АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

УТВЕРЖДАЮ

Директор АНО ПО БИТ

_____ В.В.Сергеев

«01» сентября 2021 г.

ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Калининград
2021 г.

Программа междисциплинарного курса разработана на основе Федерального государственного образовательного стандарта (далее — ФГОС) по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1553 и примерной основной образовательной программы СПО, разработанной ФУМО 2017 г.

Организация-разработчик: АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

Разработчик: _____ Околот Денис Ярославович, преподаватель

Рассмотрена
методической комиссией,
протокол № _____
от «____» _____2021 г.
председатель
_____Т.В. Славинская

СОДЕРЖАНИЕ

1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ «МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

1.1. Место дисциплины в структуре основной профессиональной образовательной программы: Программа «МДК.02.01 *ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»* является частью профессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности: 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

В результате изучения МДК.02.01 студент должен освоить основной вид деятельности ВД.2, выполнение работ по проектированию сетевой инфраструктуры, соответствующие ему общие и профессиональные компетенции.

1.1.1. Перечень общих компетенций

Учебная дисциплина «МДК.02.01 *ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»* наряду с другими учебными дисциплинами обеспечивает формирование следующих общих и профессиональных компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
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 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	***Защита информации в автоматизированных системах программными и программно-аппаратными средствами***
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.

Общие требования к личностным результатам выпускников СПО

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации программы воспитания**
Портрет выпускника СПО	
Осознающий себя гражданином и защитником великой страны.	**ЛР 1**
Готовый использовать свой личный и профессиональный потенциал для защиты национальных интересов России.	**ЛР 2**
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.	**ЛР 3**
Принимающий семейные ценности своего народа, готовый к созданию семьи и воспитанию детей; демонстрирующий	**ЛР 4**

неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания.	
Занимающий активную гражданскую позицию избирателя, волонтера, общественного деятеля.	**ЛР 5**
Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение.	**ЛР 6**
Готовый соответствовать ожиданиям работодателей: проектно мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость.	**ЛР 7**
Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы; управляющий собственным профессиональным развитием; рефлексивно оценивающий собственный жизненный опыт, критерии личной успешности.	**ЛР 8**
Уважающий этнокультурные, религиозные права человека, в том числе с особенностями развития; ценящий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности».	**ЛР 9**
Принимающий активное участие в социально значимых мероприятиях, соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России; готовый оказать поддержку нуждающимся.	**ЛР 10**
Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением.	**ЛР 11**
Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.	**ЛР 12**

1.1.3. В результате освоения дисциплины студент должен:

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

	программно-аппаратных средств защиты информации ; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; применять средства гарантированного уничтожения информации; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
знать	особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

	основные понятия криптографии и типовых криптографических методов и средств защиты информации; особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ «МДК 02.01 Программные и программно-аппаратные средства защиты информации»

2.1. Объем профессионального модуля МДК 02.01 и виды учебной работы

2.1. Структура дисциплины

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.						
			Обучение по МДК, в час.				Практики		Самостоятельная работа
			Всего	в том числе			учебная практика, часов	производственная практика, часов	
				Лабораторных и практических занятий	Теоретическое обучение	курсовая работа (проект), часов			
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	Применение программных и программно-аппаратных средств защиты информации	**148**	**122**	**48**	**44**	**30**	–	–	**14**

Количество часов, отводимое на освоение изучения дисциплины

Всего **148** час, из них

в том числе на консультацию промежуточной аттестации + Курсовой работы по МДК 01.04 - **12 часов**

2.2. Тематический план и содержание профессионального модуля «МДК 02.01 Программные и программно-аппаратные средства защиты информации»

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов	Уровень освоения	Осваиваемые элементы компетенций
1	2	3	4	5
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**222**		
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации				
		2		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**			
	1.Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
		2		
Тема 1.2. Стандарты безопасности	**Содержание**			
	2.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	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		

	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. Работа с содержанием нормативных правовых актов. Обзор стандартов. Работа с содержанием стандартов			
Тема 1.3. Защищенная автоматизированная система	**Содержание**	**2**		
	3.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	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**4**		
	2.Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.			
	3.Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации.Управление политикой безопасности. Шаблоны безопасности. Криптографическая защита. Обзор программ шифрования данных. Управление политикой безопасности. Шаблоны безопасности			
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**2**		
	4. Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		
	4.Распределение каналов в соответствии с источниками			

	воздействия на информацию			
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	**2**		
	5. 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	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		
	5.Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД			
Раздел 2. Защита автономных автоматизированных систем				
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**	**2**		
	6.Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка). Применение закладок, направленных на снижение эффективности средств, замыкающих среду.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
Тема 2.2.Защита программ от изучения	**Содержание**	**2**		
	7. Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям.		1	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
Тема 2.3. Вредоносное	**Содержание**	**4**		

программное обеспечение	8.Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения. Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	9.Бот-неты. Принцип функционирования. Методы обнаружения. Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии		2	
	Тематика практических занятий и лабораторных работ	**2**		
	6.Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО			
Промежуточная аттестация по МДК.02.01				
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**	**2**		
	10.Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		
	7.Защита информации от несанкционированного копирования с использованием специализированных программных средств. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)			
Тема 2.5. Защита	**Содержание**	**2**		

информации на машинных носителях	11.Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов. Безвозвратное удаление данных. Принципы и алгоритмы.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**8**		
	8.Применение средства восстановления остаточной информации на примере Foremost или аналога			
	9.Применение специализированного программно средства для восстановления удаленных файлов			
	10.Применение программ для безвозвратного удаления данных			
	11.Применение программ для шифрования данных на съемных носителях			
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**2**		
	12.Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ. Устройства Touch Memory		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**	**2**		
	13.СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ. Программный компонент СОВ. Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		
	12.Моделирование проведения атаки. Изучение			

	инструментальных средств обнаружения вторжений			
Раздел 3. Защита информации в локальных сетях				
Тема 3.1. Основы построения защищенных сетей	**Содержание**	**2**		
	14.Сети, работающие по технологии коммутации пакетов.Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
Тема 3.2. Средства организации VPN	**Содержание**	**4**		
	15.Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	16.Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки		2	
	Тематика практических занятий и лабораторных работ	**2**		
	13.Развертывание VPN			
Раздел 4. Защита информации в сетях общего доступа		**4**		
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**			
	17.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.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12

	18.Уровень 3. Proxy-сервера прикладного уровня. Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов		2	
	Тематика практических занятий и лабораторных работ	**4**		
	14.Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.			
	15.Изучение различных способов закрытия "опасных" портов			
Раздел 5. Защита информации в базах данных				
	Содержание	**2**		
Тема 5.1. Защита информации в базах данных	19.Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом. Средства контроля целостности информации в базах данных. Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**4**		
	16.Изучение механизмов защиты СУБД MS Access			
	17.Изучение штатных средств защиты СУБД MSSQL Server			
Раздел 6. Мониторинг систем защиты				
	Содержание	**4**		
Тема 6.1. Мониторинг систем защиты	20.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.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК.

	21.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	10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		
	18.Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов. Проведение аудита ЛВС сетевым сканером			
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	**2**		
	22.Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
	Тематика практических занятий и лабораторных работ	**2**		
	19.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	**Тематика практических занятий и лабораторных работ**	**10**		

современных программно-аппаратных комплексов.	20.Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов. 21.Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов. 22.Изучение типовых решений для построения VPN на примере VipNet или других аналогов. 23.Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. 24.Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов		2	ПК 2.1 – ПК 2.6 ОК. 1- ОК. 10 ЛР 01-12
Курсовая работа				
Примерная тематика курсовых работ Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) Проблема защиты информации в облачных хранилищах данных и ЦОДах Защита сред виртуализации	**30**		
Примерная тематика самостоятельной работы при изучении МДК.02.01 Изучение новых технологий хранения информации Статистика и анализ крупных утечек информации за год Поиск информации о новых видах атак на информационную систему	**46**		

Обзор современных программных и программно-аппаратных средств защиты Сравнительный анализ современных программных и программно-аппаратных средств защиты Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.			
Экзамен по профессиональному модулю	**12**		
Самостоятельные работы	**14**		
Всего:	**148**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:
*1 – **ознакомительный** (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);*
*2 – **репродуктивный** (выполнение деятельности по образцу, инструкции или под руководством);*
*3 – **продуктивный** (самостоятельное планирование и выполнение деятельности, решение проблемных задач).*

Учебная практика по разделу 1 модуля
Виды работ:
Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах
Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности
Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности
Составление документации по учету, обработке, хранению и передаче конфиденциальной информации

Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации
Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.
Устранение замечаний по результатам проверки
Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.
Применение математических методов для оценки качества и выбора наилучшего программного средства

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ «МДК 02.01 Программные и программно-аппаратные средства защиты информации»

3.1. Для реализации программы дисциплины профессионального модуля должны быть предусмотрены следующие специальные помещения:
Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».
Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.
Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:
рабочие места студентов, оборудованные персональными компьютерами;
лабораторные учебные макеты;
рабочее место преподавателя;
учебно-методическое обеспечение модуля;
интерактивная доска, комплект презентаций;
антивирусные программные комплексы;
программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
средства уничтожения остаточной информации в запоминающих устройствах;
программные средства криптографической защиты информации.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе.

3.2.1 Основные печатные источники:

1.Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.
2.Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2018.- 248 с.

3.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2019. – 184 с.
4.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.
5.Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2019. – 336с
6.Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2018.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
7.Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2019. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности
8.Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2019
9.Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019
10.Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2018. – 416 с.

3.2.2. Дополнительные печатные источники:

1.Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2016. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2016 г
2.Федеральный закон от 27 июля 2016 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3.Федеральный закон от 27 июля 2016 г. № 152-ФЗ «О персональных данных».
4.Федеральный закон от 27 декабря 2016 г. № 184-ФЗ «О техническом регулировании».
5.Федеральный закон от 4 мая 2017 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6.Федеральный закон от 30 декабря 2017 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7.Указ Президента Российской Федерации от 16 августа 2017 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8.Указ Президента Российской Федерации от 6 марта 2017 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9.Указ Президента Российской Федерации от 17 марта 2018 г. № 351 «О мерах по обеспечению информационной безопасности Российской

Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10.Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 2017 г. № 608.

11.Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2016 г. № 21.

12.Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2016 г.

13.Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2016 г. № 83.

14.Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2017 г. № 84.

15.Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2017 г. № 282.

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

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

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

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

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

Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с

ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

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

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

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

3.2.3. Периодические издания:

Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

Защита информации. Инсайд: Информационно-методический журнал

Информационная безопасность регионов: Научно-практический журнал

Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4. Электронные источники:

ЭБС – ipr.books. Доступ к электронной библиотечной системе для сотрудников техникума и студентов осуществляется при помощи авторизации бесплатно.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Справочно-правовая система «Консультант Плюс» www.consultant.ru

Справочно-правовая система «Гарант» » www.garant.ru

Федеральный портал «Российское образование www.edu.ru

Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

Российский биометрический портал www.biometrics.ru

Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК 02.01

Код и наименование профессиональных и общих компетенций, формируемые в 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
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и	- демонстрация ответственности за принятые решения - обоснованность	

личностное развитие.	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 учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
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 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и	