Министерство образования Ставропольского края
Государственное бюджетное профессиональное образовательное учреждение
«Пятигорский техникум торговли, технологий и сервиса»
(ГБПОУ ПТТТиС)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация – техник по защите информации

2024 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1.1. Область применения рабочей программы.

Рабочая программа профессионального модуля (далее рабочая программа) – является частью основной профессиональной образовательной программы по специальности СПО в соответствии с ФГОС по специальности СПО образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» укрупненной группы 10.00.00 Информационная безопасность базовой подготовки в части освоения основного вида профессиональной деятельности (ВПД):

Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующих профессиональных компетенций (ПК):

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2. Цели и планируемые результаты освоения профессионального модуля:

В результате изучения профессионального модуля студент должен освоить основной вид деятельности: осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации, обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами, осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации, осуществлять обработку, хранение и передачу информации ограниченного доступа, уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств, осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.3В результате освоения профессионального модуля студент должен:

Владеть навыками	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. *Определения правил и процедур управления системой защиты информации автоматизированной системы;* *Определения правил и процедур выявления инцидента;* *Определения правил и процедур реагирования на инциденты;* *Определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации.* *Определения правил и процедур управления системой защиты информации автоматизированной системы;* *Определения правил и процедур выявления инцидента;* *Определения правил и процедур реагирования на инциденты;* *Определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации.* *Выбора и обоснования критериев выбора эффективности функционирования защищенных автоматизированных систем;* *Проведения экспертизы состояния защищенности информации*

	автоматизированных систем; *Проведения предварительных испытаний системы защиты информации автоматизированной системы;* *Уточнения модели угроз безопасности информации автоматизированной системы.;* *Проведения занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне.*
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; *Применять нормативные документы по противодействию технической разведке* *Применять нормативные документы для оценки уязвимости* *Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы* *Реализовывать правила разграничения доступа персонала к*

	объектам доступа *Настраивать параметры программного обеспечения системы защиты информации автоматизированной системы* *Работать с программой шифрования данных kryptelite* *Классифицировать каналы утечки информации* *Реализовывать многоуровневую политику разграничения доступа средствами программно –аппаратного комплекса «страж nt»* *Определять параметры работы с windows registry recovery и registry explorer* *Выбирать методы защиты условно-бесплатного программного обеспечения* *Реализовывать защитные механизмы в приложениях свободно-распространяемого по* *Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации* *Устранять известные уязвимости автоматизированной системы, приводящих к возникновению угроз безопасности информации* *Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированной системы* *Управлять рисками* *Применять механизмы и службы защиты* *Применять привилегии безопасности и доступа* *Применять протокол ssl* *Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем* *Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе* *Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации* *Обеспечивать безопасность рабочих станций и серверов* *Применять режимы работы блочных шифров, схемы кратного*

	шифрования *Проводить криптоанализ алгоритмов с открытым ключом* *Применять протоколы wpa, wep для организации безопасного функционирования беспроводной сети* *Подбирать оборудование для реализации проекта беспроводной сети предприятия*
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. *Доктрину информационной безопасности российской федерации, № пр-1895 от 9 сентября 2000г* *Положение о методах и способах защиты информации в информационных системах персональных данных (утверждено приказом фстэк россии от 5 февраля 2010 г. N 58)* *Руководящий документ "средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"* *Основные методы снижения затрат на защиту информации в автоматизированных системах* *Отсутствие применимых средств реализации мандатного механизма разграничения доступа* *Сущностные проявления угрозы* *Определение причин и условий дестабилизирующего воздействия на информацию* *Методика выявления способов воздействия на информацию*

	Средства защиты от несанкционированного доступа (сзи от нсд) *Защита носителей информации.* *Выбор надежного оборудования* *Гост р 51583-2014 защита информации. Порядок создания автоматизированных систем в защищенном исполнении.* *Общие положения* *Особенности построения защищенных автоматизированных систем на основе существующих компонентов* *Уровни контроля на отсутствие недекларированных возможностей (ндв) в по средств защиты информации* *Функции прикладного программирования, экспортируемые электронным ключом* *Средства ликвидации последствий от вредоносного по* *Ответственность за создание, использование и распространение вредоносного по* *Построение системы антивирусной защиты серверов и рабочих станций* *Системы обнаружения и предотвращения вторжений (ids, ips)* *Стратегический план построения системы защиты* *Разработка методов реагирования в случае инцидентов и восстановление* *Классификация методов защиты информации от несанкционированного копирования.* *Создание и использование систем защиты от копирования.* *Альтернативные способы уничтожения данных* *Биометрическая идентификация и аутентификация пользователей* *Бесконтактные смарт-карты и usb-ключи* *Анализ методов обнаружения злоупотреблений* *Методы, основанные на моделировании поведения злоумышленника* *Направления совершенствования сов* *Безопасность сетевых устройств osi* *Особенности обеспечения безопасности в беспроводных локальных сетях* *Подготовка и технологии проведения и создания карты покрытия* *Реализация технологий брандмауера* *Линейка оборудования cisco aironet для беспроводных сетей* *Компоненты сети vpn* *Построение vpn-туннелей.* *Шлюз безопасности vpn* *Средства обеспечения безопасности vpn* *Варианты построения виртуальных защищенных каналов типа лвс-лвс*

	Варианты построения виртуальных защищенных каналов типа клиент-лвс *Сервисы безопасности vpn* *Обеспечение конфиденциальности, целостности и аутентичности передаваемой информации с виртуальных частных сетях* *Классификация vpn по рабочему уровню модели osi.* *Классификация vpn по архитектуре технического решения* *Vpn-решения для построения защищенных корпоративных сетей* *Технические и экономические преимущества внедрения технологий vpn в корпоративные сети* *Функции межсетевого экранирования* *Применение систем корпоративного и персонального экранирования* *Особенности межсетевого экранирования на различных уровнях модели osi* *Обзор современных межсетевых экранов* *Осуществление систематического управления неизвестным трафиком* *Аппаратный и виртуальный форм-фактор* *Встроенный межсетевой экран (firewall) windows server* *Проблемы в сфере сертификации межсетевых экранов* *Виды, обнаружение и защита от ddos-атак* *Cisco firepower ngfw, asa с сервисами firepower* *Контекстно-ориентированная защита* *Метод случайного выбора записей* *Контроль поступающих запросов на наличие "подозрительных" запросов или комбинации запросов* *Компоненты смиб: программно-техническая часть, документационная часть, кадровая составляющая* *Основные этапы создания смиб* *Интеллектуальный анализ угроз информационной безопасности* *Система централизованного управления событиями информационной безопасности* *Система для централизованного управления безопасностью, событиями и информацией* *Система выявления угроз в режиме онлайн* *Разработка технического проекта* *Меры защиты информации в государственных информационных системах* *Выбор мер защиты информации для реализации в информационной системе в рамках системы защиты информации* *Содержание мер защиты информации в информационной*

	системе *Регламентация и контроль использования в информационной системе мобильных технических средств* *Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)* *Ограничение программной среды (опс)* *Контроль (анализ) защищенности информации (анз)* *Влияние уязвимости ос на безопасность средств защиты.* *Реализация внешнего контроля ос* *Комплексные средства обеспечения защиты рабочих станций и серверов на уровне данных, приложений, сети, ос и периферийного оборудования* *Программные средства оценки защищенности и аудита информационной безопасности* *Отечественные типовые решения для построения vpn: аппаратно-программный комплекс криптон-ip компании «анкад» для vpn, решение vipnet custom российской компании «инфотекс», решения «микротест» на базе сертифицированных vpn-продуктов компании «инфотекс»* *Зарубежные типовые решения для построения vpn: межсетевые экраны juniper networks (netscreen), решение компании lucent technologies(lucent secure vpn), решение компании cisco systems* *Сравнительный анализ оборудования для филиалов при построении vpn: check point в филиале, check point в центре-branch в филиале* *Принципы подключения мобильных пользователей, находящихся за динамическим nat-ом, по защищенному каналу к разделяемым ресурсам* *Принципы построения отказоустойчивого решения с балансировкой трафика (gre+eigrp)* *Современная антивирусная индустрия: отечественные и зарубежные разработки.* *Одновендорные и мультивендорные комплексные системы автоматизированной защиты* *Правовые основы обеспечения антивирусной защиты информационных систем* *Организация антивирусной защиты н предприятии.* *Dlp системы: назначение и принципы работы* *Применение современных программных и аппаратных криптографических средств для организации защищенных компьютерных систем* *Оценка защищенности систем электронных платежей*

1.4. Количество часов, отводимое на освоение профессионального модуля:

Всего часов – 906 часов

В том числе в форме практической подготовки – 482 часа

Из них на освоение МДК 02.01 – 396 часов

В том числе самостоятельная работа – 20 часов

Промежуточная аттестация в форме экзамена – 6 часов

Из них на освоение МДК 02.02 –144 часа

В том числе самостоятельная работа – 6 часов

Промежуточная аттестация в форме дифференцированного зачета

Практики, в том числе учебная – 144 часа

Производственная – 216 часов

Промежуточная аттестация в форме экзамена по модулю – 6 часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.2.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2.3 Перечень личностных результатов

Код	Наименование личностных результатов
ЛР 1.	Осознающий себя гражданином и защитником великой страны
ЛР 2.	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 3.	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 4.	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 5.	Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России
ЛР.6	Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях
ЛР.7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР.8	Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства
ЛР.9.	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 10.	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР 11.	Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры
ЛР 12.	Принимающий семейные ценности, 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 КК 1.	Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы, управляющий собственным профессиональным развитием, рефлексивно оценивающий собственный жизненный опыт, критерии успешности
ЛР КК 2.	Экономически активный, предприимчивый, готовый к самозанятости

3.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональных и общих компетенций, личностных результатов	Наименования разделов профессионального модуля	Всего, ч	В т.ч. в форме практической подготовки	Работа обучающихся во взаимодействии с преподавателем					Самостоятельная работа
				Обучение по МДК			Практики		
				Всего	В том числе				
					Лаборат. и практ. занятий	Курсовых работ (проектов)	Учебная	Производственная	
1	2	3	4	5	6	7	8	9	10
ПК 2.1 – ПК 2.6 ОК 1-10 ЛР 1-11, КК1, КК 2	МДК 02.01 Программные и программно-аппаратные средства защиты информации	**492**	152	**376**	56	**30**	**96**		**20**
ПК 2.4 ОК 1-10 ЛР 1-11, КК1, КК 2	МДК.02.02. Криптографические средства защиты информации	**192**	108	**138**	60	-	**48**		**6**
	Производственная практика (по профилю специальности), часов	216	216					216	-
	Всего	900	476	308	116	30	144	216	26

3.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа ()	Объем, ак. ч / в том числе в форме практической подготовки
1	2	3
ПМ.02 Применение программных и программно-аппаратных средств защиты информации		*484/116*
МДК 02.01 Программные и программно-аппаратные средства защиты информации		*346/56*
В том числе промежуточная аттестация		**6**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**	**6**
	Тема 1.1.1 Предмет и задачи программно-аппаратной защиты информации	2
	Тема 1.1.2 Основные понятия программно-аппаратной защиты информации	2
	Тема 1.1.3 Классификация методов и средств программно-аппаратной защиты информации	2
Тема 1.2. Стандарты безопасности	**Содержание**	**16**
	Тема 1.2.1 Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
	Тема 1.2.2 *Доктрина информационной безопасности Российской Федерации, № Пр-1895 от 9 сентября 2000г*	2
	Тема 1.2.3 *Положение о методах и способах защиты информации в информационных системах персональных данных (Утверждено приказом ФСТЭК России от 5 февраля 2010 г. N 58)*	2
	Тема 1.2.4 *Руководящий документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"*	2
	Тема 1.2.5 Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных	2

	носителей информации, средств доверенной загрузки, средств антивирусной защиты)	
	Тема 1.2.6 Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №1 (в форме практической подготовки) **Тема 1.2.7** 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: *Применение нормативных документов по противодействию технической разведке*	2
	Практическое занятие №2 (в форме практической подготовки) **Тема 1.2.8** Обзор стандартов. Работа с содержанием стандартов: *Применение нормативных документов для оценки уязвимости*	2
Тема 1.3. Защищенная автоматизированная система	**Содержание**	**18**
	Тема 1.3.1 Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении.	2
	Тема 1.3.2 Основные виды АС в защищенном исполнении. Методы создания безопасных систем.	2
	Тема 1.3.3 *Основные методы снижения затрат на защиту информации в автоматизированных системах*	2
	Тема 1.3.4 Методология проектирования гарантированно защищенных КС. Дискреционные модели.	2

	Мандатные модели.	
	Тема 1.3.5 *Отсутствие применимых средств реализации мандатного механизма разграничения доступа*	2
	В том числе практических и лабораторных занятий:	**8**
	Практическое занятие №3 (в форме практической подготовки) **Тема 1.3.6** Учет, обработка, хранение и передача информации в АИС: *Определение параметров настройки программного обеспечения системы защиты информации автоматизированной системы*	2
	Практическое занятие №4 (в форме практической подготовки) **Тема 1.3.7** Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа. Регистрация событий (аудит): *Реализация правил разграничения доступа персонала к объектам доступа*	2
	Практическое занятие №5 (в форме практической подготовки) **Тема 1.3.8** Контроль целостности данных. Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности: *Настройка параметров программного обеспечения системы защиты информации автоматизированной системы*	2
	Практическое занятие №6 (в форме практической подготовки) **Тема 1.3.9** Криптографическая защита. Обзор программ шифрования данных: *Работа с программой шифрования данных Kryptelite*	2
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**14**
	Тема 1.4.1 Источники дестабилизирующего воздействия на объекты защиты	2
	Тема 1.4.2 *Сущностные проявления угрозы*	2

	Тема 1.4.3 Способы воздействия на информацию	2
	Тема 1.4.4 Причины и условия дестабилизирующего воздействия на информацию	2
	Тема 1.4.5 *Определение причин и условий дестабилизирующего воздействия на информацию*	2
	Тема 1.4.6 *Методика выявления способов воздействия на информацию*	2
	В том числе практических и лабораторных занятий:	**2**
	Практическое занятие №7 (в форме практической подготовки) **Тема 1.4.7** Распределение каналов в соответствии с источниками воздействия на информацию: *Классификация каналов утечки информации*	2
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	**16**
	Тема 1.5.1 Понятие несанкционированного доступа к информации.	2
	Тема 1.5.2 Основные подходы к защите информации от НСД	2
	Тема 1.5.3 *Средства защиты от несанкционированного доступа (СЗИ от НСД)*	2
	Тема 1.5.4 Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса	2
	Тема 1.5.6 Особенности защиты данных от изменения. Шифрование.	2
	Тема 1.5.7 *Защита носителей информации.*	2
	Тема 1.5.8 *Выбор надежного оборудования*	2
	В том числе практических и лабораторных занятий:	**2**
	Практическое занятие №8 (в форме практической подготовки) **Тема 1.5.5** Организация доступа к файлам. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД: *Реализация многоуровневой политики разграничения доступа средствами*	2

	программно –аппаратного комплекса «Страж NT»	
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**	**14**
	Тема 2.1.1 *ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения*	2
	Тема 2.1.2 Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды.	2
	Тема 2.1.3 *Особенности построения защищенных автоматизированных систем на основе существующих компонентов*	2
	Тема 2.1.4 Расширение BIOS как средство замыкания программной среды	2
	Тема 2.1.5 Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	2
	Тема 2.1.6 Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	2
	Тема 2.1.7 *Уровни контроля на отсутствие недекларированных возможностей (НДВ) в ПО средств защиты информации*	2
Тема 2.2.Защита программ от изучения	**Содержание**	**8**
	Тема 2.2.1 Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение	2
	Тема 2.2.2 Задачи защиты от изучения и способы их решения. Защита от отладки.	2
	Тема 2.2.3 Защита от дизассемблирования. Защита от трассировки по прерываниям.	2
	Тема 2.2.4 *Функции прикладного программирования, экспортируемые электронным ключом*	2
Тема 2.3. Вредоносное программное обеспечение	**Содержание**	**22**
	Тема 2.3.1 Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного	2

	обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.	
	Тема 2.3.2 *Средства ликвидации последствий от вредоносного ПО*	2
	Тема 2.3.3 *Ответственность за создание, использование и распространение вредоносного ПО*	2
	Тема 2.3.4 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	2
	Тема 2.3.6 Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме".	2
	Тема 2.3.7 Основные концепции построения систем антивирусной защиты на предприятии.	2
	Тема 2.3.8 *Построение системы антивирусной защиты серверов и рабочих станций*	2
	Тема 2.3.9 *Системы обнаружения и предотвращения вторжений (IDS, IPS)*	2
	Тема 2.3.10 *Стратегический план построения системы защиты*	*2*
	Тема 2.3.11 *Разработка методов реагирования в случае инцидентов и восстановление*	*2*
	В том числе практических и лабораторных занятий:	**2**
	Практическое занятие №9 (в форме практической подготовки) **Тема 2.3.5** Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО: *Параметры работы с Windows Registry Recovery и Registry Explorer*	2
Тема 2.4. Защита программ и данных от	**Содержание**	**12**
	Тема 2.4.1 Несанкционированное копирование программ как тип НСД.	2

несанкционированного копирования	Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.	
	Тема 2.4.2 *Классификация методов защиты информации от несанкционированного копирования.*	2
	Тема 2.4.3 *Создание и использование систем защиты от копирования.*	2
	Тема 2.4.6 Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office.	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №10 (в форме практической подготовки) **Тема 2.4.4** Защита информации от несанкционированного копирования с использованием специализированных программных средств: *Методы защиты условно-бесплатного программного обеспечения*	2
	Практическое занятие №11 (в форме практической подготовки) **Тема 2.4.5** Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint): *Реализация защитных механизмов в приложениях свободно-распространяемого ПО*	2
Тема 2.5. Защита информации на машинных носителях	**Содержание**	**12**
	Тема 2.5.1 Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование.	2
	Тема 2.5.2 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	2

	Тема 2.5.3 Безвозвратное удаление данных. Принципы и алгоритмы.	2
	Тема 2.5.6 *Альтернативные способы уничтожения данных*	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №12 (в форме практической подготовки) **Тема 2.5.4** Применение средства восстановления остаточной информации на примере Foremost или аналога. Применение специализированного программно средства для восстановления удаленных файлов: *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации*	2
	Практическое занятие №13 (в форме практической подготовки) **Тема 2.5.5** Применение программ для безвозвратного удаления данных. Применение программ для шифрования данных на съемных носителях: *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации*	2
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**8**
	Тема 2.6.1 Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2
	Тема 2.6.2 *Биометрическая идентификация и аутентификация пользователей*	2
	Тема 2.6.3 Устройства Touch Memory	2
	Тема 2.6.4 *Бесконтактные смарт-карты и usb-ключи*	2
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**	**14**
	Тема 2.7.1 СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ	2
	Тема 2.7.2 Аппаратный компонент СОВ. Программный компонент СОВ	2
	Тема 2.7.3 Модели системы обнаружения вторжений, Классификация систем	2

	обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	Тема 2.7.5 *Анализ методов обнаружения злоупотреблений*	2
	Тема 2.7.6 *Методы, основанные на моделировании поведения злоумышленника*	2
	Тема 2.7.7 *Направления совершенствования СОВ*	2
	В том числе практических и лабораторных занятий:	**2**
	Практическое занятие №14 (в форме практической подготовки) **Тема 2.7.4** Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений: *Устранение известных уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации*	2
Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей	**Содержание**	**14**
	Тема 3.1.1 Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации.	2
	Тема 3.1.2 *Безопасность сетевых устройств OSI*	2
	Тема 3.1.3 Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	2
	Тема 3.1.4 *Особенности обеспечения безопасности в беспроводных локальных сетях*	2
	Тема 3.1.5 *Подготовка и технологии проведения и создания карты покрытия*	2
	Тема 3.1.6 *Реализация технологий брандмауера*	2
	Тема 3.1.7 *Линейка оборудования Cisco Aironet для беспроводных сетей*	2
Тема 3.2. Средства организации	**Содержание**	**32**

VPN	**Тема 3.2.1** Виртуальная частная сеть. Функции, назначение, принцип построения	2
	Тема 3.2.2 *Компоненты сети VPN*	2
	Тема 3.2.3 Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	2
	Тема 3.2.4 Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы архитектура, модель нарушителя, достоинства и недостатки	2
	Тема 3.2.5 *Построение VPN-туннелей.*	*2*
	Тема 3.2.6 *Шлюз безопасности VPN*	*2*
	Тема 3.2.7 *Средства обеспечения безопасности VPN*	*2*
	Тема 3.2.9 *Варианты построения виртуальных защищенных каналов типа ЛВС-ЛВС*	2
	Тема 3.2.10 *Варианты построения виртуальных защищенных каналов типа клиент-ЛВС*	2
	Тема 3.2.11 *Сервисы безопасности VPN*	2
	Тема 3.2.12 *Обеспечение конфиденциальности, целостности и аутентичности передаваемой информации с виртуальных частных сетях*	*2*
	Тема 3.2.13 *Классификация VPN по рабочему уровню модели OSI.*	*2*
	Тема 3.2.14 *Классификация VPN по архитектуре технического решения*	*2*
	Тема 3.2.15 *VPN-решения для построения защищенных корпоративных сетей*	*2*
	Тема 3.2.16*Технические и экономические преимущества внедрения технологий VPN в корпоративные сети*	*2*
	В том числе практических и лабораторных занятий:	**2**
	Практическое занятие №15 (в форме практической подготовки) **Тема 3.2.8** Развертывание VPN: *Разработка предложений по совершенствованию*	2

	системы управления защиты информации автоматизированной системы	
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**36**
	Тема 4.1.1 Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.	2
	Тема 4.1.2 *Функции межсетевого экранирования*	2
	Тема 4.1.3 *Применение систем корпоративного и персонального экранирования*	2
	Тема 4.1.4 *Особенности межсетевого экранирования на различных уровнях модели OSI*	2
	Тема 4.1.5 *Обзор современных межсетевых экранов*	2
	Тема 4.1.6 *Осуществление систематического управления неизвестным трафиком*	2
	Тема 4.1.7 Основные типы firewall. Симметричные и несимметричные firewall.	2
	Тема 4.1.8 *Аппаратный и виртуальный форм-фактор*	2
	Тема 4.1.9 *Встроенный межсетевой экран (firewall) Windows Server*	2
	Тема 4.1.10 Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня	2
	Тема 4.1.11 Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall.	2
	Тема 4.1.12 Требования к каждому хосту исходя из архитектуры и выполняемых функций	2
	Тема 4.1.13 Требования по сертификации межсетевых экранов	2
	Тема 4.1.14 *Проблемы в сфере сертификации межсетевых экранов*	2
	Тема 4.1.15 *Виды, обнаружение и защита от DDOS-атак*	2

	Тема 4.1.16 *Cisco Firepower NGFW, ASA с сервисами FirePOWER*	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №16 (в форме практической подготовки) **Тема 4.1.17** Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr: *Управление рисками*	2
	Практическое занятие №17 (в форме практической подготовки) **Тема 4.1.18** Изучение различных способов закрытия "опасных" портов: *Применение механизмов и служб защиты*	2
Раздел 5. Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных	**Содержание**	**18**
	Тема 5.1.1 Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом.	**2**
	Тема 5.1.2 Средства контроля целостности информации в базах данных.	2
	Тема 5.1.3 Средства аудита и контроля безопасности. Критерии защищенности баз данных	2
	Тема 5.1.4 Применение криптографических средств защиты информации в базах данных	2
	Тема 5.1.7 *Контекстно-ориентированная защита*	*2*
	Тема 5.1.8 *Метод случайного выбора записей*	*2*
	Тема 5.1.9 *Контроль поступающих запросов на наличие "подозрительных" запросов или комбинации запросов*	*2*
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №18 (в форме практической подготовки) **Тема 5.1.5** Изучение механизмов защиты СУБД MS Access: *Привилегии безопасности и доступа*	2

	Практическое занятие №19 (в форме практической подготовки) **Тема 5.1.6** Изучение штатных средств защиты СУБД MSSQL Server: *Протокол SSL*	2
Раздел 6. Мониторинг систем защиты		
Тема 6.1. Мониторинг систем защиты	**Содержание**	**30**
	Тема 6.1.1 Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	2
	Тема 6.1.2 *Компоненты СМИБ: программно-техническая часть, документационная часть, кадровая составляющая*	2
	Тема 6.1.3 *Основные этапы создания СМИБ*	2
	Тема 6.1.4 Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2
	Тема 6.1.5 Классификация отслеживаемых событий. Особенности построения систем мониторинга	2
	Тема 6.1.6 Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	2
	Тема 6.1.7 Классификация сетевых мониторов	2
	Тема 6.1.10 Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	2
	Тема 6.1.11 *Интеллектуальный анализ угроз информационной безопасности*	*2*
	Тема 6.1.12 *Система централизованного управления событиями информационной безопасности*	*2*
	Тема 6.1.13 *Система для централизованного управления безопасностью, событиями и информацией*	*2*
	Тема 6.1.14 *Система выявления угроз в режиме онлайн*	*2*

	Тема 6.1.15 *Разработка технического проекта*	*2*
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №20 (в форме практической подготовки) **Тема 6.1.8** Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов: *Анализ программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем*	2
	Практическое занятие №21 (в форме практической подготовки) **Тема 6.1.9** Проведение аудита ЛВС сетевым сканером. *Определение методов управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе*	2
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	**20**
	Тема 6.2.1 Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	2
	Тема 6.2.2 *Меры защиты информации в государственных информационных системах*	*2*
	Тема 6.2.3 *Выбор мер защиты информации для реализации в информационной системе в рамках системы защиты информации*	*2*
	Тема 6.2.6 *Содержание мер защиты информации в информационной системе*	*2*
	Тема 6.2.7 *Регламентация и контроль использования в информационной системе мобильных технических средств*	*2*

	Тема 6.2.8 *Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)*	*2*
	Тема 6.2.9 *Ограничение программной среды (ОПС)*	*2*
	Тема 6.2.10 *Контроль (анализ) защищенности информации (АНЗ)*	*2*
	В том числе практических и лабораторных занятий:	4
	Практическое занятие №22 (в форме практической подготовки) **Тема 6.2.4** Выбор мер защиты информации для их реализации в информационной системе: *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации*	2
	Практическое занятие №23 (в форме практической подготовки) **Тема 6.2.5** Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке: *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации*	2
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Содержание**	**36**
	Тема 6.3.1 *Влияние уязвимости ОС на безопасность средств защиты.*	*2*
	Тема 6.3.2 *Реализация внешнего контроля ОС*	*2*
	Тема 6.3.3 *Комплексные средства обеспечения защиты рабочих станций и серверов на уровне данных, приложений, сети, ОС и периферийного оборудования*	*2*
	Тема 6.3.4 *Программные средства оценки защищенности и аудита информационной безопасности*	*2*
	Тема 6.3.5 *Отечественные типовые решения для построения VPN: аппаратно-программный комплекс КРИПТОН-IP КОМПАНИИ «АНКАД» для VPN, решение ViPNet Custom российской компании «Инфотекс», решения*	*2*

	«Микротест» на базе сертифицированных VPN-продуктов компании «Инфотекс»	
	Тема 6.3.6 *Зарубежные типовые решения для построения VPN: межсетевые экраны Juniper Networks (NetScreen), решение компании Lucent Technologies(Lucent Secure VPN), решение компании Cisco Systems*	*2*
	Тема 6.3.7 *Сравнительный анализ оборудования для филиалов при построении VPN: Check Point в филиале, Check Point в центре- Branch в филиале*	*2*
	Тема 6.3.8 *Принципы подключения мобильных пользователей, находящихся за динамическим NAT-ом, по защищенному каналу к разделяемым ресурсам*	*2*
	Тема 6.3.9 *Принципы Построения отказоустойчивого решения с балансировкой трафика (GRE+EIGRP)*	*2*
	Тема 6.3.10 *Современная антивирусная индустрия: отечественные и зарубежные разработки.*	*2*
	Тема 6.3.13 *Одновендорные и мультивендорные комплексные системы автоматизированной защиты*	*2*
	Тема 6.3.14 *Правовые основы обеспечения антивирусной защиты информационных систем. Организация антивирусной защиты на предприятии.*	*2*
	Тема 6.3.17 *DLP системы: назначение и принципы работы*	*2*
	В том числе практических и лабораторных занятий:	**10**
	Практическое занятие №24 (в форме практической подготовки) **Тема 6.3.11** Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов: *Обеспечение безопасности рабочих станций и серверов*	2
	Практическое занятие №25 (в форме практической подготовки) **Тема 6.3.12**	2

	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов: *Обеспечение безопасности рабочих станций и серверов*	
	Практическое занятие №26 (в форме практической подготовки) **Тема 6.3.15** Изучение типовых решений для построения VPN на примере VipNet или других аналогов: *Обеспечение безопасности рабочих станций и серверов*	2
	Практическое занятие №27 (в форме практической подготовки) **Тема 6.3.16** Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов: *Обеспечение безопасности рабочих станций и серверов*	2
	Практическое занятие №28 (в форме практической подготовки) **Тема 6.3.18** Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов: *Обеспечение безопасности рабочих станций и серверов*	2
		30
Курсовая работа		
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 7. Виброакустические средства современных систем обеспечения информационной безопасности. 8. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 9. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 10. Средства обеспечения информационной безопасности банков данных. 11. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 12. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации. 13. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 14. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 15. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 16. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 17. Инструментальные средства анализа рисков информационной безопасности. 18. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 19. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности). 20. Анализ методов и средств анализа защищенности беспроводных сетей. 21. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения	

В том ччисле промежуточная аттестация		6
МДК.02.02. Криптографические средства защиты информации		*138/60*
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**	30
	Тема 1.1.1 Элементы теории множеств. Группы, кольца, поля.	2
	Тема 1.1.2 Делимость чисел. Признаки делимости. Простые и составные числа.	2
	Тема 1.1.3 Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2
	Тема 1.1.4 Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2
	Тема 1.1.5 Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	2
	Тема 1.1.6 Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	2
	Тема 1.1.7 Китайская теорема об остатках.	2
	Тема 1.1.8 Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	2
	Тема 1.1.9 Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2
	Тема 1.1.10 Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2

	Тема 1.1.11 Арифметические операции над большими числами.	2
	Тема 1.1.12 Эллиптические кривые и их приложения в криптографии.	2
	В том числе практических и лабораторных занятий:	**6**
	Практическое занятие №1 (в форме практической подготовки) **Тема 1.1.13** Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	2
	Практическое занятие №2 (в форме практической подготовки) **Тема 1.1.14** Проверка чисел на простоту	2
	Практическое занятие №3 (в форме практической подготовки) **Тема 1.1.15** Решение задач с элементами теории чисел.	2
Раздел 2. Классическая криптография		
Тема 2.1. Методы криптографического защиты информации	**Содержание**	**14**
	Тема 2.1.1 Классификация основных методов криптографической защиты. Методы симметричного шифрования	2
	Тема 2.1.2 Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2
	Тема 2.1.3 Методы перестановки. Табличная перестановка, маршрутная перестановка	2
	Тема 2.1.4 Гаммирование. Гаммирование с конечной и бесконечной гаммами	2
	В том числе практических и лабораторных занятий:	**6**
	Практическое занятие №4 (в форме практической подготовки) **Тема 2.1.5** Применение классических шифров замены	2

	Практическое занятие №5 (в форме практической подготовки) **Тема 2.1.6** Применение классических шифров перестановки	2
	Практическое занятие №6 (в форме практической подготовки) **Тема 2.1.7** Применение метода гаммирования	2
Тема 2.2. Криптоанализ	**Содержание**	**12**
	Тема 2.2.1 Основные методы криптоанализа. Криптографические атаки.	2
	Тема 2.2.2 Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	2
	Тема 2.2.3 Перспективные направления криптоанализа, квантовый криптоанализ.	2
	В том числе практических и лабораторных занятий:	**6**
	Практическое занятие №7 (в форме практической подготовки) **Тема 2.2.4** Криптоанализ шифра простой замены методом анализа частотности символов	2
	Практическое занятие №8 (в форме практической подготовки) **Тема 2.2.5** Криптоанализ классических шифров методом полного перебора ключей	2
	Практическое занятие №9 (в форме практической подготовки) **Тема 2.2.6** Криптоанализ шифра Вижинера	2
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание**	**6**
	Тема 2.3.1 Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	2
	Тема 2.3.2 Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	2

	В том числе практических и лабораторных занятий:	**2**
	Практическое занятие №10 (в форме практической подготовки) **Тема 2.3.3** Применение методов генерации ПСЧ	2
Раздел 3. Современная криптография		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание**	**18**
	Тема 3.1.1 Кодирование информации. Символьное кодирование. Смысловое кодирование.	2
	Тема 3.1.2 Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.	2
	Тема 3.1.3 Компьютеризация шифрования. Аппаратное и программное шифрование	2
	Тема 3.1.4 Стандартизация программно-аппаратных криптографических систем и средств.	2
	Тема 3.1.5 Изучение современных программных и аппаратных криптографических средств	2
	Тема 3.1.6 *Применение современных программных и аппаратных криптографических средств для организации защищенных компьютерных систем*	2
	В том числе практических и лабораторных занятий:	**6**
	Практическое занятие №11 (в форме практической подготовки) **Тема 3.1.7** Кодирование информации	2
	Практическое занятие №12 (в форме практической подготовки) **Тема 3.1.8** Программная реализация классических шифров	2
	Практическое занятие №13 (в форме практической подготовки) **Тема 3.1.9**	2

	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
Тема 3.2. Симметричные системы шифрования	**Содержание**	**6**
	Тема 3.2.1 Общие сведения. Структурная схема симметричных криптографических систем 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	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №14 (в форме практической подготовки) **Тема 3.2.2** *Применение режимов работы блочных шифров. Схемы кратного шифрования*	2
	Практическое занятие №15 (в форме практической подготовки) **Тема 3.2.3** Изучение программной реализации современных симметричных шифров	2
Тема 3.3. Асимметричные системы шифрования	**Содержание**	**8**
	Тема 3.3.1 Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом.	2
	В том числе практических и лабораторных занятий:	**6**
	Практическое занятие №16 (в форме практической подготовки) **Тема 3.3.2** Применение различных асимметричных алгоритмов.	2
	Практическое занятие №17 (в форме практической подготовки) **Тема 3.3.3** *Проведение криптоанализа алгоритмов с открытым ключом*	*2*

	Практическое занятие №18 (в форме практической подготовки) **Тема 3.3.4** Изучение программной реализации асимметричного алгоритма RSA	2
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание**	**10**
	Тема 3.4.1 Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	2
	В том числе практических и лабораторных занятий:	**8**
	Практическое занятие №19 (в форме практической подготовки) **Тема 3.4.2** Применение различных функций хеширования.	2
	Практическое занятие №20 (в форме практической подготовки) **Тема 3.4.3** Анализ особенностей хешей	2
	Практическое занятие №21 (в форме практической подготовки) **Тема 3.4.4** Применение криптографических атак на хеш-функции.	2
	Практическое занятие №22 (в форме практической подготовки) **Тема 3.4.5** Изучение программно-аппаратных средств, реализующих основные функции ЭП	2
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание**	**6**
	Тема 3.5.1 Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №23 (в форме практической подготовки) **Тема 3.5.2** Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2

	Практическое занятие №24 (в форме практической подготовки) **Тема 3.5.3** Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание**	**8**
	Тема 3.6.1 Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	2
	Тема 3.6.2 Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №25 (в форме практической подготовки) **Тема 3.6.3** *Применение протоколов WPA, WEP для организации безопасного функционирования беспроводной сети*	2
	Практическое занятие №26 (в форме практической подготовки) **Тема 3.6.4** *Подбор оборудования для реализации проекта беспроводной сети предприятия*	2
Тема 3.7. Защита информации в электронных платежных системах	**Содержание**	**10**
	Тема 3.7.1 Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	2
	Тема 3.7.2 Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2
	Тема 3.7.3 *Оценка защищенности систем электронных платежей*	2
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №27 (в форме практической подготовки) **Тема 3.7.4** Применение аутентификации по одноразовым паролям.	2

	Практическое занятие №28 (в форме практической подготовки) **Тема 3.7.5** Реализация алгоритмов создания одноразовых паролей	2
Тема 3.8. Компьютерная стеганография	**Содержание**	**8**
	Тема 3.8.1 Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации.	1
	Тема 3.8.2 Защита авторских прав. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	1
	В том числе практических и лабораторных занятий:	**4**
	Практическое занятие №29 (в форме практической подготовки) **Тема 3.8.3** Обзор существующего ПО для встраивания ЦВЗ	2
	Практическое занятие №30 (в форме практической подготовки) **Тема 3.8.4** Сравнительный анализ существующего ПО для встраивания ЦВЗ	2
В том числе промежуточная аттестация в форме дифференцированного зачета		**2**
Примерная тематика самостоятельной работы: 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 6. История развития криптографии 7. Программная реализация классических шифров 8. Оптимизация методов частотного анализа моноалфавитных шифров. 9. Программная реализация классических шифров 10. Методы механизации шифрования		**26**

11. Цифровое представление различных форм информации 12. Анализ современных симметричных криптоалгоритмов 13. Анализ современных асимметричных криптоалгоритмов 14. Программная реализация современных криптоалгоритмов 15. Сравнительный анализ функций хеширования 16. Аутентификация сообщений 17. Законодательство в области криптографической защиты информации 18. Перспективные направления криптографии	
Тематика домашних заданий: 1. Изучение аналитических обзоров в области построения систем защиты информации 2. Выполнение индивидуального задания по теме «Комплекс мер по защите информации для автономного объекта». 3. Выполнение индивидуального задания по теме «Анализ уязвимости объектов защиты» 4. Изучение сетевых утилит 5. Конфигурирование сетевого интерфейса 6. Анализ политик безопасности информационного объекта 7. Изучение аналитических обзоров в области построения систем безопасности 8. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации. 9. Оценка защищенности беспроводной линии связи 10. Проектирование безопасной беспроводной сети 11. Сбор информации о клиентских устройствах 12. Анализ существующей сети 13. Средства обеспечения целостности информации. 14. Активное сетевое оборудование и защита информации. 15. Списки контроля доступа. 16. Защита информации в ОС семейства Windows. 17. Защита информации в ОС семейства Linux.	

18. Защита информации в ОС семейства MacOS. 19. Реализация программной системы парольной аутентификации. 20. Принципы построения VPN. 21. Архитектура систем активного аудита. 22. Атака на переполнение буфера. 23. ГОСТ 28147-89 24. Симметричное блочное шифрование. 25. Электронный документ и его атрибуты. 26. Неотрекаемость цифровой подписи. 27. Написать программу для расчёта значения HASH для строки: «There are no shortcuts to any place worth going» 28. Формирование запроса на сертификат и выпуск сертификата в тестовом УЦ КриптоПРО. 29. Облачная подпись. 30. Работа с облачным сервисом ЭЦП	
Учебная практика: 1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах 2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации 5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации 6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 7. Устранение замечаний по результатам проверки 8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. 9. Применение математических методов для оценки качества и выбора наилучшего программного средства	**144**

10. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи *11. Определение правил и процедур управления системой защиты информации автоматизированной системы;* *12. Определение правил и процедур выявления инцидента;* *13. Определение правил и процедур реагирования на инциденты;* 14. *Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации.*	
Производственная практика: 1. Анализ принципов построения систем информационной защиты производственных подразделений. 2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. 3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; 4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении 5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации *6.* Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. *7. Определение правил и процедур управления системой защиты информации автоматизированной системы;* *8. Определение правил и процедур выявления инцидента;* *9. Определение правил и процедур реагирования на инциденты;* 10. *Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации.* *11. Выбора и обоснования критериев выбора эффективности функционирования защищенных автоматизированных систем;* *12. Проведения экспертизы состояния защищенности информации автоматизированных систем;* *13. Проведения предварительных испытаний системы защиты информации автоматизированной системы;* *14. Уточнения модели угроз безопасности информации автоматизированной системы.;* 15. *Проведения занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне*	**216**

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к матераально-техническому обеспечению

Реализация программы предполагает наличие учебных кабинетов - Кабинет №23 Лаборатория Программных и программно-аппаратных средств обеспечения информационной безопасности

Оборудование учебного кабинета и рабочих мест кабинета

– лекционная аудитория: посадочных мест 30,

рабочее место преподавателя,

проектор,

персональный компьютер,

комплект презентаций.

Антивирусные программные комплексы,

программно – аппаратные средства защиты информации от НСД,

блокировка доступа и нарушения целостности,

программные и программно – аппаратные средства обнаружения вторжений;

средства уничтожения остаточной информации в запоминающих устройствах;

программные средства выявления уязвимостей в АС и СВТ;

программные средства криптографической защиты информации;

программные средства защиты среды виртуализации –VIPNet PKI Client. Крипто АРМ.

4.2. Информационное обеспечение обучения

4.2.1 Основные печатные источники:

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-

Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111053 (дата обращения: 11.07.2023). — Режим доступа: для авториз. пользователей.

2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черёмушкин - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности – ISBN 658-9-2568-3258-8 - Текст : непосредственный.

3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов – М.: Горячая линия – Телеком, 2017.- 175 с. – ISBN 654-8-4468-7764-5- Текст : непосредственный.

4. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов М.: Горячая линия – Телеком, 2016.- 248 с. – ISBN 852-4-5691-7764-5- Текст : непосредственный.

5. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии:/ С.А. Жданов, Н.Ю. Иванова, В.Г Маняхина – М.: Издательский центр «Академия», 2014. – ISBN 852-6-54-159874 - Текст : непосредственный.

6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие / М.А.Иванов - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений. – ISBN 6589-4468-2885-8 - Текст : непосредственный.

7. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с. – ISBN 852-8-4468-3383-3 - Текст : непосредственный.

8. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации :/ Б. В. Костров, В. Н Ручкин – М.: Издательский центр «Академия», 2016. – ISBN 978-5-4468-7764-5 - Текст : непосредственный.

9. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд. :/ А.П. Курило, Н.Г Милославская, М.Ю. Сенаторов, А.И. Толстой - М.: Горячая линия-Телеком, 2014. – ISBN 456-5-4468-2878-5 Текст : непосредственный.

10. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. ПетраковМ.: Академия, - 336 с. – 2012 – ISBN 652-8-4468-3698-8 - Текст : непосредственный.

11. Мельников Д. Информационная безопасность открытых систем. :/ Д. Мельников. - М.: Форум, 2013. – ISBN 987-5-3355-7788-5 Текст : непосредственный.

12. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. / В.К. Новиков М.: МИЭТ, 2013. – 184 с. – ISBN 852-8-4468-3258-5 - Текст : непосредственный.

13. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание :/ В. Олифер, Н. Олифер – Питер, 2015. – ISBN 2658-5-4468-454-5 Текст : непосредственный.

14. 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 – ISBN 654-8-5679-3258-5 - Текст : непосредственный.

15. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы :/ С.В. Синицын, А.В. Батаев, Н.Ю. Налютин – М.: Издательский центр «Академия», 2013. – ISBN 5689-4468-7764-5 Текст : непосредственный.

16. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие :/ Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – ISBN 8978-8899-7764-5 Текст : непосредственный.

17. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд :/ Э. Таненбаум, Д. Уэзеролл – Питер, 2013. – ISBN 6657-4468-2365-5 Текст : непосредственный.

18. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, / В.Ф. Шаньгин - 2012 – ISBN 869-8-4468-3266-8 - Текст : непосредственный.

4.2.2. Дополнительные печатные источники:

19. 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. / Б.А. Погорелов, В.Н. Сачков – М.: МЦНМО, 2006 г – ISBN 852-8-3697-3258-5 - Текст : непосредственный.

20. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – Текст : непосредственный.
21. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – Текст : непосредственный.
22. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». – Текст : непосредственный.
23. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». – Текст : непосредственный.
24. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». – Текст : непосредственный.
25. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». – Текст : непосредственный.
26. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». – Текст : непосредственный.
27. 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». – Текст : непосредственный.
28. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. – Текст : непосредственный.
29. 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. – Текст : непосредственный.
30. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. – Текст : непосредственный.
31. 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. – Текст : непосредственный.
32. 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. – Текст : непосредственный.

33. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. – Текст : непосредственный.
34. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Текст : непосредственный.
35. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Текст : непосредственный.
36. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. – Текст : непосредственный.
37. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Текст : непосредственный.
38. 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. – Текст : непосредственный.
39. 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». – Текст : непосредственный.
40. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». – Текст : непосредственный.

41. 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 – Текст : непосредственный.
42. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий – Текст : непосредственный.
43. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Текст : непосредственный.
44. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети – Текст : непосредственный.
45. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью – Текст : непосредственный.
46. 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 – Текст : непосредственный.
47. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности – Текст : непосредственный.
48. 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. – Текст : непосредственный.
49. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Текст : непосредственный.
50. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования" – Текст : непосредственный.
51. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Текст : непосредственный.
52. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Текст : непосредственный.

53. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Текст : непосредственный.
54. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Текст : непосредственный.
55. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Текст : непосредственный.
56. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005. – Текст : непосредственный.
57. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993. – Текст : непосредственный.
58. 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. – Текст : непосредственный.
59. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014. – Текст : непосредственный.
60. 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. – Текст : непосредственный.
61. 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. – Текст : непосредственный.
62. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Текст : непосредственный.

63. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002. – Текст : непосредственный.
64. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Текст : непосредственный.
65. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Текст : непосредственный.
66. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002. – Текст : непосредственный.
67. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Текст : непосредственный.
68. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. – Текст : непосредственный.
69. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г. – Текст : непосредственный.

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

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

4.2.3. Периодические издания:

62. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей. – Текст : непосредственный.
63. Защита информации. Инсайд: Информационно-методический журнал – Текст : непосредственный.
64. Информационная безопасность регионов: Научно-практический журнал – Текст : непосредственный.
65. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области

информационной безопасности.. URL: http://cyberrus.com/. – Текст : электронный.
66. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/. – Текст : электронный.

4.2.4. Электронные источники:

67. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) : URL: www.fstec.ru – Текст : электронный.
68. Информационно-справочная система по документам в области технической защиты информации :URL: www.fstec.ru – Текст : электронный.
69. Образовательные порталы по различным направлениям образования и тематике :URL: http://depobr.gov35.ru/ – Текст : электронный.
70. Справочно-правовая система «Консультант Плюс» :URL: www.consultant.ru – Текст : электронный.
71. Справочно-правовая система «Гарант» » :URL: www.garant.ru – Текст : электронный.
72. Федеральный портал «Российское образование :URL: www.edu.ru – Текст : электронный.
73. Федеральный правовой портал «Юридическая Россия» :URL: http://www.law.edu.ru/ – Текст : электронный.
74. Российский биометрический портал :URL: www.biometrics.ru – Текст : электронный.
75. Федеральный портал «Информационно- коммуникационные технологии в образовании» :URL: htpp\\:www.ict.edu.ru – Текст : электронный.
76. Сайт Научной электронной библиотеки :URL: www.elibrary.ru – Текст : электронный.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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 обеспеч защиты информа автоматизирован 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	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

последствий компьютерных атак.		
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- участие в профориентационной работе; - участие в профессиональных конкурсах; - участие в научно-исследовательской работе.	-отчеты по итогам производственной (по профилю специальности) практики. - создание портфолио обучающихся. - отзывы научных руководителей.
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- планирование информационного поиска из широкого набора источников, необходимого для выполнения профессиональных задач; - провсдение анализа полученной информации, выделяет в ней главные аспекты; структурировать отобранную информацию в соответствии с параметрами поиска; - интерпретация полученной информации в контексте профессиональной деятельности	Наблюдение и экспертная оценка на практических занятиях и при выполнении работ на учебной практике
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	- использование актуальной нормативно-правовой документацию по специальности; - применение современной научной профессиональной терминологии; - определение траектории профессионального развития и самообразования	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с	- участие в деловом общении для эффективного решения деловых задач; - планирование	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по

коллегами, руководством, клиентами.	профессиональной деятельности; - организация работы коллектива и команды; - взаимодействие с коллегами, руководством, клиентами в ходе профессиональной деятельности.	профилю специальности) практиках
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- использование вербальных и невербальных способов коммуникации на государственном языке с учетом особенностей и различий социального и культурного контекста; - соблюдение норм публичной речи и регламента; - самостоятельный выбор стиля монологического высказывания (служебный доклад, выступление на совещании, презентация проекта и т.п.) в зависимости от его цели и целевой аудитории и с учетом особенностей и различий социального и культурного контекста; - создание продукта письменной коммуникации определенной структуры на государственном языке; - самостоятельный выбор стиля (жанра) письменной коммуникации на государственном языке в зависимости от цели, содержания и адресата.	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках
ОК 6. Проявлять гражданско-патриотическую	- осознание конституционных прав и обязанностей;	Наблюдение и экспертная оценка на учебных занятиях и на учебной и

позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение закона и правопорядка. - участие в мероприятиях гражданско-патриотического характера, волонтерском движении. - аргументированное представление и отстаивание свое мнение с соблюдением этических норм и общечеловеческих ценностей. - осуществление своей деятельности на основе соблюдения этических норм и общечеловеческих ценностей; - демонстрирование сформированности российской гражданской идентичности, патриотизма, уважения к своему народу, уважения к государственным символам (гербу, флагу, гимну).	производственной (по профилю специальности) практиках
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- обладание нормами экологической чистоты и безопасности. - осуществление деятельности по сбережению ресурсов и сохранению окружающей среды. - прогнозирование техногенные последствия для окружающей среды, бытовой и производственной деятельности человека; - прогнозирование возникновений опасных ситуаций по характерным признакам их появления, а	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках

	также на основе анализа специальной информации, получаемой из различных источников; - владение приемами эффективных действий в опасных и чрезвычайных ситуациях природного, техногенного и социального характера.	
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- классифицирование оздоровительных систем физического воспитания, направленных на укрепление здоровья, профилактику профессиональных заболеваний, вредных привычек и увеличения продолжительности жизни; - соблюдение норм здорового образа жизни, осознанное выполнение правил безопасности жизнедеятельности; - составление своего индивидуального комплекса физических упражнений для поддержания необходимого уровня физической подготовленности; - организация собственной деятельности по укреплению здоровья и физической выносливости	Наблюдение и экспертная оценка на практических занятиях и при выполнении работ на учебной практике
ОК 9. Использовать информационные технологии в профессиональной деятельности.	- планирование информационного поиска; - принятие решения о завершении (продолжении) информационного поиска на основе оценки достоверности	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках

	(противоречивости) полученной информации для решения профессиональных задач; - осуществление обмена информации с использованием современного оборудования и программного обеспечения, в том числе на основе сетевого взаимодействия; - анализ информации, выделение в ней главных аспектов, структурирование, презентация.	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- изучение нормативно-правовой документации, технической профессиональной документации на государственном и иностранном языке, литературы и современных научных разработок в области будущей профессиональной деятельности на государственном языке; - применение необходимого лексического и грамматического минимума для чтения и перевода иностранных текстов профессиональной направленности; - владение современной научной и профессиональной терминологией; - самостоятельное совершенствование устной	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках

	и письменной речи и пополнение словарного запаса; - владение навыками технического перевода текста, понимание содержания инструкций и графической документации на иностранном языке в области профессиональной деятельности.	