Автономная некоммерческая профессиональная образовательная организация «Многопрофильная Академия непрерывного образования»
АНПОО «МАНО»
Колледж

ПРИНЯТО
Решением Педагогического совета
АНПОО «МАНО»
Протокол № 01-01/16 от
01.06.2022 г.

УТВЕРЖДАЮ
Ректор АНПОО «МАНО»
В.И. Гам
«1» июня 2022 г.

РАБОЧАЯ ПРОГРАММА
по профессиональному модулю
ПМ.03. Программно-аппаратные и технические средства защиты информации
МДК.03.01 Технические методы и средства, технологии защиты информации
МДК.03.02 Программно-аппаратные средства защиты информации
ПП.03.01. Производственная практика
Специальность 10.02.01 Организация и технология защиты информации
Квалификация: Техник по защите информации
Заочная форма обучения

Омск, 2022

Рабочая программа профессионального модуля «Программно-аппаратные и технические средства защиты информации» разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) **10.02.01** Организация и технология защиты информации, утвержденного приказом Министерства образования и науки Российской Федерации от 28 июля 2014 г. № 805.

Организация-разработчик:
АНПОО «Многопрофильная Академия непрерывного образования».
Разработчик:
Бугаев А.П., преподаватель Колледжа АНПОО «МАНО».

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 Программно-аппаратные и технические средства защиты информации

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации в части освоения вида профессиональной деятельности (ВПД): программно-аппаратные и технические средства защиты информации.

Программа по профессиональному модулю ПМ. 3. «Программно-аппаратные и технические средства защиты информации» содержит МДК. 3.1 «Технические методы и средства, технологии защиты информации», МДК. 3.2 «Программно-аппаратные средства защиты информации», ПП.3.01. Производственная практика.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Программа профессионального модуля «Программно-аппаратные и технические средства защиты информации» входит в профессиональный цикл специальности 10.02.01 «Организация и технология защиты информации».

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

В результате изучения профессионального модуля обучающийся должен:

иметь практический опыт:

- участия в эксплуатации систем и средств защиты информации защищаемых объектов;
- применения технических средств защиты информации;
- выявления возможных угроз информационной безопасности объектов защиты;

уметь:

- работать с техническими средствами защиты информации;
- работать с защищенными автоматизированными системами;
- передавать информацию по защищенным каналам связи;
- фиксировать отказы в работе средств вычислительной техники;

знать:

- виды, источники и носители защищаемой информации;
- источники опасных сигналов;
- структуру, классификацию и основные характеристики технических каналов утечки информации;

- классификацию технических разведок и методы противодействия им;
- методы и средства технической защиты информации;
- методы скрытия информации;
- программно-аппаратные средства защиты информации;
- структуру подсистемы безопасности операционных систем и выполняемые ею функции;
- средства защиты в вычислительных сетях;
- средства обеспечения защиты информации в системах управления базами данных;
- критерии защищенности компьютерных систем;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.

1.4. Количество часов на освоение программы профессионального модуля:

всего - 496 часов, в том числе:

максимальной учебной нагрузки обучающегося – 388 часов, включая

обязательной аудиторной учебной нагрузки обучающегося – 54 часа;

самостоятельной работы обучающегося – 334 часа;

учебная практика – 36 часов;

производственная практика - 72 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Программно-аппаратные и технические средства защиты информации», в том числе общими и профессиональными компетенциями.

5.1. Техник по защите информации должен обладать общими компетенциями, включающими в себя способность:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Применять математический аппарат для решения профессиональных задач.

ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.

ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

5.2. Техник по защите информации должен обладать профессиональными компетенциями, соответствующими видам деятельности:

5.2.3. Применение программно-аппаратных и технических средств защиты информации.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств

защиты.
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Код профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)						Практика	
			Обязательная аудиторная учебная нагрузка обучающегося				Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лекции	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	11
ПК 3.1-3.4	**МДК. 3.1** Технические методы и средства, технологии защиты информации	**186**	**26**	**12**	**14**		**160**			
ПК 3.1-3.4	**МДК. 3.2** Программно-аппаратные средства защиты информации	**202**	**28**	**12**	**12**	**4**	**174**			
	Учебная практика	**36**							**36**	
	Производственная практика, (по профилю специальности), часов	**72**								**72**
Всего:		**496**	**54**	**24**	**26**	**4**	**334**		**36**	**72**

3.2. Содержание обучения по профессиональному модулю
Программно-аппаратные и технические средства защиты информации

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работ (проект)	Объем часов	Уровень освоения
1	2	3	4
МДК.03.01. Технические методы и средства, технологии защиты информации		**26/160**	
Системный подход к защите информации	**Содержание учебного материала**	6	1,2,3
	1. **Лекция.** Основные концептуальные положения инженерно-технической защиты информации. Структура и основные характеристики технических каналов утечки информации.		
	2. **Лекция.** Характеристика инженерно-технической защиты информации как области информационной безопасности.		
	3. **Лекция.** Основные проблемы инженерно-технической защиты информации.		
	Самостоятельная работа обучающихся	6	2
	Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Классификация технических каналов утечки информации.		
	Практические занятия	4	2,3
	1. Определение разрешения объектов защиты от возможного наблюдения с использованием современных визуально-оптических и оптико-электронных приборов. Применение программно-аппаратных и технических средств защиты информации на защищаемых объектах.		
	2. Расчёт уровней речевых сигналов в местах возможного нахождения злоумышленника или его подслушивающих технических средств. Применение программно-аппаратных и технических средств защиты информации на защищаемых объектах.		
	Самостоятельная работа обучающихся Оценка утечки информации по радиоканалу при использовании специальных технических средств (закладных устройств) и за счёт побочных электромагнитных излучений	4	1,2,3

Информация как предмет защиты. Источники опасных сигналов	**Самостоятельная работа обучающихся** Особенности информации как предмета защиты Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие о текущей и эталонной признаковой структуре.	10	2
	Самостоятельная работа обучающихся Состав и краткая характеристика основных и вспомогательных технических средств и систем. Источники опасных сигналов. Практическая работа: Расчёт зон 1 и 2 для основных технических средств и систем, размещённых в помещении	6	2
	Самостоятельная работа обучающихся Подготовка рефератов по следующей тематике: 1. Технические каналы утечки информации при передаче ее по каналам связи. 2. Каналы утечки информации за счет паразитных связей. 3. Демаскирующие признаки объектов. 4. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра. 5. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра. 6. Демаскирующие признаки радиоэлектронных средств. 7. Способы скрытого видео наблюдения и съемки. 8. Индикаторы электромагнитного поля. 9. Сканирующие радиоприемники. 10. Анализаторы спектра, радиочастотомеры.	12	1,2,3
Средства технической разведки	**Самостоятельная работа обучающихся** Классификация технических разведок и методы противодействия им. Визуально-оптические приборы. Фотоаппараты. Оптоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.	10	2

	Самостоятельная работа обучающихся Работа с техническими средствами защиты информации. Технические средства защиты речевой информации в телефонных линиях Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, излучающих в радио- и инфракрасном диапазонах.	8	2
Средства инженерной защиты и технической охраны	**Самостоятельная работа обучающихся** Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Методы и средства технической защиты информации. Методы скрытия информации. Программно-аппаратные средства защиты информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Автоматизированные интегральные системы охраны. Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем пожарной и охранной сигнализаций. Контроль эффективности защиты речевой информации.	10	2
	Самостоятельная работа обучающихся Эксплуатация систем и средств защиты информации защищаемых объектов. Работа с техническими средствами защиты информации (практические задания). Работа с защищенными автоматизированными системами (практические задания).	8	2,3
	Самостоятельная работа обучающихся Творческий проект на тему: «Построение технической защиты информации зала для проведения совещаний колледжа» (выделенное помещение может быть изменено по желанию обучающихся)	8	2,3
Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации.	**Содержание учебного материала**	6	1,2
	1. **Лекция.** Основные задачи, структура и характеристика государственной системы противодействия технической разведке.		
	2. **Лекция.** Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.		
	3. **Лекция.** Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности.		

	Самостоятельная работа обучающихся Термины и определения в области технической защиты информации: объект информатизации. Место технической защиты информации в государственной системе защиты информации в Российской Федерации.	5	1,2
	Самостоятельная работа обучающихся Цели и задачи защиты информации от утечки информации по техническим каналам. Структура, классификация и основные характеристики технических каналов утечки информации. Нормативные документы по технической защите информации. Технические методы и средства защиты информации. Деловая игра: «Применение технических средств защиты информации». Анализ деловых ситуаций по теме: «Выявление возможных угроз информационной безопасности объектов защиты».	10	1,2,3
Основные показатели технических средств	**Практическое занятие** Практическая работа по теме: «Оценка дальности перехвата сигналов». Передача информации по защищенным каналам связи. Фиксация отказов в работе средств вычислительной техники;	2	2,3
	Практическое занятие Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.	2	2,3
	Практическое занятие Участие в эксплуатации систем и средств защиты информации защищаемых объектов. Практическая работа по теме: «Провести регламентные работы и зафиксировать отказы средств защиты».	2	2,3
	Практическое занятие **Индивидуальный проект:** Выявить и проанализировать возможные угрозы информационной безопасности объекта (на выбор). Результаты представить в виде таблицы	2	2,3
	Самостоятельная работа обучающихся Микрофонный эффект в основных и вспомогательных технических средствах. Устройства несанкционированного съема акустической информации.	4	1,2

Технические каналы утечки информации, обрабатываемой СВТ и АС	**Самостоятельная работа обучающихся** Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Работа с защищенными автоматизированными системами. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Методы и средства съема информации с телефонных линий. Побочные электромагнитные излучения средств вычислительной техники.	10	2
Технические каналы утечки акустической (речевой) информации.	**Самостоятельная работа обучающихся** Общая характеристика и классификация технических каналов утечки акустической информации. Передача информации по защищенным каналам связи. Прямые акустические каналы утечки речевой информации. Средства акустической разведки и их технические характеристики. Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях. Выявление информативных частот ПЭМИН ПК. Выделение речевого сигнала на фоне шумов и помех.	12	2
Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	**Самостоятельная работа обучающихся** Методы и средства технической защиты информации, объектов информатизации и их классификация. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры. Защищенные средства вычислительной техники. Структура подсистемы безопасности операционных систем и выполняемые ею функции. Средства защиты в вычислительных сетях. Средства обеспечения защиты информации в системах управления базами данных. Критерии защищенности компьютерных систем. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.	8	2
Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	**Самостоятельная работа обучающихся** Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки. Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации.	10	2,3

Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	**Самостоятельная работа обучающихся** Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Фиксация отказов в работе средств вычислительной техники. Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений; порядок проведения измерений.	8	1,2,3
	Самостоятельная работа обучающихся Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств вычислительной техники. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. Принципы построения и использования охранных, охранно-пожарных и пожарных извещателей. План-схема защиты помещений средствами охранных, охранно-пожарных и пожарных извещателей.	7	1,2
	Самостоятельная работа обучающихся Принципы моделирования объектов защиты. Технический канал утечки информации создаваемый СВТ. Характеристики речевого сигнала. Экранированные помещения. Основные характеристики систем радиолокационного наблюдения	4	1,2
	Дифференцированный зачет	2	
МДК 03.02. Программно-аппаратные средства защиты информации		**28/174**	
Общие принципы защиты операционных систем	**Содержание учебного материала**	**2**	1
	Лекция. **Функционирование операционных систем.** Назначение, функции и типы операционных систем. Принципы внутреннего функционирования. Виды, источники и носители защищаемой информации. Источники опасных сигналов. Структура, классификация и основные характеристики технических каналов утечки информации. Классификация технических разведок и методы противодействия им. Методы и средства технической защиты информации. Методы скрытия информации. Программно-аппаратные средства защиты информации.		

	Самостоятельная работа обучающихся **Атаки на сетевые службы.** Возможные атаки и методы взлома операционной системы. Классификация атак по основным механизмам реализации угроз. Локальные атаки. Удаленные атаки. **Удаленный доступ к сети.** Основные уязвимости удаленного доступа. Атаки на серверы удаленного доступа. Автоматические программы.	**6**	2
	Содержание учебного материала	**2**	2
	Лекция. **Критерии защищенности ОС.** Анализ рисков и политика безопасности. Критерии оценки защищенности ОС. Защита от разрушающих программных воздействий. Защита от изменения и контроль целостности. Структура подсистемы безопасности операционных систем и выполняемые ею функции.		
Базовый уровень безопасности	**Самостоятельная работа обучающихся** **Безопасность в ОС** Набор настроек, применяемый к ОС для повышения ее защищенности. Шаблон безопасности. Основные проблемы с безопасностью и возможные решения в Unix-подобных системах. **Защита ОС.** Защитные механизмы операционных систем. Основные задачи системы защиты операционных систем. **Доступ к элементам системы.** Способы управления доступом. Права доступа к элементам файловой системы.	**8**	2

Комплексный подход к обеспечению информационной безопасности ОС.	**Самостоятельная работа обучающихся** **Защита информации в ОС.** Уровни реализации защиты информации: защита операционной системы, приложений и локальных служб. Защита от изменения и контроль целостности. **Компоненты безопасности локальной сети организации.** Зоны безопасности и их компоненты: внутренняя локальная сеть организации, интернет. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. **Атаки на программное обеспечение.** Атаки на программное обеспечение: атака на настройки безопасности по умолчанию, злоупотребление привилегиями, атаки на пароли. Обнаружения атак. **Обеспечение информационной безопасности организации.** Методы обеспечения информационной безопасности организации. Основные требования к политике безопасности.	**10**	3
	Самостоятельная работа обучающихся Разработка подсистемы защиты операционной системы Linux. Реализация подсистемы защиты операционной системы Windows. Обеспечение защиты вычислительной сети. Управление доступом в операционных системах. Идентификация и аутентификация пользователей операционных систем.	**14**	2,3
	Практическое занятие Практическая работа по теме: «Применение программно-аппаратных и технических средств защиты информации на защищаемых объектах» (объект по выбору студента).	**2**	2,3
Защита информации в системах управления базами данных	**Содержание учебного материала**	**2**	1,2
	Лекция. **Понятия безопасности БД** Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит.		

	Самостоятельная работа обучающихся **Критерии защищенности БД** Критерии оценки надежных компьютерных систем. Понятие политики безопасности. Современное применение различных политик безопасности в рамках единой модели. **Модели безопасности в СУБД** Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД. Дискреционные (избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS). **Механизмы обеспечения целостности СУБД** Основные виды и причины возникновения угроз целостности. Способы противодействия. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. **Механизмы обеспечения конфиденциальности в СУБД** Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД. Организация взаимодействия СУБД и базовой ОС. Подотчетность действий пользователя и аудит связанных с безопасностью событий.	12	2
	Самостоятельная работа обучающихся Организация защиты данных СУБД. Создание Web страниц. Создание БД Access с помощью SQL. Создание группы пользователей, уровни доступа. Средства создания резервных копий и восстановления баз данных.	**12**	2,3
	Самостоятельная работа обучающихся Подбор материала и создание презентации по теме: «Защита ОС от сетевых атак». Подготовить реферат по теме: «Информационная безопасность организаций». Подбор материала и создание презентации по теме: «Защита баз данных в организации».	**8**	2,3
	Практическое занятие Эксплуатация систем и средств защиты информации защищаемых объектов. Подготовка докладов и презентаций: Средства защиты в вычислительных сетях. Средства обеспечения защиты информации в системах управления базами данных. Критерии защищенности компьютерных систем. Методика проверки защищенности объектов информатизации на соответствие требо-	**2**	2

	ваниям нормативных правовых актов.		
Антивирусная защита компьютерных систем	**Самостоятельная работа обучающихся** **Понятие компьютерного вируса** Типичные предпосылки к внедрению компьютерных вирусов. Классификация компьютерных вирусов и вредоносных программ. Файловые, загрузочные и сетевые вирусы. Методы и средства борьбы с вирусами и вредоносными программами. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения. **Специализированные средства и методы выявления вредоносных программ.** Сигнатурное и эвристическое сканирование. Контроль целостности. Мониторинг информационных потоков. Изолированная программная среда. Программные ловушки.	**7**	3
	Практическое занятие Настройка антивирусной защиты операционной системы Windows.	**2**	2
	Самостоятельная работа обучающихся Работа с антивирусной программой Касперский, Dr.Web, Avira Free, ESET NOD32 Smart Security Family. Настройка и использование специализированного антивирусного программного обеспечения.	**5**	2,3
Организационно-правовые аспекты защиты информации	**Содержание учебного материала**	**2**	1
	Лекция. **Организационные основы защиты информации.** Принципы организационной защиты информации.		
	Самостоятельная работа обучающихся **Государственные регуляторы в области защищенности объектов информатизации.** Обзор стандартов и методических документов в области защиты информации, регулирующие организации в области защиты информации **Классификация информации по категориям доступа.** Критерии оценки информации. Категории нарушений по степени важности. **Проверка защищенности объектов информатизации на соответствие требованиям нормативных документов.** Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.	**8**	1,2
	Самостоятельная работа обучающихся Аудит в операционных системах	**2**	2

Комплексная система защиты информации	**Самостоятельная работа обучающихся** **Общая характеристика комплексной защиты информации.** Основы обеспечения комплексной защиты информации. Стратегия комплексной защиты информации. Структура и основные характеристики комплексной защиты информации. **Способы и средства обнаружения угроз.** Комплексное обследование защищенности информационной системы. Средства нейтрализации угроз.	**6**	3
	Самостоятельная работа обучающихся Разработка проекта системы комплексной защиты информации в АИС Комплексное обеспечение информационной безопасности объекта Исследование корректности систем защиты Исследование методов блокирования средств несанкционированного доступа к информации Оценка защищенности информации от утечки в АИС организации.	**15**	
Криптографическая защита информации	**Самостоятельная работа обучающихся** **Основы криптографии.** Структура криптосистемы. Основные методы криптографического преобразования данных. **Симметричные криптосистемы.** Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования. **Криптосистемы с открытым ключом.** Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи – Холлмана. **Системы электронной подписи.** Проблемы аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Цифровые сертификаты. Отечественный стандарт цифровой подписи. **Криптоанализ.** Понятие криптоанализа.	**10**	3
	Самостоятельная работа обучающихся Кодирование информации с помощью алфавитного кодирования Применение простейших криптографических шифров для кодирования информации.	**5**	1,2
	Практическое занятие Выявление и анализ возможных угроз информационной безопасности объектов. Практические задачи: выбрать объект защиты, выявить возможные угрозы информационной безопасности данного объекта, проанализировать характер и количество угроз и разработать программу защиты объекта.	**2**	2,3

Аттестация и лицензирование объектов защиты	**Содержание учебного материала**	4	1,2
	Лекция. **Общие вопросы по аттестации объектов информатизации (ОИ) по требованиям безопасности информации.** Основные стадии создания системы защиты информации на ОИ.		
	Самостоятельная работа обучающихся **Порядок проведения аттестации объектов информатизации.** Программа и методика проведения аттестационных испытаний. **Лицензирование деятельности в области защиты конфиденциальной информации.** Документы, разрабатываемые на объектах информатизации. Порядок действия при лицензировании.	6	1,2
	Практическое занятие Разработка комплекта документации на объект информатизации.	2	3
	Практическое занятие Деловая игра по проведению регламентных работ и фиксации отказов средств защиты.	2	2,3
	Самостоятельная работа обучающихся Аттестация объектов информатизации Проведение аттестации объектов информатизации Лицензирование объектов информатизации Лицензирование деятельности в области защиты информации. Утечки в области защиты информации Защита от утечек в области ЗИ	14	2,3
	Самостоятельная работа Подбор материала и создание презентации по темам: 1. Возможности и технические характеристики программно-аппаратных средств защиты информации 2. Перспективы и направления развития комплексных средств защиты информации 3. Применение криптографических средств защиты информации в государственном учреждение.	**10**	1,2
	Самостоятельная работа Выполнить сравнительный анализ применения различных программ для оперативного и гарантированного восстановления информации на ПК. Ознакомиться с основополагающими документами, затрагивающих интересы РФ в информационной сфере. Составить список уязвимостей предложенного объекта.	**6**	1,2

	Подготовить реферат по теме: 1. Практическое применение антивирусных программ для защиты информации от несанкционированного доступа. 2. Виды угроз информационной безопасности Российской Федерации. 3. Источники угроз информационной безопасности Российской Федерации. 4. Анализ информационной инфраструктуры государства. 5. Виды, каналы утечки и искажения информации 6. Технические средства и методы защиты информации. 7. Программно-аппаратные средства обеспечения информационной безопасности. 8. Аудит безопасности, резервирование ресурсов и компонентов автоматизированной системы. 9. Идентификации и аутентификации. 10. Сетевое оборудование для обеспечения информационной безопасности. 11. Биометрические устройства для обеспечения безопасности.	**10**	2,3
Тематика курсового проектирования: 1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей. 3. Анализ методов и средств анализа защищенности беспроводных сетей. 4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения. 5. Виброакустические средства современных систем обеспечения информационной безопасности. 6. Средства защиты от побочных электромагнитных излучений и наводок, современное состояние, проблемы и решения. 7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 8. Средства обеспечения информационной безопасности банков данных. 9. Использование электронной цифровой подписи для обеспечения защиты информации при использовании системы электронного документооборота. 10. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 11. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 12. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 13. Инструментальные средства анализа рисков информационной безопасности.	**4**	2,3

14. Сравнительный анализ международных стандартов в области информационной безопасности и управления рисками. 15. Сравнительный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности). 16. Анализ аппаратных средств защиты персонального компьютера. 17. Разработка программных средств на основе асимметричного шифрования для защиты операционной системы. 18. Разработка программных средств для защиты операционной системы с помощью цветовой схемы. 19. Разработка программно-аппаратного комплекса для защиты операционной системы. 20. Разработка электронного ключа для защиты от несанкционированного доступа к персональному компьютеру 21. Разработка программного средства для защиты от спама. 22. Анализ существующих методов защиты операционной системы. 23. Разработка программного средства для защиты от фишинговых атак 24. Аудит комплексной защиты информации организации.		
Экзамен		
Учебная практика **Ознакомление с предприятием и рабочими местами.** 1. Задачи и краткое содержание практики по специальности. 2. Инструктаж по общим вопросам, охране труда и технике безопасности, по режиму работы предприятия. 3. Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия. **Технические методы и средства, технологии защиты информации** 1. Виды потенциальных угроз безопасности информации предприятия. 2. Структура средств перехвата и их функции. 3. Способы предотвращения утечки информации по материально-вещественному каналу. 4. Способы и средства наблюдения. 5. Виды информации, защищаемой техническими средствами. 6. Источники и носители конфиденциальной информации. 7. Источники опасных сигналов. 8. Способы записи информации на различные виды носителей. **Программно-аппаратные средства защиты информации** 1. Виды информации предприятия, защищаемой техническими средствами. 2. Источники и носители конфиденциальной информации.	**36**	

3. Способы и средства перехвата сигналов. 4. Системы управления доступом в Интернет и контроля корпоративной электронной почты. 5. Проблемы безопасности «виртуальных» инфраструктур. 6. Защита персональных данных, типовые решения. 7. Управление рисками.		
Производственная практика (по профилю специальности) *Задания:* **Ознакомление с предприятием и рабочими местами.** 4. Задачи и краткое содержание производственной практики по специальности. 5. Инструктаж по общим вопросам, охране труда и технике безопасности, по режиму работы предприятия. 6. Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия. **Технические методы и средства, технологии защиты информации** 9. Виды потенциальных угроз безопасности информации предприятия. 10. Структура средств перехвата и их функции. 11. Способы предотвращения утечки информации по материально-вещественному каналу. 12. Способы и средства наблюдения. 13. Виды информации, защищаемой техническими средствами. 14. Источники и носители конфиденциальной информации. 15. Источники опасных сигналов. 16. Способы записи информации на различные виды носителей. **Программно-аппаратные средства защиты информации** 8. Виды информации предприятия, защищаемой техническими средствами. 9. Источники и носители конфиденциальной информации. 10. Способы и средства перехвата сигналов. 11. Системы управления доступом в Интернет и контроля корпоративной электронной почты. 12. Проблемы безопасности «виртуальных» инфраструктур. 13. Защита персональных данных, типовые решения. 14. Управление рисками.	**72**	1,2,3
Итоговый контроль по ПМ. 3. Программно-аппаратные и технические средства защиты информации объекта: квалификационный экзамен		
Всего часов с учетом практики	**496**	

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 профессионального модуля предполагает наличие учебного кабинета по профилю дисциплины.

Оборудование учебного кабинета:

- мебель по количеству студентов;
- доска;
- наглядные пособия, дидактические средства.

Технические средства обучения:

- персональный компьютер;
- мультимедиа-проектор;
- программное обеспечение (Linux Mint, Apache OpenOffice, Kaspersky Anti-Virus (Пробная версия), Консультант Плюс, браузер).
- Демонстрационные версии Dr.Web, ESET NOD32 Smart Security Family.

4.2. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. *Гасумова, С. Е.* Информационные технологии в социальной сфере : учебник и практикум для среднего профессионального образования / С. Е. Гасумова. — 6-е изд. — Москва : Издательство Юрайт, 2023. — 284 с. — (Профессиональное образование).
2. Гаврилов, М. В. Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 355 с. — (Профессиональное образование). Информационная без-оп.комп.систем и сетей: Уч.пос./В.Ф.Шаньгин -М.:ИД ФОРУМ,НИЦ ИНФРА-М,2018-416с - 978-5-8199-0754-2.

Дополнительные источники:

1. Белкин П.Ю., Михальский О.О. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов. – М.: Радио и связь, 2011.
2. Васильева И.Н., Стельмашонок Е.В. Информационные технологии и защита информации. Учебное пособие. – СПб, СПбГИЭУ, 2011.

3. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2012
4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2012.
5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие. – Спб.: НИУ ИТМО, 2012.
6. Мельников В.П. Информационная безопасность: Учебное пособие/ В.П.Мельников, С.А.Клейменов, А.М. Петраков; Под ред.С.А.Клейменова.-6-е изд., Стереотип.-М.: Академия, 2011.
7. Мельников В.П. Информационная безопасность и защита информации: Учебное пособие для студентов высших учебных заведений / В.П.Мельников, С.А.Клейменов, А.М.Петраков; Под ред. С.А.Клейменова.-5-е изд., стер .-М.: Академия, 2011.
8. Сидорин Ю.С. Технические средства защиты информации: Учеб.пособие. – Спб.: Изд-во Политех. ун-та, 2013.
9. Дикарев В.И., Заренков В.А., Заренков Д.В., Койнаш Б.В. Защита объектов и информации от несанкционированного доступа/ Под ред. В.А. Заренкова.– СПб.: ОАО «Издательство Стройиздат СПб», 2009.
10. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере: учебное пособие. – М.: Форум, 2009.
11. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2010.
12. Меньшаков Ю.К. Виды и средства иностранных технических разведок: Учеб. пособие/ Под ред. М.П. Сычева.– М.: Изд-во МГТУ им. Н.Э. Баумана, 2009.
13. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки: Учеб. пособие.– М.: Российск. гос. гуманит. ун-т, 2010.
14. Рудометов Е.А., Рудометов В.Е. Электронные средства разведки и защиты информации.– М.: ООО «Фирма «Издательство АСТ»; СПб.: ООО «Издательство ПОЛИГОН», 2008.
15. Степанов Е.А. Защита информации и информационная безопасность. Курс лекций. — М.: Изд-во ГУУ, 2009.
16. Торокин А. А. Инженерно-техническая защита информации: Учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности.– М.: Гелиос АРВ, 2011.
17. Хорев А.А. Техническая защита информации: Учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации.– М.: НПЦ «Аналитика», 2010.
18. Зверева, В. П. Технические средства информатизации: учебник / В. П. Зверева, А. В. Назаров. - М. : НИЦ ИНФРА, 2017. - 256 с. - 978-5-906818-88-1.
19. Гаврилов, М. В. Информатика и информационные технологии : учебник для СПО / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — М. : Изда-

тельство Юрайт, 2017. — 383 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-03051-8.
20. Информационная безоп.комп.систем и сетей: Уч.пос./В.Ф.Шаньгин -М.:ИД ФОРУМ,НИЦ ИНФРА-М,2018-416с - 978-5-8199-0754-2.
21. Бубнов А. А. , Пржегорлинский В. Н. , Савинкин О. А. Основы информационной безопасности: учеб. Пособие, 3-е изд. 2017, 256 с. - 978-5-4468-4651-1.

4.3. ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Освоение программы модуля базируется на изучении общепрофессиональных дисциплин «Основы информационной безопасности», «Технические средства информатизации».

Реализация программы модуля предполагает производственную практику, которая проводится концентрированно в соответствии с освоением всех разделов модуля. Практика проводится с целью закрепления и углубления теоретических знаний, а также формирования у обучающихся профессиональных компетенций.

Обязательным условием допуска к производственной практике в рамках профессионального модуля является освоение междисциплинарного курса «Программно-аппаратные и технические средства защиты информации». Аттестация по итогам практики проводится на основании результатов, подтверждаемых отчётами и дневниками практики студентов, а также отзывами руководителей практики на студентов.

Производственная практика завершается зачётом освоенных общих и профессиональных компетенций. Изучение программы модуля завершается итоговой аттестацией, результаты которой оцениваются в форме квалификационного экзамена по модулю.

4.4. КАДРОВОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу:

- наличие высшего профессионального образования, соответствующего профилю модуля;
- опыт деятельности в организациях соответствующей профессиональной сферы;
- преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин.

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

Образовательная организация, реализующая подготовку по программе данного профессионального модуля, обеспечивает организацию и проведение текущего контроля индивидуальных образовательных достижений – демонстрируемых обучающимися знаний, умений и навыков.

Текущий контроль проводится преподавателем в процессе обучения.

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения устных опросов, тестирования, практических занятий, а также выполнения обучающимися индивидуальных и групповых заданий. Аттестация по модулю в целом проводится в форме квалификационного экзамена.

Целями освоения дисциплины является формирование у студентов чёткого представления о программно-аппаратных и технических средств защиты информации.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.	- анализ научной литературы; - правильный выбор решений по обеспечению инженерно-технической и программной защиты информации; - выбор методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации	Текущий контроль: - ситуационные задачи, - практические работы, - самостоятельная работа. Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах производственной практики
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов	- умение выработать предложения по разработке программ защиты информации на объекте; - умение самостоятельно разрабатывать методики защиты информации на пред-	Текущий контроль: - ситуационные задачи, - практические работы,

	приятии. - умение самостоятельно применять технические средства защиты информации - определение и анализ недостатков выбранной системы защиты, ее совершенствование.	- самостоятельная работа. Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах производственной практики
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	- демонстрация навыков проведения работ по инженерно-технической защите информации; - демонстрация навыков аппаратно-программной защиты информации; -демонстрация навыков регламентных работ по отношению к средствам ЗИ; - фиксация отказов системы защиты.	Текущий контроль: - ситуационные задачи, - практические работы, - самостоятельная работа. Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах производственной практики
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	- демонстрация навыков поиска возможных угроз информационной безопасности; -умение самостоятельно выявлять существующие угрозы информационной безопасности; -умение анализировать выявленные угрозы информационной безопасности.	Текущий контроль: - ситуационные задачи, - практические работы, - самостоятельная работа. Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на различных этапах производственной практики.

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 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	– участие во внеурочной деятельности, связанной с будущей профессией (конкурсы профессионального мастерства, выставки и т. д.) – высокие показатели производственной деятельности.	Наблюдение за деятельностью обучающихся в процессе освоения образовательной программы: - на практических занятиях, лабораторных работах; - при подготовке рефератов, окладов и т. д.; - при выполнении работ на различных этапах производственной практики
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	– выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– решение стандартных и нестандартных профессиональных задач	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	– эффективный поиск необходимой информации; – использование различных источников, включая электронные при изучении теоретического материала и прохождении различных этапов производственной практики	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	– демонстрация умений использовать информационно-коммуникационные технологии в профессиональной деятельности	
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	– проявление ответственности за работу подчиненных, результат выполнения заданий	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	– организация самостоятельных занятий при изучении профессионального модуля.	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	– проявление интереса к новейшим технологиям в области защиты информации.	

ОК 10. Применять математический аппарат для решения профессиональных задач.	– уметь применять средства математической логики для решения задач	
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.	– уметь оценивать документы, используемые в области защиты информации.	
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	– проявление интереса к структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	

ВОПРОСЫ ИТОГОВОГО КОНТРОЛЯ

МДК. 3.1 Технические методы и средства, технологии защиты информации

1. Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.
2. Информация как предмет защиты. Свойства информации. Виды, источники и носители защищаемой информации.
3. Структура и основные характеристики технических каналов утечки информации. Классификация технических каналов утечки информации.
4. Классификация технических разведок и методы противодействия им.
5. Государственная система защиты информации.
6. Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
7. Общая характеристика и классификация технических каналов утечки акустической информации. Передача информации по защищенным каналам связи.
8. Методы и средства технической защиты информации, объектов информатизации и их классификация.
9. Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.
10. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки. Специальные технические средства подавления электронных устройств перехвата речевой информации.
11. Средства инженерной защиты и технической охраны.
12. Основные задачи, структура и характеристика государственной системы противодействия технической разведке.
13. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.

14. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности.
15. Термины и определения в области технической защиты информации: объект информатизации.
16. Место технической защиты информации в государственной системе защиты информации в Российской Федерации.
17. Цели и задачи защиты информации от утечки информации по техническим каналам.
18. Нормативные документы по технической защите информации.
19. Технические методы и средства защиты информации.
20. Основные показатели технических средств.
21. Скрытие и защита информации от утечки по техническим каналам.
22. Технический контроль эффективности мер защиты информации.
23. Виды контроля эффективности инженерно-технической защиты информации.
24. Виды зон безопасности.
25. Методы технического контроля.
26. Особенности инструментального контроля эффективности инженерно-технической защиты информации.
27. Аттестация объектов, лицензирование деятельности по защите информации.
28. Основные организационные и технические меры по защите информации.
29. Основные руководящие, нормативные и методические документы по защите информации ипротиводействия технической разведке.
30. Основные задачи, структура и характеристика государственной системы противодействия.
    технической разведке.
31. Средства маскировки и дезинформации в оптическом и радиодиапазонах.
32. Средства обнаружения, локализации и подавления сигналов закладных устройств.

33. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.
34. Генераторы линейного и пространственного зашумления.
35. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.
36. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.
37. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз.
38. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом.
39. Программно-аппаратные и технические средства защиты информации на защищаемых объектах.
40. Эксплуатация систем и средств защиты информации защищаемых объектов.
41. Проведение регламентных работ и фиксация отказов средств защиты.
42. Выявление и анализ возможных угроз информационной безопасности объектов.

МДК. 3.2 Программно-аппаратные средства защиты информации

1. Функции программно-аппаратных средств защиты информации.
2. Содержание и задачи процесса обеспечения информационной безопасности с использованием программно-аппаратных средств.
3. Методы защиты информации от несанкционированного доступа
4. Требования к специализированным средствам защиты информации от несанкционированного доступа.
5. Контроль целостности системного программного обеспечения и аппаратных средств. Организация виртуальных логических дисков.
6. Шифрование пользовательских виртуальных дисков.
7. Формирование ключевой информации.

8. Методы обеспечения целостности аппаратного обеспечения автоматизированных систем

9. Средства обеспечения целостности составных частей компьютера.

10. Защита узлов и блоков компьютеров от несанкционированного доступа. Средства контроля доступа к рабочему месту пользователя.

11. Программные средства выявления фактов физического доступа к системному блоку и узлам автоматизированной системы.

12. Анализ уязвимости программного обеспечения автоматизированных систем

13. Понятие вредоносного кода. Программные закладки.

14. Классификация программных закладок. Предпосылки к внедрению программных закладок.

15. Уязвимости программного обеспечения.

16. Принципы построения политики безопасности. Уязвимости политики безопасности.

17. Сокрытие программных закладок.

18. Методы защиты от вредоносных программ

19. Сигнатурное и эвристическое сканирование. Аппаратные средства противодействия вредоносному коду.

20. Контроль целостности программного обеспечения. Мониторинг информационных потоков.

21. Изолированная программная среда.

22. Цифровая подпись исполняемого кода. Шифрование исполняемого кода.

23. Средства анализа уязвимостей.

24. Средства идентификация и аутентификации пользователей автоматизированных систем

25. Применение парольных систем.

26. Аутентификация с помощью физических предметов хранящихся у пользователя.

27. Электронные ключи. Пластиковые карты.

28. Особенности идентификации и аутентификации с помощью биометрических характеристик пользователей.

29. Использование криптографических методов в системах аутентификации.

30. Протоколы и алгоритмы аутентификации и идентификации пользователей в современных операционных системах ОС.

31. Программно-аппаратные и технические средства защиты информации на защищаемых объектах.

32. Эксплуатация систем и средств защиты информации защищаемых объектов.

33. Проведение регламентных работ и фиксация отказов средств защиты.

34. Выявление и анализ возможных угроз информационной безопасности объектов.

Оценка индивидуальных образовательных достижений по результатам текущего контроля и промежуточной аттестации производится в соответствии с универсальной шкалой (таблица).

Процент результативности (правильных ответов)	**Качественная оценка индивидуальных образовательных достижений**	
	балл (отметка)	**вербальный аналог**
85 ÷ 100	5	отлично
70 ÷ 84	4	хорошо
50 ÷ 69	3	удовлетворительно
менее 50	2	не удовлетворительно

6.ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ

№ изменения, дата изменения; № страницы с изменением	
БЫЛО	**СТАЛО**
Основание: Подпись лица внесшего изменения	