информационной безопасности		**95**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание учебного материала**	**8**
	Цели, задачи и содержание курса. Основные понятия. Предмет и задачи программно-аппаратной защиты информации. Автоматизированная система. Структура и компоненты АС. Сети ЭВМ. Способы защиты конфиденциальности, целостности и доступности в КС.	*2*
	Практические занятия/ Лабораторные занятия	*4*
	1. Цели, задачи и содержание курса. 2. Основные понятия. 3. Предмет и задачи программно-аппаратной защиты информации. 4. Автоматизированная система. 5. Структура и компоненты АС. Сети ЭВМ. 6. Способы защиты конфиденциальности, целостности и доступности в КС.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.2.	**Содержание учебного материала**	**8**

Проблема защиты программного обеспечения информационных систем	Проблема защиты программного обеспечения информационных систем. Объекты защиты. Жизненный цикл программного обеспечения информационных систем. Технологическая и эксплуатационная безопасность программного обеспечения. Основные принципы обеспечения безопасности программного обеспечения. Защита программного обеспечения как система научных дисциплин. Уязвимости программного обеспечения. Угрозы безопасности программного обеспечения. Вредоносные программы. Несанкционированные исследование и копирование программ.	*2*
	Практические занятия/ Лабораторные занятия	*4*
	1. Проблема защиты программного обеспечения информационных систем. 2. Объекты защиты. 3. Жизненный цикл программного обеспечения информационных систем. 4. Технологическая и эксплуатационная безопасность программного обеспечения. 5. Основные принципы обеспечения безопасности программного обеспечения. 6. Защита программного обеспечения как система научных дисциплин. 7. Уязвимости программного обеспечения. 8. Угрозы безопасности программного обеспечения. 9. Вредоносные программы. 10. Несанкционированные исследование и копирование программ.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.3. Стандарты безопасности	**Содержание учебного материала**	**8**
	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). Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	*2*

	Практические занятия/ Лабораторные занятия	*4*
	1. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. 2. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). 3. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. 4. 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. 5. Работа с содержанием нормативных правовых актов.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*2*
Тема 1.4. Защищенная автоматизированная система	**Содержание учебного материала**	**8**
	Автоматизация процесса обработки информации. 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.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Автоматизация процесса обработки информации. 2. Понятие автоматизированной системы. 3. . Особенности автоматизированных систем в защищенном исполнении. 4. Основные виды АС в защищенном исполнении. Методы создания безопасных систем. 5. Методология проектирования гарантированно защищенных КС Дискреционные модели Мандатные модели.	

	6. Учет, обработка, хранение и передача информации в АИС 7. Ограничение доступа на вход в систему. 8. Идентификация и аутентификация пользователей 9. Разграничение доступа. 10. Регистрация событий (аудит). 11. Контроль целостности данных 12. Уничтожение остаточной информации. 13. Управление политикой безопасности. Шаблоны безопасности 14. Криптографическая защита. Обзор программ шифрования данных. 15. Управление политикой безопасности. Шаблоны безопасности	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*2*
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание учебного материала**	**8**
	Понятие несанкционированного доступа к информации. 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.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Организация доступа к файлам. 2. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД. 3. Понятие несанкционированного доступа к информации. 4. Основные подходы к защите информации от НСД. 5. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. 6. Доступ к данным со стороны процесса Особенности защиты данных от изменения. Шифрование.	
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в	*2*

	сетях.	
Раздел 2. Защита информации в локальных сетях		
Тема 2.1. Основы построения защищенных сетей	**Содержание учебного материала**	**8**
	Сети, работающие по технологии коммутации пакетов 14 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.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Сети, работающие по технологии коммутации пакетов. 2. Стек протоколов TCP/IP. Особенности маршрутизации. 3. Штатные средства защиты информации стека протоколов TCP/IP. 4. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения. 5. Виртуальная частная сеть. 6. Функции, назначение, принцип построения.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*2*
Тема 2.2. Средства организации VPN	**Содержание учебного материала**	**8**
	Виртуальная частная сеть. Функции, назначение, принцип построения 10 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.	*2*
	Практические занятия/ Лабораторные занятия:	*4*

	1. Виртуальная частная сеть. Функции, назначение, принцип построения. 2. Криптографические и некриптографические средства организации VPN. 3. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. 4. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. 5. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*2*
Тема 2.3. Обеспечение безопасности межсетевого взаимодействия	**Содержание учебного материала**	
	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.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Методы защиты информации при работе в сетях общего доступа. 16 Межсетевые экраны типа firewall. 2. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall. 3. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2. 4. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. 5. Proxy-сервера прикладного уровня. 6. Однохостовые и мультихостовые firewall. 7. Основные типы архитектур мультихостовых firewall. 8. Требования к каждому хосту исходя из архитектуры и выполняемых функций.	

	9. Требования по сертификации межсетевых экранов	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*2*
Тема 2.4. Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	**Содержание учебного материала**	**8**
	Сертификация средств защиты информации по требованиям безопасности информации. Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей. Методы проведения испытаний. Документация, представляемая на испытания. Статический анализ исходных текстов и исполняемых модулей ПО. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду. Контроль связей функциональных объектов по управлению и информации. Синтаксический контроль наличия заданных конструкций. Формирование и анализ маршрутов выполнения функциональных объектов.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Сертификация средств защиты информации по требованиям безопасности информации. 2. Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей. 3. Методы проведения испытаний. Документация, представляемая на испытания. 4. Статический анализ исходных текстов и исполняемых модулей ПО. 5. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов. 6. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду. 7. Контроль связей функциональных объектов по управлению и информации. 8. Синтаксический контроль наличия заданных конструкций. 9. Формирование и анализ маршрутов выполнения функциональных объектов.	

	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*2*
Раздел 4. Мониторинг систем защиты		
Тема 4.1. Мониторинг систем защиты	**Содержание учебного материала**	**8**
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. 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.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. 2. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25. 3. Классификация отслеживаемых событий. 4. Особенности построения систем мониторинга. 5. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. 6. Классификация сетевых мониторов. 7. Системы управления событиями информационной безопасности (SIEM). 8. Обзор SIEM-систем на мировом и российском рынке.	
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с учебной литературой, выполнение домашнего задания.	*2*
Тема 4.2. Изучение современных	**Содержание учебного материала**	**7**
	Изучение требований о защите информации, не составляющей государственную	*2*

программно-аппаратных комплексов	тайну. Изучение методических документов ФСТЭК по применению мер защиты. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol или других аналогов Изучение функционала и областей применения DLP систем на примере nfoWatchTrafficMonitor или других аналогов.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Изучение требований о защите информации, не составляющей государственную тайну. 2. Изучение методических документов ФСТЭК по применению мер защиты. 3. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов 4. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol или других аналогов. 5. Изучение типовых решений для построения VPN на примере VipNet или других аналогов. 6. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. 7. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов.	
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Тема 4.3. **Методы обеспечения технологической и эксплуатационной**	**Содержание учебного материала**	**8**
	Классификация вредоносных программ. Защита от вредоносных программ Методы тестирования программного обеспечения на его защищенность. Методы тестирования программ. Фаззинг программ. Методы защиты программ от	*2*

безопасности программного обеспечения	несанкционированного исследования. Классификация средств несанкционированного исследования программ. Способы защиты программ от несанкционированного исследования. Обфускация программ. Способы встраивания защитных механизмов в программное обеспечение. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Классификация вредоносных программ. 2. Защита от вредоносных программ. 3. Методы тестирования программного обеспечения на его защищенность. 4. Методы тестирования программ. 5. Фаззинг программ. 6. Методы защиты программ от несанкционированного исследования. 7. Классификация средств несанкционированного исследования программ. 8. Способы защиты программ от несанкционированного исследования. 9. Обфускация программ. Способы встраивания защитных механизмов в программное обеспечение. 10. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. 11. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. 12. Манипуляции с кодом программы. 13. Методы противодействия динамическим способам снятия защиты программ от копирования.	
	Консультации	*1*
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
МДК.02.02. Криптографические средства и методы защиты информации		***95***

Раздел 1. **Основные понятия и характеристика шифров**		
Тема 1.1 Основные понятия. Криптографическая система. Классификация шифров.	**Содержание учебного материала**	**8**
	Криптография. Цели криптографии. История развития криптографии. Классификация криптографических методов. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. Основные понятия: шифр, открытый текст, шифр текст, электронная подпись, хэш-функция. Математические примитивы. Криптографические алгоритмы. Криптографическая схема. Криптографическая система. Классификация шифров.	*2*
	Практические занятия/ Лабораторные занятия	*4*
	1. Криптография. 2. Цели криптографии. 3. История развития криптографии. 4. Классификация криптографических методов. 5. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. 6. Основные понятия: шифр, открытый текст, шифр текст, электронная подпись, хэш-функция. 7. Математические примитивы. 8. Криптографические алгоритмы. 9. Криптографическая схема. 10. Криптографическая система. 11. Классификация шифров.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.2 Алгебраическая модель шифра. Вероятностная модель шифра. Модели	**Содержание учебного материала**	**8**
	Алгебраическая модель шифра. Алгебраическая модель шифра замены. Алгебраическая модель шифра перестановки. Алгебраическая модель шифра гаммирования. Вероятностная модель шифра. Распределения на множествах открытых текстов,	*2*

открытых текстов.	ключей, шифр текстов. Математические модели открытых текстов.	
	Практические занятия/ Лабораторные занятия	*4*
	1. Алгебраическая модель шифра. 2. Алгебраическая модель шифра замены. 3. Алгебраическая модель шифра перестановки. 4. Алгебраическая модель шифра гаммирования. 5. Вероятностная модель шифра. 6. Распределения на множествах открытых текстов, ключей, шифр текстов. 7. Математические модели открытых текстов.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.3. Криптографическая и теоретическая стойкость шифров.	**Содержание учебного материала**	**8**
	Атаки на шифры. Понятие стойкости шифров. Классификация атак на шифры. Виды атак на схемы шифрования. Цели криптоанализа. Теоретико-информационная стойкость. Условная вероятность. Энтропия. Понятие абсолютно стойкого шифра. Теоретико-сложностная стойкость шифров. Понятие практической стойкости шифра. Модель противника.	*2*
	Практические занятия/ Лабораторные занятия	*4*

	1. Атаки на шифры. 2. Понятие стойкости шифров. 3. Классификация атак на шифры. 4. Виды атак на схемы шифрования. 5. Цели криптоанализа. 6. Теоретико-информационная стойкость. 7. Условная вероятность. 8. Энтропия. Понятие абсолютно стойкого шифра. 9. Теоретико-сложностная стойкость шифров. 10.Понятие практической стойкости шифра. 11.Модель противника.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*2*
Раздел 2. Симметричная криптография		
Тема 2.1. Блочные и поточные шифры. Принципы построения блочных шифров	**Содержание учебного материала**	**8**
	Классификация симметричных криптографических систем. Требования к блочным шифрам. Требования к поточным шифрам. Криптографические параметры узлов и блоков блочных шифров. Базовые криптографические преобразования блочных шифров. Способы реализации блочных шифров. Процедура развертывания ключа	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Классификация симметричных криптографических систем. 2. Требования к блочным шифрам. 3. Требования к поточным шифрам. 4. Криптографические параметры узлов и блоков блочных шифров. 5. Базовые криптографические преобразования блочных шифров. 6. Способы реализации блочных шифров. 7. Процедура развертывания ключа	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*2*
Тема 2.2.	**Содержание учебного материала**	**8**

Сеть Фейстеля. Шифр DES. Поточные шифры.	Сеть Фейстеля. Шифр DES. Основные преобразования. Алгоритм зашифрования. Алгоритм расшифрования. Процедура развертывания ключа. Типовые методы построения поточных шифров. Синхронные и самосинхронизирующиеся поточные шифры. Генераторы псевдослучайных последовательностей. Статистические характеристики генераторов псевдослучайных последовательностей. Методы усложнения последовательностей.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Сеть Фейстеля. 2. Шифр DES. 3. Основные преобразования. 4. Алгоритм зашифрования. 5. Алгоритм расшифрования. Процедура развертывания ключа. 6. Типовые методы построения поточных шифров. 7. Синхронные и самосинхронизирующиеся поточные шифры. 8. Генераторы псевдослучайных последовательностей. 9. Статистические характеристики генераторов псевдослучайных последовательностей. Методы усложнения последовательностей.	
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*2*
Раздел 3. Криптография с открытым ключом		
Тема 3.1. Односторонние функции, функции с секретом	**Содержание учебного материала**	**8**
	Элементы теории сложности. Односторонние функции. Односторонние функции с секретом. Примеры односторонних функций с секретом. Алгебраическая модель асимметричного шифра. Понятие открытого ключа.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Элементы теории сложности. 2. Односторонние функции. 3. Односторонние функции с секретом. 4. Примеры односторонних функций с секретом. 5. Алгебраическая модель асимметричного шифра. 6. Понятие открытого ключа.	

	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*2*
Тема 3.2. Схемы шифрования RSA и Эль-Гамаля	**Содержание учебного материала**	**8**
	Схема шифрования RSA. Процедура генерации ключей. Процедура шифрования. Схема Эль-Гамаля. Стойкость схем шифрования RSA и Эль-Гамаля.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Схема шифрования RSA. 2. Процедура генерации ключей. 3. Процедура шифрования. 4. Схема Эль-Гамаля. 5. Стойкость схем шифрования RSA и Эль-Гамаля.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*2*
Раздел 4.Электроная подпись.		
Тема 4.1. Понятие электронной подписи. Способы построения электронной подписи	**Содержание учебного материала**	**8**
	Понятие электронной подписи. Связь с понятием электронной подписи ФЗ-63. Процессы формирования и проверки электронной подписи. Алгебраическая модель схемы электронной подписи. Конструкция схемы электронной подписи на односторонней функции с секретом. Электронная подпись на основе схемы шифрования с открытым ключом, электронная подпись с извлечением сообщения, электронная подпись с дополнением.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Понятие электронной подписи. 2. Связь с понятием электронной подписи ФЗ-63. 3. Процессы формирования и проверки электронной подписи. 4. Алгебраическая модель схемы электронной подписи. 5. Конструкция схемы электронной подписи на односторонней функции с	

	секретом. 6. Электронная подпись на основе схемы шифрования с открытым ключом, электронная подпись с извлечением сообщения, электронная подпись с дополнением.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*2*
Тема 4.2. Криптографическая хэш-функция	**Содержание учебного материала**	**8**
	Криптографическая хэш-функция без ключа. Слабая хэш-функция. Сильная хэшфункция. Стойкость криптографической хэш-функции. Применение хэш-функций. Типовые конструкции криптографических хэш-функций. Хэш-функция ГОСТ Р 34.11–94. Конструкция хэш-функции на основе алгоритма шифрования. Шаговая функция хэширования.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Криптографическая хэш-функция без ключа. 2. Слабая хэш-функция. Сильная хэшфункция. 3. Стойкость криптографической хэш-функции. 4. Применение хэш-функций. 5. Типовые конструкции криптографических хэш-функций. 6. Хэш-функция ГОСТ Р 34.11–94. 7. Конструкция хэш-функции на основе алгоритма шифрования. 8. Шаговая функция хэширования.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*2*
Раздел 5. **Применение криптографических методов и средств для обеспечения информационной безопасности**		
Тема 5.1. Коды аутентификации сообщений.	**Содержание учебного материала**	
	Коды аутентификации сообщений. Методы построения кодов аутентификации сообщений. Основные понятия. Цели безопасности криптографических	*2*

Криптографические протоколы	протоколов. Протоколы передачи сообщений. Протоколы передачи ключей. Протоколы аутентификации.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Коды аутентификации сообщений. 2. Методы построения кодов аутентификации сообщений. 3. Основные понятия. Цели безопасности криптографических протоколов. Протоколы передачи сообщений. 4. Протоколы передачи ключей. 5. Протоколы аутентификации.	
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с учебной литературой, выполнение домашнего задания.	*2*
Тема 5.2. Управление ключами. Инфраструктура открытых ключей	**Содержание учебного материала**	**7**
	Универсальная модель жизненного цикла ключа. Управление ключами. Службы управления ключами. Назначение инфраструктуры открытых ключей. Удостоверяющий центр. Функции удостоверяющего центра. Сертификат открытого ключа	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Универсальная модель жизненного цикла ключа. 2. Управление ключами. 3. Службы управления ключами. 4. Назначение инфраструктуры открытых ключей. 5. Удостоверяющий центр. 6. Функции удостоверяющего центра. 7. Сертификат открытого ключа	
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Тема 5.3. Принципы разработки	**Содержание учебного материала**	**8**
	Общие принципы построения СКЗИ. Принципы применения криптографических	*2*

и модернизации СКЗИ. Нормативное обеспечение КМЗИ	механизмов защиты. Принципы применения инженерно-криптографических механизмов защиты. Положение ПКЗ-2005.Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств. Приказ ФАПСИ 152. Приказ ФСБ РФ 378.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Общие принципы построения СКЗИ. 2. Принципы применения криптографических механизмов защиты. 3. Принципы применения инженерно-криптографических механизмов защиты. Положение ПКЗ-2005. **4.** Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств. Приказ ФАПСИ 152. Приказ ФСБ РФ 378.	
	Консультации	*1*
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
МДК.02.03. Корпоративная защита внутренних угроз информационной безопасности		***69***
Раздел 1. Основные понятия и характеристика шифров		
Тема 1.1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	**Содержание учебного материала**	**12**
	Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке. Установка и настройка агентского мониторинга. Проведена синхронизация с LDAPсервером, раздел персоны заполнен корректно. Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность.	*2*
	Практические занятия/ Лабораторные занятия	*6*
	1. Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п. 2. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке.	

	3. Установка и настройка агентского мониторинга. 4. Проведена синхронизация с LDAPсервером, раздел персоны заполнен корректно. 5. Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*4*
Тема 1.2. Исследование (аудит) организации с целью защиты от внутренних угроз	**Содержание учебного материала**	**12**
	Угрозы информационной безопасности. Изучение структуры организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем. Определить объекты защиты. Перечень субъектов/персон сформулирован верно, роли пользователей, права доступа.	*2*
	Практические занятия/ Лабораторные занятия	*6*
	1. Угрозы информационной безопасности. 2. Самостоятельно изучить структуру организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем. 3. Определить объекты защиты. Перечень субъектов/персон сформулирован верно, роли пользователей, права доступа . 4. Определить каналы передачи данных и потенциальных утечек. Типы циркулирующих данных определены верно. 5. Выявить потоки передачи данных и возможные каналы утечки информации. Заполнить шаблон модели угроз . 6. Подготовить отчёт о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п. Определить перечень нормативных актов РФ, задействованных в рамках модели угроз. 7. Разработать перечень, описание и шаблоны нормативно -правовых документов организации по легальному применению корпоративной защиты от внутренних	

	угроз информационной безопасности.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*4*
Тема 1.3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	**Содержание учебного материала**	**12**
	Политика безопасности. Модифицировать политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. Работа с интерфейсом управления системы корпоративной защиты информации	*2*
	Практические занятия/ Лабораторные занятия	*6*
	1. Политика безопасности 2. Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания. 3. Использовать различные технологии защиты: печатей, бланков, графических объектов, баз данных и т.п. 4. Модифицировать политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата. 5. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности. **6.** Работа с интерфейсом управления системы корпоративной защиты информации	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*4*
Тема 1.4.	**Содержание учебного материала**	**12**
Технологии анализа и	Технологии анализа и защиты сетевого трафика. Развёртывание, настройка и	*2*

защиты сетевого трафика	проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре. Развёртывание, настройка и проверка работоспособности IDS - системы на существующей и вычислительной. Межсетевое взаимодействие и туннелированные. VPN. Централизованные политики безопасности. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий	
	Практические занятия/ Лабораторные занятия:	*6*
	1. Технологии анализа и защиты сетевого трафика. 2. Развёртывание, настройка и проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре. 3. Развёртывание, настройка и проверка работоспособности IDS -системы на существующей и вычислительной 4. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. Восстановление связи. 5. Обновление ключевой информации. VPN. Межсетевое взаимодействие и туннелированные. VPN. **6.** Централизованные политики безопасности. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*4*
Тема 1.5. Технологии агентского мониторинга	**Содержание учебного материала**	**11**
	Технологии агентского мониторинга. Продемонстрировать знание механизмов работы агентского мониторинга. Разработать и применить политики агентского мониторинга для работы с носителями и устройствами. Разработать и применить политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата	*2*
	Практические занятия/ Лабораторные занятия:	
	1. Технологии агентского мониторинга. 2. Продемонстрировать знание механизмов работы агентского мониторинга. 3. Разработать и применить политики агентского мониторинга для работы с	*6*

	носителями и устройствами . **4.** Разработать и применить политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата	
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*3*
Тема 1.6. Анализ выявленных инцидентов	**Содержание учебного материала**	**10**
	Анализ выявленных инцидентов. Подготовка отчётов о нарушениях. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. Проведение классификацию уровня угроз инцидентов. Оценка ущерба; Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса . Разработка план по дальнейшему расследованию. Текущий контроль (устный опрос) 11 выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.	*2*
	Практические занятия/ Лабораторные занятия:	*6*
	1. Анализ выявленных инцидентов. 2. Подготовка отчётов о нарушениях. 3. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов. 4. Проведение классификацию уровня угроз инцидентов. 5. Оценка ущерба; Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса. 6. Разработка план по дальнейшему расследованию. **7.** Текущий контроль (устный опрос) 11 выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*2*

Примерная тематика самостоятельной учебной работы при изучении раздела « Программные и программно-аппаратные средства обеспечения информационной безопасности» **Самостоятельная работа:** • Изучение рекомендованной литературы; • Подготовка к практическим занятиям; • Оформление в виде конспекта основных положений дисциплины; • Подготовка реферативных докладов. **Примерная тематика домашних заданий:** • Создание отказоустойчивых информационных систем; • Случайные угрозы; • Составление схемы подсистемы защиты от несанкционированного доступа. Основные признаки несанкционированного доступа. К информации; • Оптимизация взаимодействия пользователей и обслуживающего персонала; • Минимизация ущерба от аварий и стихийных бедствий; • Дублирование информации; • Модель защиты информации значение информационной безопасности для субъектов информационных отношений; • Изучение принципа написания вредоносного программного кода; • Изучение алгоритма электронной цифровой подписи Эль-Гамаля; • Изучение создание виртуальной машины; • Воздействие программных закладок на компьютеры; • Защита от программных закладок; • Классификация и общая характеристика программно-аппаратных средств защиты информации.	**22**

Примерная тематика самостоятельной учебной работы при изучении раздела «Криптографические средства и методы защиты информации» **Самостоятельная работа:** • Изучение рекомендованной литературы; • Подготовка к практическим занятиям; • Оформление в виде конспекта основных положений дисциплины; • Подготовка реферативных докладов. **Примерная тематика домашних заданий:** • Подготовка к практическим работам • Криптозащита информации в проводных и беспроводных сетях передачи данных; • Развитие шифрования в древней Руси и России. Развитие шифрования в древней Руси и России; • Тюремные шифры; • Методы стенографии; • Водяные знаки; • Туннелирование; • Поточное кодирование; • Решение задач по образцу; • Защита информации в электронных платежных системах.	***22***
Примерная тематика самостоятельной учебной работы при изучении раздела « Корпоративная защита внутренних угроз информационной безопасности» **Самостоятельная работа:** • Изучение рекомендованной литературы; • Подготовка к практическим занятиям; • Оформление в виде конспекта основных положений дисциплины; • Подготовка реферативных докладов. **Примерная тематика домашних заданий:** • подготовка к практическим работам; • развёртывание, настройка и проверка работоспособности vpn-сети на существующей и вычислительной инфраструктуре; • выполнение компрометации узлов, ключей, пользователей. восстановление связи. обновление ключевой	***21***

информации; • произвести настройку туннелирования между незащищенными узлами поверх защищенной сети; • развернуть структуру защищенной сети согласно схеме с помощью дистрибутивов; • установить межсетевое взаимодействие между разными сетями; • произвести перенастройку пользователей и узлов защищенной сети; • произвести проверку связи между узлами различных защищенных сетей; • субъекты, объекты защиты и факторы внутренней и внешней угрозы; • роль службы безопасности в обеспечении корпоративной безопасности и принципы организации её деятельности; • юридические аспекты корпоративной безопасности; • аудит защищенности ит-инфраструктуры; • анализ защищенности критичных информационных систем; • оценка рисков; • инструментальный анализ защищенности, osint; • выявление векторов атак, приоритизация шагов по устранению недостатков; • проведение работ с минимальным воздействием на ит-инфраструктуру; • анализ возможных последствий атак.	
Производственная практика по ПМ.02 Виды работ: • анализ принципов построения систем информационной защиты производственных подразделений4 • 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;	***72***

• 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	
Экзамен по модулю	
Всего максимальная нагрузка по ПМ.02.	***331***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оснащение аудитории:

- комплект учебной мебели: парты, стол преподавательский, стулья, доска;
- мультимедийная система: проектор, экран настенный, ноутбук.

Программное обеспечение ноутбука лекционных аудиторий:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

Практические занятия проводятся в кабинете интернет-технологий и информатики, оборудованным ПЭВМ с установленным программным обеспечением:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- система программирования «Microsoft Visual Studio Express»;
- программа просмотра pdf-документов Sumatra PDF Reader.

Для самостоятельной работы студентов используется кабинет интернет-технологий и информатики.

Оснащение кабинета:

- комплект учебной мебели: стол преподавательский, столы компьютерные, стулья
- персональные компьютеры, сетевой коммутатор, сетевая кабельная система.

Программное обеспечение:

- лицензионное программное обеспечение:
- ОС Microsoft Windows
- Антивирус Касперского
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

Производственная практика проводятся при освоении обучающимися профессиональных компетенций в рамках профессиональных модулей и реализовываются как в несколько периодов, так и рассредоточено, чередуясь с теоретическими занятиями в рамках профессиональных модулей.

Производственная практика проводится на предприятиях (в организациях) города и района. Оборудование предприятий (организаций) и технологическое оснащение рабочих мест производственной практики соответствует содержанию деятельности и дает возможность обучающемуся овладеть профессиональными

компетенциями по всем осваиваемым видам деятельности, предусмотренным программой с использованием современных технологий, материалов и оборудования.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд имеет печатные, электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Учебники и учебные пособия по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем находятся в свободном доступе для преподавателей и студентов в библиотеке Колледжа ДГУ, в том числе электронные издания на официальном сайте Колледжа ДГУ. Библиотека колледжа оборудована рабочими местами в читальном зале и выходом в Интернет для работы с электронными книгами, учебниками, учебными пособиями, размещёнными на сайте Колледжа ДГУ. В колледже созданы все условия, позволяющие широко использовать в образовательном процессе информационные технологии, своевременно обеспечивать обновление нормативной документации, необходимой информации и оперативный доступ к ней.

Колледж имеет выход в Интернет, работает электронная почта, созданы и поддерживаются сайты (официальный сайт ДГУ - www.dgu.ru), официальный сайт Колледжа ДГУ (http:/law.dgu.ru/college/).

Основная литература:

1. *Запечников, С. В.* Криптографические методы защиты информации : учебник для сузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва : Издательство Юрайт, 2021. - 309 с. - (Профессиональное образование). - ISBN 978-5-534-02574-3. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/468902

2. *Васильева, И. Н.* Криптографические методы защиты информации : учебник и практикум для сузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2020. - 349 с. - (Профессиональное образование). - ISBN 978-5-534-02883-6. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/450998

3. 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, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — URL : https://urait.ru/bcode/476997

Дополнительная литература:

2. Коржик В.И. Основы криптографии [Электронный ресурс]: Учебное пособие/ Коржик В.И., Яковлев В.А.- Электронно - текстовые данные.- СПб.:Интермедия, 2017.- 312 с.- Режим доступа: http://www.bibliocomplectator.ru/book/?id=66798.-

3. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — URL : https://urait.ru/bcode/469133
4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL : https://urait.ru/bcode/489745
5. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — URL : https://urait.ru/bcode/470279
6. ГОСТ 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г.www.standartgost.ru
7. ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств. 2002 г.www.standartgost.ru
8. ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. 2006 г.www.standartgost.ru
9. ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г.www.standartgost.ru
10. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. 2009 г.www.standartgost.ru
11. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. 2001 г.www.standartgost.ru
12. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.www.standartgost.ru
13. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru 3. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru
14. ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru 5. ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru

Интернет-ресурсы:

1. Электронно-библиотечная система издательства ЮРАЙТ - URL: www.: urait.ru
2. Электронно-библиотечная система «Университетская библиотека онлайн» www.biblioclub.ru
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс].

URL: http://elibrary.ru
4. Национальная электронная библиотека [Электронный ресурс]. URL: http://нэб.рф/.
5. Справочно-правовая система «КонсультантПлюс». URL: http://www.consultant.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных компетенций, формируемыхв рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и 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

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно-практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	- использование различных источников, включая электронные ресурсы, медиа ресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	-взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с	-грамотность устной и письменной речи	

учетом особенностей социального и культурного контекста.		
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	