МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ХАБАРОВСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ХАБАРОВСКИЙ ТЕХНИКУМ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ И ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»

РАБОЧАЯ ПРОГРАММА

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

базовой подготовки

Хабаровск

2020

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

Организация-разработчик: КГБ ПОУ ХТТБПТ

Разработчики: Соцков Михаил Юрьевич, преподаватель краевого государственного бюджетного профессионального образовательного учреждения «Хабаровский техникум техносферной безопасности и промышленных технологий».

Рассмотрено и одобрено на заседании

ПЦК Информатики и вычислительной техники

Протокол № _____ от «____»_____20_____г.

Председатель ПЦК _____ (Иващенко Л. В.).

Согласовано на заседании методического совета

Протокол № _____ от «____»_____20_____г.

Председатель МС _____ (Линевич О.Г.).

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО

10.02.05 Обеспечение информационной безопасности автоматизированных систем

в части освоения основного вида профессиональной деятельности (ВПД): Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

Перечень общих 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.

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.

.

- личностные результаты

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации Программы воспитания**
Портрет выпускника ПОО	
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 неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания	**ЛР 4**
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**
Способный в цифровой среде использовать различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»	**ЛР 13**
Способный ставить перед собой цели под возникающие жизненные задачи, подбирать способы решения и средства развития, в том числе с использованием цифровых средств; содействующий поддержанию престижа своей профессии и образовательной организации	**ЛР 14**
Способный генерировать новые идеи для решения задач цифровой экономики, перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов; позиционирующий себя в сети как результативный и привлекательный участник трудовых отношений.	**ЛР 15**
Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.	**ЛР 16**
Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению	**ЛР 17**
Осознающий значимость системного познания мира, критического осмысления накопленного опыта	**ЛР 18**
Развивающий творческие способности, способный креативно мыслить	**ЛР 19**
Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации	**ЛР 20**
Готовый к профессиональной конкуренции и конструктивной реакции на критику	**ЛР 21**
Демонстрирующий приверженность принципам честности, порядочности, открытости	**ЛР 22**
Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством	**ЛР 23**
Проявляющий эмпатию, выражающий активную гражданскую позицию, участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций, а также некоммерческих организаций, заинтересованных в развитии гражданского общества и оказывающих поддержку нуждающимся	**ЛР 24**

Препятствующий действиям, направленным на ущемление прав или унижение достоинства (в отношении себя или других людей)	**ЛР 25**
Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп	**ЛР 26**
Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства	**ЛР 27**
Вступающий в конструктивное профессионально значимое взаимодействие с представителями разных субкультур	**ЛР 28**
Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д.	**ЛР 29**
Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой	**ЛР 30**
Гармонично, разносторонне развитый, активно выражающий отношение к преобразованию общественных пространств, промышленной и технологической эстетике предприятия, корпоративному дизайну, товарным знакам	**ЛР 31**
Оценивающий возможные ограничители свободы своего профессионального выбора, предопределенные психофизиологическими особенностями или состоянием здоровья, мотивированный к сохранению здоровья в процессе профессиональной деятельности	**ЛР 32**
Открытый к текущим и перспективным изменениям в мире труда и профессий	**ЛР 33**
Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики	**ЛР 34**
Экономически активный, предприимчивый, готовый к самозанятости	**ЛР 35**
Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях	**ЛР 36**

Рабочая программа профессионального модуля может быть использована В программах ДПО повышения квалификации и профессиональной переподготовки по направлению 10.00.00.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

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

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – __656__ часов, в том числе:
максимальной учебной нагрузки обучающегося – _470__ часов, включая:
обязательной аудиторной учебной нагрузки обучающегося – _434_ часов;
в том числе за счет вариативной части - _____ часов;
самостоятельной работы обучающегося – __12__ часов;
учебной и производственной практики – _180_ часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами, в том числе профессиональными (ПК), общими (ОК) компетенциями и личностными результатами (ЛР), указанными в п. 1.1.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов *(макс. учебная нагрузка и практики)*	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика		Экзамен по модулю, часов	Консультации, часов
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов *(если предусмотрена рассредоточенная практика)*		
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	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 2.6 ОК 1-ОК 10 ЛР 01-36	**МДК.02.01.** Программные и программно-аппаратные средства защиты информации	180	170	36	30*	**4**	*	*	*	**6**	**2**
ПК 2.4 ОК 1-ОК 10 ЛР 01-36	**МДК.02.02.** Криптографические средства защиты информации	144	**134**	**78**		**4**		*	*	**6**	**2**
ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36	**МДК.02.03** Кибербезопасность и защита данных	74	**66**	38		**2**				**6**	**2**
ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36	**МДК.02.04** Корпоративная защита от внутренних угроз	72	**64**	36		**2**				**6**	**2**

* Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

	информационной безопасности										
	Учебная практика	**72**							**72**		
	Производственная практика (по профилю специальности), часов	**108**							**108** *)*		
	Экзамен по модулю	**6**									
	Консультации										
	Всего:	**656**	**434**	**188**	**30**	**12**	**-**	**-**	**180***	**24**	**8**

Ячейки в столбцах 3, 4, 7, 9, 10 заполняются жирным шрифтом, в 5, 6, 8 - обычным. Если какой-либо вид учебной работы не предусмотрен, необходимо в соответствующей ячейке поставить прочерк. Количество часов, указанное в ячейках столбца 3, должно быть равно сумме чисел в соответствующих ячейках столбцов 4, 7, 9, 10 (жирный шрифт) по горизонтали. Количество часов, указанное в ячейках строки «Всего», должно быть равно сумме чисел соответствующих столбцов 3, 4, 5, 6, 7, 8, 9, 10 по вертикали. Количество часов, указанное в ячейке столбца 3 строки «Всего», должно соответствовать количеству часов на освоение программы профессионального модуля в пункте 1.3 паспорта программы. Количество часов на самостоятельную работу обучающегося должно соответствовать указанному в пункте 1.3 паспорта программы. Сумма количества часов на учебную и производственную практику (в строке «Всего» в столбцах 9 и 10) должна соответствовать указанному в пункте 1.3 паспорта программы. Для соответствия сумм значений следует повторить объем часов на производственную практику по профилю специальности (концентрированную) в колонке «Всего часов» и в предпоследней строке столбца «Производственная, часов». И учебная, и производственная (по профилю специальности) практики могут проводиться параллельно с теоретическими занятиями междисциплинарного курса (рассредоточено) или в специально выделенный период (концентрированно)

3.2. Содержание обучения по профессиональному модулю (ПМ)

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	ОК, ПК, ЛР
1	2	3	4	5
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**180**		
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации				
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**	**6**		ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Предмет и задачи программно-аппаратной защиты информации		2	
	Основные понятия программно-аппаратной защиты информации			
	Классификация методов и средств программно-аппаратной защиты информации			
Тема 1.2. Стандарты безопасности	**Содержание**	**6**		ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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)		2	
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.			
	Тематика практических занятий и лабораторных работ	**2**		

	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.		3	
	Обзор стандартов. Работа с содержанием стандартов			
Тема 1.3. Защищенная автоматизированная система	**Содержание**	**4**		
	Автоматизация процесса обработки информации		2	ПК 2.1 – ПК 2.6 ОК 1- ОК 10 ЛР 01- 36
	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			
	Тематика практических занятий и лабораторных работ	**6**		
	Учет, обработка, хранение и передача информации в АИС		3	
	Ограничение доступа на вход в систему.			
	Идентификация и аутентификация пользователей			
	Разграничение доступа.			
	Регистрация событий (аудит).			
	Контроль целостности данных			
	Уничтожение остаточной информации.			
	Управление политикой безопасности. Шаблоны безопасности			
	Криптографическая защита. Обзор программ шифрования данных			
	Управление политикой безопасности. Шаблоны безопасности			
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**4**		
	Источники дестабилизирующего воздействия на объекты защиты		2	ПК 2.1 – ПК 2.6 ОК 1-
	Способы воздействия на информацию			
	Причины и условия дестабилизирующего воздействия на информацию			
	Тематика практических занятий и лабораторных работ	**2**		

	Распределение каналов в соответствии с источниками воздействия на информацию		3	ОК 10 ЛР 01-36
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	**6**		
	Понятие несанкционированного доступа к информации		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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.			
	Тематика практических занятий и лабораторных работ	**4**		
	Организация доступа к файлам		3	
	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**	**6**		
	Работа автономной АС в защищенном режиме		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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.			
Тема 2.2 Защита программ от изучения	**Содержание**	**6**		
	Изучение и обратное проектирование ПО		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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.			

Тема 2.3. Вредоносное программное обеспечение	**Содержание**	**4**		
	Вредоносное программное обеспечение как особый вид разрушающих воздействий		2	ПК 2.1 – ПК 2.6 ОК 1- ОК 10 ЛР 01- 36
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения			
	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.			
	Бот-неты. Принцип функционирования. Методы обнаружения			
	Классификация антивирусных средств. Сигнатурный и эвристический анализ			
	Защита от вирусов в "ручном режиме"			
	Основные концепции построения систем антивирусной защиты на предприятии			
	Тематика практических занятий и лабораторных работ	**2**		
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО		3	
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**	**4**		
	Несанкционированное копирование программ как тип НСД		2	ПК 2.1 – ПК 2.6 ОК 1- ОК 10 ЛР 01- 36
	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			
	Тематика практических занятий и лабораторных работ	**2**		
	Защита информации от несанкционированного копирования с использованием специализированных программных средств		3	
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)			
Тема 2.5. Защита информации на машинных носителях	**Содержание**	**6**		
	Проблема защиты отчуждаемых компонентов ПЭВМ.		2	ПК 2.1 – ПК 2.6 ОК 1-
	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			ОК 10 ЛР 01-36
	Безвозвратное удаление данных. Принципы и алгоритмы.			
	Тематика практических занятий и лабораторных работ	**6**		
	Применение средства восстановления остаточной информации на примере Foremost или аналога		3	
	Применение специализированного программно средства для восстановления удаленных файлов			
	Применение программ для безвозвратного удаления данных			
	Применение программ для шифрования данных на съемных носителях			
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**6**		
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Устройства Touch Memory			
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**	**4**		
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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.			
	Тематика практических занятий и лабораторных работ	**2**		
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений		3	

Раздел 3. Защита информации в локальных сетях				
Тема 3.1. Основы построения защищенных сетей	**Содержание**	**4**	**2**	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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.			
Тема 3.2. Средства организации VPN	**Содержание**	**4**		
	Виртуальная частная сеть. Функции, назначение, принцип построения		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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			
	Тематика практических занятий и лабораторных работ	**2**		
	Развертывание VPN		3	
Раздел 4. Защита информации в сетях общего доступа				
Тема 4.1 Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**8**		
	Методы защиты информации при работе в сетях общего доступа.		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности			
	Основные типы firewall. Симметричные и несимметричные firewall.			
	Уровень 1. Пакетные фильтры			
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.			
	Уровень 3. Proxy-сервера прикладного уровня			
	Однохостовые и мультихостовые firewall.			

	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций			
	Требования по сертификации межсетевых экранов			
	Тематика практических занятий и лабораторных работ	**2**		
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.		3	
	Изучение различных способов закрытия "опасных" портов			
Раздел 5. Защита информации в базах данных				
Тема 5.1. Защита информации в базах данных	**Содержание**	**6**		
	Основные типы угроз. Модель нарушителя		**2**	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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			
	Тематика практических занятий и лабораторных работ	**2**		
	Изучение механизмов защиты СУБД MS Access		3	
	Изучение штатных средств защиты СУБД MSSQL Server			
Раздел 6. Мониторинг систем защиты				
Тема 6.1. Мониторинг систем защиты	**Содержание**	**6**		
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	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.			
	Тематика практических занятий и лабораторных работ	**2**		

	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов		3	
	Проведение аудита ЛВС сетевым сканером			
Курсовая работа		**30**		
Примерная тематика курсовых работ 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах 6. Защита сред виртуализации				ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
Примерная тематика самостоятельной работы при изучении МДК.02.01 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты		**4**		
Промежуточная аттестация по МДК.02.01		**2**		
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	**2**		ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.		2	
	Тематика практических занятий и лабораторных работ	**2**		
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.		3	
Тема 6.3. Изучение	**Содержание**	**8**		

современных программно-аппаратных комплексов.	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов			
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов			
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов			
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов			
Консультация		**2**		
Промежуточная аттестация по МДК.02.01		**6**		
Примерные виды самостоятельных работ при изучении раздела 1 модуля 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.				ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
МДК.02.02. Криптографические средства защиты информации		**144**		
Введение	**Содержание**	**2**		
	Предмет и задачи криптографии. История криптографии. Основные термины		2	
Раздел 1. Математические основы защиты информации				
Тема 1.1. Математические основы криптографии	**Содержание**	**16**		
	Элементы теории множеств. Группы, кольца, поля.		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10
	Делимость чисел. Признаки делимости. Простые и составные числа.			
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.			
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.			

	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.			ЛР 01-36
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.			
	Китайская теорема об остатках.			
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.			
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.			
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.			
	Арифметические операции над большими числами.			
	Эллиптические кривые и их приложения в криптографии.			
	Тематика практических занятий и лабораторных работ	**6**		
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений		3	
	Проверка чисел на простоту			
	Решение задач с элементами теории чисел.			
Раздел 2. Классическая криптография				
Тема 2.1. Методы криптографического защиты информации	**Содержание**	**4**		
	Классификация основных методов криптографической защиты. Методы симметричного шифрования		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр			
	Методы перестановки. Табличная перестановка, маршрутная перестановка			
	Гаммирование. Гаммирование с конечной и бесконечной гаммами			
	Тематика практических занятий и лабораторных работ	**8**		
	Применение классических шифров замены		3	
	Применение классических шифров перестановки			
	Применение метода гаммирования			
Тема 2.2. Криптоанализ	**Содержание**	**6**		

	Основные методы криптоанализа. Криптографические атаки.		2	ПК 2.1 – ПК 2.6 ОК 1- ОК 10 ЛР 01-36
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса			
	Перспективные направления криптоанализа, квантовый криптоанализ.			
	Тематика практических занятий и лабораторных работ	**10**		
	Криптоанализ шифра простой замены методом анализа частотности символов		3	
	Криптоанализ классических шифров методом полного перебора ключей			
	Криптоанализ шифра Вижинера			
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**4**		
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии		2	ПК 2.1 – ПК 2.6 ОК 1- ОК 10 ЛР 01-36
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.			
	Тематика практических занятий и лабораторных работ	**4**		
	Применение методов генерации ПСЧ		3	
Раздел 3. Современная криптография				
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**4**		
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII		2	ПК 2.1 – ПК 2.6 ОК 1- ОК 10 ЛР 01-36
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств			
	Тематика практических занятий и лабораторных работ	**8**		
	Кодирование информации		3	
	Программная реализация классических шифров			
	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.			
	Содержание учебного материала	**4**		

Тема 3.2. Симметричные системы шифрования	Общие сведения. Структурная схема симметричных криптографических систем		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, **ГОСТ 28147-89, RC4**			
	Тематика практических занятий и лабораторных работ	**4**		
	Изучение программной реализации современных симметричных шифров		3	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**4**		
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Элементы теории чисел в криптографии с открытым ключом.			
	Тематика практических занятий и лабораторных работ	**6**		
	Применение различных асимметричных алгоритмов.		3	
	Изучение программной реализации асимметричного алгоритма RSA			
Примерная тематика самостоятельной работы при изучении МДК.02.02 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов		**2**		
Промежуточная аттестация по МДК.02.02		**2**		
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**2**		
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи		2	ПК 2.1 – ПК 2.6 ОК 1-
	Тематика практических занятий и лабораторных работ	**8**		
	Применение различных функций хеширования, анализ особенностей хешей		3	

	Применение криптографических атак на хеш-функции.			ОК 10 ЛР 01-36
	Изучение программно-аппаратных средств, реализующих основные функции ЭП			
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**2**		
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Тематика практических занятий и лабораторных работ	**6**		
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.		3	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.			
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	**2**		
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.			
	Тематика практических занятий и лабораторных работ	**4**		
	Работа с программой CriptoAPI		**3**	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**	**2**		
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.			
	Тематика практических занятий и лабораторных работ	**6**		
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей		3	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	**2**		
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.		2	

	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ			ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Тематика практических занятий и лабораторных работ	**6**		
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ		3	
	Реализация простейших стеганографических алгоритмов			
Примерная тематика самостоятельной работы при изучении МДК.02.02 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии		**2**		
Консультация		**2**		
Промежуточная аттестация по МДК.02.02		**6**		
Примерные виды самостоятельной работы при изучении раздела 2 модуля 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 лабораторно-практических работ, отчетов к их защите.				
МДК.02.03. Кибербезопасность и защита данных		**74**		
Тема 1 Кибербезопасность и плоскости атак	**Содержание учебного материала**	**6**		
	Правовые основы киберпространства, субъекты и объекты			ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Кибербезопасность			
	Правила безопасного поведения в сети Интернет			
	Интернет банкинг			
	Internet-вещей			
	Проблема информационного взаимодействия кибернетических устройств без участия человека			
	Защищенность механизма управления доступом и сессиями			

	Поиск уязвимостей к атакам XSS			
	Устойчивость к атакам отказа в обслуживании			
	Сетевые уязвимости			
	Критическая информационная инфраструктура			
	Аспекты уязвимости объектов КИИ			
	Тематика практических занятий и лабораторных работ	**8**		
	Методы идентификации устройств без участия человека.			
	Пентест автоматизированных систем			
	Защита веб-приложений			
	Сбор информации о WEB-приложении			
	Требования к системам защиты информации при интеграции с системами реального времени			
	Взаимодействие доверенных систем в недоверенных средах.			
	Поиск уязвимостей к атакам SQL-INJECTION			
Тема 2 Средства и методы предотвращения и обнаружения кибератак	**Содержание учебного материала**	**20**		
	Системы предотвращения вторжения			ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Предотвращение инцидентов и управление событиями информационной безопасности			
	Технологии защиты узла и агентского мониторинга			
	Программный комплекс VipNet IDS назначение, структура, функционал			
	Программный комплекс ViPNet TIAS назначение, структура, функционал			
	Тематика практических занятий и лабораторных работ	**30**		
	Настройка групповых политик средствами ОС			
	Методы детектирования атак			
	Выявление атаки на веб-сервер с поддержкой PHP			
	Выявление атаки по протоколу SMB			
	Выявление атаки на сервис FTP			
	Выявление DOS атаки на HTTP-сервер			

	Выявление атаки по протоколу Modbus			
Самостоятельная работа		**2**		
Консультация		**2**		
Промежуточная аттестация по МДК.02.03		**6**		
Примерные виды самостоятельной работы при изучении раздела 3 модуля 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 лабораторно-практических работ, отчетов к их защите.				
МДК 02.04 Корпоративная защита от внутренних угроз информационной безопасности		**72**		
1. Основные понятия и анализ угроз информационной безопасности	**Содержание учебного материала**	**2**		ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Основные понятия корпоративной защиты информации и информационной безопасности		2	
	Анализ угроз информационной безопасности			
2. Основы защиты информации от внутренних угроз информационной безопасности	**Содержание учебного материала**	**6**		
	Понятия внутренней и внешней угрозы и «нарушителя»		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Ключевые алгоритмы и системы защиты.			
	Ключевые направления в защите информации			
	Защита информации от внутренних угроз			
	Теория и практика применения Data Leakage Prevention (DLP-систем)			
	DLP-система InfoWatch			
	Выявление утечек с использованием технологии DLP.			
3. Установка, конфигурирование и устранение неисправностей в системе	**Содержание учебного материала**	**4**		
	Домен: функции и назначение		2	ПК 2.1 – ПК 2.6
	Доменная сеть, аспекты безопасности			
	Установка IWTM			

корпоративной защиты от внутренних угроз.	Установка и работа с Crawler			ОК 1-ОК 10 ЛР 01-36
	Конфигурирование DLP IWTM			
	Исправление типовых неисправностей.			
	Тематика практических занятий и лабораторных работ	**4**		
	Установка WinServer 2016		3	
	Установка DLP IWTM в виртуальном окружении.			
	Установка Device Monitor			
	Варианты установки Deploy Agent			
	Создание доменной сети			
4. Технологии агентского мониторинга	**Содержание учебного материала**	**2**		
	Назначение агентского мониторинга		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Интерфейс консоли DLP IWDM			
	Создание и проверка политик.			
	Тематика практических занятий и лабораторных работ	**6**		
	Политики агентского мониторинга, особенности их настройки		3	
	Настройка совместных событий агентского и сетевого мониторинга			
	Исключение из событий перехвата			
5. Разработка и тестирование политик в системе DLP IWTM	**Содержание учебного материала**	**4**		
	Работа с разделом технологии системы		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Работа со сводками, виджетами			
	Работа с объектами защиты			
	Использование регулярных выражений			
	Работа с выгрузками из баз данных			
	Работа с файловыми типами			
	Тематика практических занятий и лабораторных работ	**10**		
	Мониторинг трафика		3	
	Работа с событиями, запросы			

	Работа с персонами			
	Работа с категориями и терминами			
	Работа с графическими объектами			
	Работа с печатями и бланками			
6. Технология защиты информации ViPNet	**Содержание учебного материала**	**8**		
	Технологии защиты конфиденциальной информации		2	ПК 2.1 – ПК 2.6 ОК 1-ОК 10 ЛР 01-36
	Архитектура виртуальных защищенных сетей (VPN)			
	Состав ViPNet Administrator (ЦУС и УКЦ)			
	Криптографические основы ViPNet			
	ViPNet Удостоверяющий и ключевой центр			
	Обновление ключевой информации сети ViPNet			
	Функции ViPNet Coordinator			
	Объекты, роли и связи защищенной сети ViPNet			
	Тематика практических занятий и лабораторных работ	**16**		
	Уровни полномочий		3	
	Межсетевое взаимодействие			
	Издание сертификатов открытого ключа подписи			
	Функции ViPNet Client			
Самостоятельная работа		**2**		
Консультация		**2**		
Промежуточная аттестация по МДК.02.04		**6**		
Примерные виды самостоятельной работы при изучении раздела 3 модуля 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 лабораторно-практических работ, отчетов к их защите.				
Учебная практика по разделу 1 модуля **Виды работ:**		**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 **Учебная практика раздела 2 модуля** **Виды работ:** Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи			
Производственная практика по ПМ.02 **Виды работ** – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	**108**		
Экзамен по профессиональному модулю	**6**		

Всего:	**656**		

*Внутри каждого раздела указываются междисциплинарные курсы и соответствующие темы. По каждой теме описывается содержание учебного материала (в дидактических единицах), наименования необходимых лабораторных работ и практических занятий (отдельно по каждому виду), а также примерная тематика самостоятельной работы. Если предусмотрены курсовые работы (проекты) по профессиональному модулю, описывается примерная тематика. Объем часов определяется по каждой позиции столбца 3 (отмечено звездочкой *). Уровень освоения проставляется напротив дидактических единиц в столбце 4 (отмечено двумя звездочками **).*

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

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебных кабинетов _ лекционные аудитории с мультимедийным оборудованием;

лабораторий «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета:

лекционная аудитория: посадочных мест - 25, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций

Технические средства обучения:

Оборудование лаборатории и рабочих мест лаборатории:

«Программных и программно-аппаратных средств обеспечения информационной безопасности»

- 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.

Реализация программы модуля предполагает обязательную производственную практику.

Оборудование и технологическое оснащение рабочих мест:

Наличие стендов реализованных в виртуальной среде по защите от НСД (Secret Net Studio, Dallas Lock), DLP-система IWTM, ПК Vip Net, ПО для реализации пентестов (KalyLinux), аппаратная реализация АМДЗ «Аккорд»

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.

3. Бубнов А.А. и др. Техническая защита информации в объектах информационной структуры. СПО. М.; Академия, 2019.-10

4. Бутакова, Н. Г. Криптографические методы и средства защиты информации / Н. Г. Бутакова, Н. В. Федоров. – Санкт-Петербург : Общество с ограниченной ответственностью "Издательский центр "Интермедия", 2020. – 380 с. – ISBN 978-5-4383-0210-0. (Элайбрери)

5. Гашков С.Б. Криптографические методы защиты информации. М. Академия,2013

6. Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа: http://e.lanbook.com/book/68466.

7. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.

8. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

9. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

10. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

11. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180099

12. Нестеров С.А. Основы информационной безопасности. СПб.: Лань, 2019

13. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699 (дата обращения: 07.10.2020). — Режим доступа: для авториз. Пользователей

14. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

15. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

16. Паркин, Д. С. Кибербезопасность / Д. С. Паркин // Цифровая экономика и финансы : Материалы IV Международной научно-практической конференции, Санкт-Петербург, 18–19 марта 2021 года / Под научной редакцией Е.А. Синцовой [и др.]. – Санкт-Петербург: Центр научно-информационных технологий "Астерион", 2021. – С. 94-96. (Элайбрери)

17. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для спо / В. И. Петренко, И. В. Мандрица. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744 (дата обращения: 29.11.2021). — Режим доступа: для авториз. пользователей.

18. Платонов В.В. Программно-аппаратные средства зашиты информации. М.: Академия, 2014

19. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

3.2.2. Дополнительные печатные источники:

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

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

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

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

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

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

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

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

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

10. Положение о сертификации средств защиты информации. Утверждено постановлением

Правительства Российской Федерации от 26 июня 1995 г. № 608.

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

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

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

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

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

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

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

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

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

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

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

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

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. 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

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

30. 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

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

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

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

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

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

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

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

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

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

40. 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.

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

42. 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.

43. 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.

44. Методика определения актуальных угроз безопасности персональных данных при их

обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

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

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

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

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

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

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

51. 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:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru

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

10. Сайт Научной электронной библиотеки www.elibrary.ru

4.3. Общие требования к организации образовательного процесса

Обучение проводится с соблюдением образовательных стандартов, требований санитарной гигиены и охраны труда. Образовательный процесс осуществляется с учетом индивидуальных особенностей обучающихся.

Для достижения поставленных целей профессионального модуля необходимо предварительное изучение общепрофессиональных дисциплин, предусмотренных учебным планом.

4.4. Кадровое обеспечение образовательного процесса

4.4.1. Реализация образовательной программы обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности, имеющих стаж работы в данной профессиональной области не менее 3 лет.

4.4.2. Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии).

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности, в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 процентов.

Педагогический состав: _____.

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

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

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты **(освоенные общие компетенции)**	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
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 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 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 ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении 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 языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

Результаты указываются в соответствии с паспортом программы и разделом 2. Перечень форм контроля должен быть конкретизирован с учетом специфики обучения по программе профессионального модуля.

***Правила определения основных показателей результатов подготовки:*

1. Основные показатели результатов подготовки должны вытекать из профессиональных компетенций как результат выполнения действий.

2. Основные показатели результатов подготовки могут отражать как комплексный результат деятельности (характеризующий целостный опыт деятельности), так и элементарный результат выполнения отдельный действий и/или операций. Показателем может быть продукт или процесс

выполнения (выполнение работы в соответствии .....).

3. Дескриптор основного показателя результата подготовки формулируются с помощью отглагольных существительных, стоящих вначале предложения.

4. Формулировка показателя не должна повторять формулировку компетенции.

5. Каждой компетенции должно соответствовать не менее двух показателей.

6. Формулировка дескриптора основного показателя результата подготовки должна быть: – ясной и понятной: использование доступных понятий; простые предложения и стиль изложения, в то же время не обедняющие языковой опыт обучающихся; логичность (последовательность, непротиворечивость); – четкой и конкретной, способствующей однозначному пониманию качественных и количественных характеристик результата деятельности

Допускается оформление согласно примерной программы модуля:

Профессиональные компетенции	Оцениваемые знания и умения, действия	Методы оценки	Критерии оценки
ПК 1.1.	Знания:		
		Тестирование	75% правильных ответов
		Контрольная работа	75% выполненных заданий
	Умения:		
		Практическое задание	Экспертное наблюдение
		Практическое задание	Экспертное наблюдение
	Действия:		
		Экзамен	Выполнение теоретических и практических заданий
	Умения: Знания:	Ролевая игра	Экспертное наблюдение
	Умения: Знания:	Ситуационные задачи	Экспертное наблюдение
	Знания:		
		Контрольная работа	75% выполненных заданий
		Тестирование	75% правильных ответов
ОК 1.		Тестирование	75% правильных ответов
ОК 2.		Контрольная работа	75% выполненных заданий

Лист изменений и дополнений

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

для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

№ изменения, дата изменения; номер страницы с изменением	
БЫЛО	**СТАЛО**
……	…….
……..	……
Основание:…….	

_____/_____
подпись *Инициалы, фамилия , внесшего изменения*

Рассмотрено и одобрено на заседании ЦМК№ ____
Протокол № ____ «____»_____20____г.
Председатель ЦМК: _____/_____
подпись *Инициалы, фамилия*