МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Саратовский государственный технический
университет имени Гагарина Ю.А.»

Профессионально-педагогический колледж

УТВЕРЖДАЮ
Директор
Профессионально-педагогического
колледжа СГТУ имени Гагарина Ю.А.
_____ Т.И. Кузнецова
«29» _____2023 г.

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ
специальность
10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рабочая программа рассмотрена
на заседании цикловой методической комиссии
информационной безопасности и компьютерных систем
протокол № 10 от « 09 » 06 2023 г.
Председатель ЦМК _____ М.А. Ястребова

Саратов 2023

Рабочая программа профессионального модуля разработана в соответствии с Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки РФ от 9 декабря 2016 года № 1553

Разработчики:
Богданов В.Ю. – преподаватель ППК СГТУ имени Гагарина Ю.А,
Гаврилова Е.А.– преподаватель ППК СГТУ имени Гагарина Ю.А.

Рецензенты:
Внутренний: Ястребова М.А. – преподаватель высшей квалификационной категории ППК СГТУ имени Гагарина Ю.А.
Внешний:Жордочкин А.В. - генеральный директор ООО «Ирис»

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 является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

1.2. Место профессионального модуля в структуре ППССЗ:

Профессиональный модуль входит в профессиональный цикл ППССЗ.

1.3. Цели и требования к результатам освоения профессионального модуля

Изучение профессионального модуля направлено на освоение основного вида деятельности 3.4.2 Защита информации в автоматизированных системах программными и программно-аппаратными средствамии соответствующих ему общих компетенций и профессиональных компетенций.

1.3.1. Перечень общих компетенций

Код	Наименование результата обучения
ОК01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.3.2. Перечень профессиональных компетенций

Код	Наименование результата обучения
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.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт в	– установке и настройке программных средств защиты информации; – тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; – учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности;
уметь	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – использовать типовые программные криптографические средства, в том числе электронную подпись; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
знать	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; – основные понятия криптографии и типовых криптографических методов и средств защиты информации;

1.4. Количество часов на освоение программы профессионального модуля:

Максимальной учебной нагрузки обучающегося – 680 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося – 376 часов;
самостоятельной работы обучающегося – 36 часов;

консультации – 4 часа;
учебной практики – 108 часов;
производственной практики – 144 часа;
экзамен квалификационный -12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	**Наименование разделов профессионального модуля**	**Суммарный объем нагрузки, час.** *(максимальная учебная нагрузка и практики)*	**Объем времени, отведенный на освоение МДК**								**Практика**		**Экзамен квалификационный**
			Обязательная аудиторная учебная нагрузка обучающегося					**Самостоятельная работа обучающегося**		**Консультации**			
			Всего часов	**в т.ч. лаборат. занятия** *(если предусмотрено)* часов	**в т.ч. практич. занятия** *(если предусмотрено)* часов	**в т.ч., курсовая работа (проект)** *(если предусмотрено)* часов	**в т.ч. семинар. занятия** *(если предусмотрено)* часов	**Всего** часов	**в т.ч., курсовая работа (проект)** *(если предусмотрено)* часов		**Учебная** *(если предусмотрено)* часов	**Производственная (по профилю специальности)** часов	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
ОК 01-11, ПК 2.1-2.6	МДК 02.01 Программные и программно-аппаратные средства защиты информации	**254**	**228**	14	36	30	-	**24**	-	**2**			
	МДК 02.02 Криптографические средства защиты информации	**162**	**148**	10	46	-	-	**12**	-	**2**			
	УП 02.01 Учебная практика	**108**									**108**		
	ПП 02.01 Производственная практика	**144**										**144**	
	Экзамен квалификационный	**12**											**12**
	Всего:	**680**	**376**	**24**	**82**	**30**	**-**	**36**	**-**	**4**	**108**	**144**	**12**

2.2. Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект) *(если предусмотрены)* , иные виды учебной работы в соответствии с учебным планом	Объем часов	Уровень освоения	Коды компетенций, формированию которых способствует элемент программ
1	2	3	4	5
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		**254**		
5 семестр				
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**254**		
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		**44**		ОК 01-11, ПК 2.1-2.6
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание учебного материала**	**6**		
	Предмет и задачи программно-аппаратной защиты информации	2	1	
	Основные понятия программно-аппаратной защиты информации	2		
	Классификация методов и средств программно-аппаратной защиты информации	2		
Тема 1.2. Стандарты безопасности	**Содержание учебного материала**	**6**		
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	2	1	
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2		
	Практическое занятие №1 Работа с содержанием нормативных правовых актов по защите информации программными и программно-аппаратными средствами	2	2	
Тема 1.3. Защищенная автоматизированная система	**Содержание учебного материала**	**12**		
	Автоматизация процесса обработки информации. Понятие автоматизированной системы.	2	1	

	Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.	2		
	Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС	2		
	Дискреционные модели. Мандатные модели	2		
	Практическое занятие №2 Исследование корректности систем защиты	2	2	
	Практическое занятие №3Реализация функциональных требований к системам анализа защищённости автоматизированных систем	2	2	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание учебного материала**	**6**		
	Источники дестабилизирующего воздействия на объекты защиты	2	1	
	Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию	2		
	Практическое занятие №4Распределение каналов в соответствии с источниками воздействия на информацию	2	2	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание учебного материала**	**14**		
	Понятие несанкционированного доступа к информации	2	1	
	Основные подходы к защите информации от НСД	2		
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	2		
	Доступ к данным со стороны процесса	2		
	Особенности защиты данных от изменения. Шифрование.	2		
	Практическое занятие №5Реализация установки и настройки программно-аппаратных средств защиты от несанкционированного доступа	2	2	
	Самостоятельная работа обучающихся№1Подготовка доклада по темам: Система защиты информации от несанкционированного доступа «Страж NT» Система защиты информации от несанкционированного доступа «DallasLock» Система защиты информации «Secret NET»	2	3	
Раздел 2. Защита автономных автоматизированных систем		**98**		ОК 01-11, ПК 2.1-2.6
Тема 2.1. Основы	**Содержание учебного материала**	**16**		

защиты автономных автоматизированных систем	Работа автономной АС в защищенном режиме	2	1	
	Алгоритм загрузки ОС. Штатные средства замыкания среды	2		
	Расширение BIOS как средство замыкания программной среды	2		
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	2		
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	2		
	Лабораторное занятие №1 Инсталляция и настройка штатных средств операционных систем, предназначенных для защиты от несанкционированного доступа	2	2	
	Лабораторное занятие №2 Инсталляция и настройка средств контроля целостности защищаемых ресурсов и создания замкнутой программной среды	2	2	
	Самостоятельная работа обучающихся№2Подготовка инструкции на тему: Активизация механизма замкнутой программной среды в СЗИ SecretNet	2	3	
Тема 2.2.Защита программ от изучения	**Содержание учебного материала**	**14**		
	Изучение и обратное проектирование ПО.Способы изучения ПО: статическое и динамическое изучение	2	1	
	Задачи защиты от изучения и способы их решения	2		
	Защита от отладки.	2		
	Защита от дизассемблирования	2		
	Защита от трассировки по прерываниям.	2		
	Лабораторное занятие №3 Исследование механизмов защиты программ от изучения и изменения	2	2	
	Самостоятельная работа обучающихся№3Подготовка доклада по темам: "Обфускация как метод защиты ПО от изучения", "Архивация данных программы как метод защиты ПО от изучения", "Метод самогенерируемого кода в защите ПО от изучения"	2	3	
Промежуточная аттестация – другие формы контроля (средний балл по текущим оценкам успеваемости)				
6 семестр				
Тема 2.3. Вредоносное программное обеспечение	**Содержание учебного материала**	**18**		
	Вредоносное программное обеспечение как особый вид разрушающих воздействий	2	1	
	Классификация вредоносного программного обеспечения. Схема	2		

	заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения			
	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	2		
	Бот-неты. Принцип функционирования. Методы обнаружения	2		
	Классификация антивирусных средств. Сигнатурный и эвристический анализ	2		
	Защита от вирусов в "ручном режиме"	2		
	Основные концепции построения систем антивирусной защиты на предприятии	2		
	Практическое занятие № 6 Работа с программно-аппаратными средствами анализа безопасности антивирусной защиты средств вычислительной техники	2	2	
	Лабораторное занятие №4 Применение средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2	2	
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание учебного материала**	**16**		
	Несанкционированное копирование программ как тип НСД	2	1	
	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	2		
	Привязка ПОк аппаратному окружению и носителям.	2		
	Защитные механизмы в современном программном обеспечении на примере MS Office	2		
	Практическое занятие №7 Работа со специализированными программными средствами защиты информации от несанкционированного копирования	2	2	
	Практическое занятие №8Анализ защитных механизмов в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	2		
	Лабораторное занятие №5 Исследование механизмов защиты программ от незаконного использования и копирования	2		
	Самостоятельная работа обучающихся№4 Подготовка доклада по темам: "Офлайн- и онлайн-программная защита ПО от несанкционированного копирования", "Аппаратная защита ПО от несанкционированного копирования"	2	3	

Тема 2.5. Защита информации на машинных носителях	**Содержание учебного материала**	**12**		
	Проблема защиты отчуждаемых компонентов ПЭВМ.	2	1	
	Методы защиты информации на отчуждаемых носителях. Шифрование.	2		
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2		
	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	2		
	Безвозвратное удаление данных. Принципы и алгоритмы.	2		
	Практическое занятие №9 Применение программ для шифрования данных на съемных носителях	2	2	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание учебного материала**	**4**		
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2	1	
	Устройства TouchMemory	2	1	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание учебного материала**	**18**		
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	2	1	
	Использование сетевых снифферов в качестве СОВ	2		
	Аппаратный компонент СОВ	2		
	Программный компонент СОВ	2		
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений.	2		
	Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	2		
	Практическое занятие №10 Моделирование проведения атаки	2	2	
	Практическое занятие №11Применение инструментальных средств обнаружения вторжений	2	2	
	Самостоятельная работа обучающихся№5Подготовка доклада по теме: "Система обнаружения вторжений Snort", "Методы DataMining в обнаружении аномалий", "Методы технологии мобильных агентов в обнаружении аномалий", "Методы построения иммунных систем", "Применение генетических алгоритмов в обнаружении аномалий", "Применение нейронных сетей в обнаружении аномалий", "Языки описания атак"	2	3	

Промежуточная аттестация – другие формы контроля (средний балл по текущим оценкам успеваемости)				
7 семестр				
Раздел 3. Защита информации в локальных сетях		**6**		
Тема 3.1. Основы построения защищенных сетей	**Содержание учебного материала**	**2**		
	Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP.Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	2	1	ОК 01-11, ПК 2.1-2.6
Тема 3.2. Средства организации VPN	**Содержание учебного материала**	**4**		
	Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2	1	
	Практическое занятие №12 Развертывание VPN	2	2	
Раздел 4. Защита информации в сетях общего доступа		**18**		ОК 01-11, ПК 2.1-2.6
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание учебного материала**	**18**		
	Методы защиты информации при работе в сетях общего доступа.	2	1	
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.	2		
	Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.Уровень 3. Proxy-сервера прикладного уровня.	2		
	Однохостовые и мультихостовыеfirewall.Основные типы архитектур мультихостовыхfirewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	2		
	Требования по сертификации межсетевых экранов	2		
	Практическое занятие №13 Сравнение архитектур DualHomedHost, BastionHost, Perimetr.	2	2	
	Практическое занятие №14Применение различных способовзакрытия "опасных" портов	2	2	

	Самостоятельная работа обучающихся № 6. Обзор современных межсетевых экранов	4	3	
Раздел 5. Защита информации в базах данных		**18**		ОК 01-11, ПК 2.1-2.6
Тема 5.1. Защита информации в базах данных	**Содержание учебного материала**	**18**		
	Основные типы угроз. Модель нарушителя	2	1	
	Средства идентификации и аутентификации. Управление доступом	2		
	Средства контроля целостности информации в базах данных	2		
	Средства аудита и контроля безопасности. Критерии защищенности баз данных	2		
	Применение криптографических средств защиты информации в базах данных	2		
	Практическое занятие №15 Анализ механизмов защиты СУБД MS Access	2	2	
	Практическое занятие №16Сравнительный анализ штатных средств защиты СУБД MSSQL Server	2	2	
	Самостоятельная работа обучающихся № 7. Подготовка доклада по темам: «Новые технологии хранения информации», «Сервисы облачного хранения данных», «Современные технологии дисковых систем»	2	3	
Раздел 6. Мониторинг систем защиты		**38**		ОК 01-11, ПК 2.1-2.6
Тема 6.1. Мониторинг систем защиты	**Содержание учебного материала**	**18**		
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.	2	1	
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2		
	Классификация отслеживаемых событий. Особенности построения систем мониторинга. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	2		
	Классификация сетевых мониторов	2		
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	2		
	Практическое занятие №17 Сравнительный анализ	2	2	

	распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов			
	Лабораторное занятие №6 Проведение аудита ЛВС сетевым сканером	4	2	
	Самостоятельная работа обучающихся № 8. Подготовка доклада по темам: «Новые виды атак на информационную систему», «Актуальные киберугрозы», «Современные методы защиты от сетевых атак»	2	3	
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание учебного материала**	**8**		
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	2	1	
	Практическое занятие №18Выбор программных и программно-аппаратных средств защиты информации в информационной системе и разработка рекомендаций по их настройке	2	2	
	Самостоятельная работа обучающихся № 9. Обзор современных программных и программно-аппаратных средств защиты	4	3	
Тема 6.3. Изучение современных программно-аппаратных комплексов.	**Содержание учебного материала**	**12**		
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	2	1	
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	2		
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	2		
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	2		
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	2		
	Самостоятельная работа обучающихся№10 Обзор крупных утечек информации за год	2	3	
Курсовое проектирование		**30**		
Примерная тематика курсовых проектов: Решение задачи кибербезопасности в условиях интернет вещей				

Решение задачи информационной безопасности детей в сети Интернет Организация защиты информации в дистанционных каналах банковского обслуживания Организация защиты компьютерных систем от программ-вымогателей Организация защиты информации в системах мобильной связи Организация защиты информации в технологии блокчейн Применение систем контроля и учёта действий персонала на предприятии Применение программных сниффероров для анализа сетевого трафика Применение систем обеспечения информационной безопасности на базе программ с открытым кодом Организация защиты информации в веб-приложениях Организация защиты компьютерной сети предприятия от внешних вторжений Организация защиты информации в современных центрах обработки данных Организация защиты интеллектуальной собственности предприятия Решение задачи выявления специальных технических средств несанкционированного получения информации Организация защиты информации в системах контроля и управления доступом Решение задачи безопасных покупок в сети Интернет Решение задач информационной безопасности в облачных технологиях Применение интеллектуальных систем видеонаблюдения на предприятии Решение задачи безопасности информации и личных данных в сети Интернет Организация защиты информации техническими средствами на предприятии Решение задачи информационной безопасности Рунета				
Консультация		2		
Промежуточная аттестация - дифференцированный зачет		2		
Раздел 2 модуля. Применение криптографических средств защиты информации		**162**		
МДК.02.02. Криптографические средства защиты информации		**162**		
5 семестр				
Введение	**Содержание учебного материала**	**2**		
	Предмет и задачи криптографии. История криптографии. Основные термины	2	1	ОК 01-10, ПК 2.4
Раздел 1. Математические основы защиты информации		**32**		
Тема 1.1. Математические основы криптографии	**Содержание учебного материала**	**32**		
	Элементы теории множеств. Группы, кольца, поля.	2	1	
	Делимость чисел. Признаки делимости. Простые и составные числа.	2		
	Основная теорема арифметики. Наибольший общий делитель.	2		

	Взаимно простые числа. Алгоритм Евклида для нахождения НОД.			
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2		
	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	2		
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	2		
	Китайская теорема об остатках.	2		
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	2		
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2		
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2		
	Арифметические операции над большими числами.	2		
	Эллиптические кривые и их приложения в криптографии.	2		
	Практическое занятие №1Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	2	2	
	Практическое занятие №2 Проверка чисел на простоту	2		
	Практическое занятие №3 Решение задач с элементами теории чисел.	2		
	Самостоятельная работа обучающихся № 1. Решение задач по теме: «Сравнения. Свойства сравнений»	2	3	
Раздел 2. Классическая криптография		**40**		ОК 01-10, ПК 2.4
Тема 2.1. Методы криптографического защиты информации	**Содержание учебного материала**	**22**		
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	2	1	
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2		
	Методы перестановки. Табличная перестановка, маршрутная перестановка	2		
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	2		
	Практическое занятие №4 Применение классических шифров	2	2	

	замены			
	Практическое занятие №5 Применение классических шифров перестановки	4		
	Практическое занятие № 6Применение метода гаммирования	4		
	Самостоятельная работа обучающихся № 2. Шифрование и дешифрование сообщений симметричными методами.	2	3	
	Самостоятельная работа обучающихся № 3. Шифрование и дешифрование сообщений асимметричными методами.	2	3	
Тема 2.2. Криптоанализ	**Содержание учебного материала**	**18**		
	Основные методы криптоанализа. Криптографические атаки.	2	1	
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	4		
	Перспективные направления криптоанализа, квантовыйкриптоанализ.	2		
	Лабораторное занятие №1 Криптоанализ шифра простой замены методом анализа частотности символов	2	2	
	Лабораторное занятие №2 Криптоанализ классических шифров методом полного перебора ключей	4		
	Практическое занятие №7 Криптоанализ шифра Вижинера	4		
Промежуточная аттестация – другие формы контроля (средний балл по текущим оценкам успеваемости)				
6 семестр				
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**6**		
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	2	1	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	2	1	
	Практическое занятие №8Применение методов генерации ПСЧ	2	2	
Раздел 3. Современная криптография		**78**		ОК 01-10, ПК 2.4
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**14**		
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	4	1	
	Компьютеризация шифрования. Аппаратное и программное	4	1	

	шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств			
	Практическое занятие №9Кодирование информации	2	2	
	Практическое занятие № 10Программная реализация классических шифров	2	2	
	Лабораторное занятие №3Исследование реализации классических шифров замены и перестановки в программе CrypTool или аналоге	2	2	
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	**10**		
	Общие сведения. Структурная схема симметричных криптографических систем	4	1	
	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	4	1	
	Практическое занятие № 11Программная реализация современных симметричных шифров	2	2	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**8**		
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	2	1	
	Элементы теории чисел в криптографии с открытым ключом.	2	1	
	Практическое занятие № 12 Применение различных асимметричных алгоритмов.	2	2	
	Практическое занятие № 13 Программная реализация асимметричного алгоритма RSA	2	2	
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	**10**		
	Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	4	1	
	Практическое занятие № 14 Применение различных функций хеширования, анализ особенностей хешей	2	2	
	Практическое занятие № 15 Применение криптографических атак на хеш-функции.	2	2	
	Лабораторное занятие №4Сравнительный анализ программно-аппаратных средств, реализующих основные функции ЭП	2	2	

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**8**		
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	4	1	
	Практическое занятие № 16Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2	2	
	Практическое занятие № 17 Принципы работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2	2	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	**10**		
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	4	1	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	4	1	
	Самостоятельная работа обучающихся № 4. Обзор современных методов криптозащиты информации в сетях передачи данных.	2	3	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**	**8**		
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	2	1	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2	1	
	Практическое занятие № 18 Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	2	2	
	Самостоятельная работа обучающихся № 5. Обзор современных методов защиты информации в электронных платежных системах	2	3	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	**10**		
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	2	1	
	Методы компьютерной стеганографии. Цифровые водяные	2	1	

	знаки. Алгоритмы встраивания ЦВЗ			
	Практическое занятие № 19 Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	2	2	
	Практическое занятие № 20 Реализация простейших стеганографических алгоритмов	2	2	
	Самостоятельная работа обучающихся № 6. Подготовка доклада по темам: «Квантовая криптография», «Многолучевая криптография», «Метеорная криптография»	2	3	
Консультация		2		
Промежуточная аттестация – дифференцированный зачет		2		
Учебная практика УП.02.01 **Примерные виды работ:** Составление документации по учету, обработке, хранению и передачи конфиденциальной информации Осуществление установки и настройки программно-аппаратных средств защиты информации Диагностика работоспособности программно-аппаратных средств защиты информации Уничтожение информации с использованием программно-аппаратных средств защиты информации Оценка эффективности применяемых программно-аппаратных средств защиты информации Использование программного обеспечения для передачи конфиденциальной информации Использование типовых криптографических средств		**108**		
Производственная практика ПП.02.01 **Примерные виды работ:** Анализ принципов построения систем информационной защиты производственных подразделений Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении Обеспечение учета, обработки, хранения и передачи конфиденциальной информации Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы Диагностика, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности		**144**		
Всего:		**680**		
Промежуточная аттестация (всего):				

Промежуточная аттестация по МДК.02.01- дифференцированный зачет		
Промежуточная аттестация по МДК.02.02- дифференцированный зачет		
Промежуточная аттестация по ПМ - экзамен квалификационный		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению профессионального модуля

Реализация программы профессионального модуля требует наличия лаборатории программных и программно-аппаратных средств защиты информации для проведения занятий лекционного типа, лабораторных занятий, практических занятий, в том числе групповых, индивидуальных, письменных, устных консультаций, текущего контроля и промежуточной аттестации.

Лаборатория программных и программно-аппаратных средств защиты информации

Оборудование:

- рабочее место преподавателя;
- специализированная мебель (столы, стулья по количеству обучающихся);
- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

Технические средства обучения:

- компьютер (ноутбук);
- мультимедийный проектор, экран.

Учебно-наглядные пособия: плакаты, учебно-наглядные пособия, обеспечивающие тематические иллюстрации по рабочей программе дисциплины, в том числе, видео-аудио материалы, компьютерные презентации.

Компьютер имеет доступ к электронно-библиотечным системам, выход в глобальную сеть Интернет, оснащен лицензионным программным обеспечением.

3.2. Учебно-методическое и информационное обеспечение реализации профессионального модуля

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/

8. 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». - Режим доступа: http://www.consultant.ru/

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. - Режим доступа: http://www.consultant.ru/

10. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/

11. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

12. Приказ ФАПСИ 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». - Режим доступа: http://www.consultant.ru/

13. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

14. 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. – Режим доступа: http://docs.cntd.ru/

15. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

16. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/
17. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/
18. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/
19. 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. – Режим доступа: http://docs.cntd.ru/
20. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/
21. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/
22. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/
23. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/
24. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/
25. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/
26. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/
27. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/
28. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/
29. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/
30. 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. – Режим доступа: http://docs.cntd.ru/

31. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

33. 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. – Режим доступа: http://docs.cntd.ru/

34. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

35. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

36. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0

37. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

38. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

39. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности / учеб. пособие для студ. учреждений сред. проф. образования / Е.Б. Белов, В.Н. Пржегорлинский. - 2-е изд., испр. и доп. - М. : Издательский центр «Академия», 2020. – 336 с. В пер. ISBN 978-5-4468-8456-8

40. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт,

2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Костров Б.В. Сети и системы передачи информации : учебник/ Б.В. Костров, В.Н. Ручкин : (2-е изд.) (в электронном формате) 2019. https://academia-library.ru

42. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

43. Бубнов А.А. Основы информационной безопасности : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. - 3-е изд., стер. - М. : Издательский центр «Академия», 2020. – 256 с. В пер. ISBN 978-5-4468-8682-1

Дополнительныеучебныеиздания

44. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

46. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

47. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

48. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

49. 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. – Режим доступа: http://docs.cntd.ru/

50. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

51. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа:

http://www.consultant.ru/
52. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/
53. 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. - Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

54. Сайт журнала Информационная безопасность - Режим доступа: http://www.itsec.ru
55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/
56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/
57. Федеральный портал. Российское образование. - Режим доступа:http://www.edu.ru

Методические указания для обучающихся по освоению профессионального модуля

58. Методические указания для обучающихся по выполнению практических работ.
59. Методические указания для обучающихся по выполнению заданий самостоятельной работы.
60. Методические указания для обучающихся по выполнению лабораторных работ.
61. Методические рекомендации по подготовке и защите курсовых работ (проектов).
62. Методические указания по выполнению заданий практики.

3.3. Общие требования к организации образовательного процесса

При реализации компетентностного подхода программа профессионального модуля предусматривает использование в образовательном процессе активных и интерактивных форм проведения занятий (применение электронных образовательных ресурсов, деловых игр, разбора конкретных ситуаций, психологических тренингов, групповых дискуссий) в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся.

Реализация практических занятий осуществляется непосредственно в ППК СГТУ имени Гагарина Ю.А.

Образовательная деятельность в форме практической подготовки организована при реализации МДК 02.01 Программные и программно-аппаратные средства защиты информации, МДК 02.02 Криптографические

средства защиты информации, учебной практики, производственной практики, предусмотренных учебным планом следующим образом:

– при реализации МДК 02.01 Программные и программно-аппаратные средства защиты информации, МДК 02.02 Криптографические средства защиты информации практическая подготовка организуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью;

– при проведении практики практическая подготовка организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Учебная практика проводится на базе ППК СГТУ имени Гагарина Ю.А.

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся. Производственная практика проводится концентрировано по завершении освоения МДК 02.01 Программные и программно-аппаратные средства защиты информации, МДК 02.02 Криптографические средства защиты информации.

Формы проведения консультаций для обучающихся: групповые, индивидуальные, письменные, устные.

Программа профессионального модуля реализуется в 5-7 семестрах 3-4 курса обучения. Освоению профессионального модуля должно предшествовать изучение учебных дисциплин: ЕН.01 Математика, ЕН.02 Информатика, ОП.01 Основыинформационной безопасности, ОП.02 Организационно-правовое обеспечение информационной безопасности, ОП.03 Основы алгоритмизации и программирования, ОП.04 Электроника и схемотехника, ОП.07Технические средства информатизации, ОП.08 Инженерная графика, ОП.09 Технологии программирования.

3.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарным курсам, учебной практике, производственной практике:

- наличие высшего профессионального образования, соответствующего профилю преподаваемого модуля;
- наличие опыта деятельности в организациях соответствующей профессиональной сферы;
- получение дополнительного профессионального образования по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Критерии оценки, формы и методы контроля и оценки результатов обучения

Код, наименование профессиональных компетенций	Критерии оценки	Формы и методы контроля и оценки результатов обучения
ПК 2.1Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	- установка и настройка программных средств защиты информации; - применение программных и программно-аппаратных средств защиты информации;	Текущий контроль успеваемости: - опрос устный (фронтальный); - выполнение практической работы (индивидуальная форма работы); - защита рефератов - собеседование по результатам выполненной работы; - наблюдение за процессом выполнения заданий; - демонстрация выполнения видов работ практики; - выполнение письменной работы "Отчет по практике". Межсессионная аттестация – тестирование. Промежуточная аттестация по МДК.02.01 , МДК.02.02 в форме дифференцированного зачета. Промежуточная аттестация по УП.02.01 в форме дифференцированного зачета. Промежуточная аттестация по ПП.02.01в форме дифференцированного зачета. Промежуточная аттестация по ПМ.02 в форме экзамена квалификационного.
ПК 2.2Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	- установка и настройка программных средств защиты информации; - установка и настройка средства антивирусной защиты в соответствии с предъявляемыми требованиями;	
ПК 2.3Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	- тестирование функций программно-аппаратных средств защиты информации; - диагностика программных и программно-аппаратных средств защиты информации; - устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;	
ПК 2.4Осуществлять обработку, хранение и передачу информации ограниченного доступа.	- хранение и передача информации, для которой установлен режим конфиденциальности; - проверка выполнения требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - использование типовых программных криптографических средств, в том числе электронной подписи;	
ПК 2.5Уничтожать информацию и носители информации с использованием	- учет, обработка, хранение и передача информации, длякоторой установлен режим конфиденциальности;	

программных и программно-аппаратных средств.	- установка, настройка, применение программных и программно-аппаратных средств защиты информации;	
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.	- осуществление мониторинга и регистрация сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	

Код, наименование общих компетенций	**Критерии оценки**	**Формы и методы контроля и оценки результатов обучения**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- распознавание задач в профессиональном и/или социальном контексте; - распознавание проблем в профессиональном и/или социальном контексте; - анализ задачи и/или проблемы; - выделение составных частей задачи и/или проблемы; - определение этапов решения задачи; - выявление информации, необходимой для решения задачи и/или проблемы; - осуществление эффективного поиска информации, необходимой для решения задачи и/или проблемы; - разработка плана действия решения задачи и/или проблемы; - определение необходимых ресурсов для решения задачи и/или проблемы; - владение актуальными методами работы в профессиональной и смежных сферах; - реализация составленного плана; - оценка результата и последствий своих действий (самостоятельно или с помощью наставника).	Текущий контроль успеваемости: - опрос устный (фронтальный); - выполнение практической работы (индивидуальная форма работы); - защита рефератов - собеседование по результатам выполненной работы; - наблюдение за процессом выполнения заданий; - демонстрация выполнения видов работ практики; - выполнение письменной работы "Отчет по практике". Межсессионная аттестация – тестирование. Промежуточная аттестация по МДК.02.01 , МДК.02.02 в форме дифференцированного зачета. Промежуточная аттестация по УП.02.01 в форме дифференцированного зачета. Промежуточная аттестация по ПП.02.01в форме дифференцированного зачета.
ОК 02. Осуществлять поиск,	- определение задач поиска	

анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	информации, необходимых источников информации; - планирование процесса поиска необходимой информации; - осуществление поиска информациинеобходимойдля выполнения задач профессиональной деятельности; - проведение анализа информации, необходимой для выполнения задач профессиональной деятельности; - осуществление интерпретации информации, необходимой для выполнения задач профессиональной деятельности; - структурирование получаемой информации; - выделение наиболее значимой в перечне информации; - оценка практической значимости результатов поиска; - оформление результатов поиска.	Промежуточная аттестация по ПМ.02 в форме экзамена квалификационного.
ОК 03.Планировать и реализовывать собственное профессиональное и личностное развитие.	- планирование собственного профессионального развития; - построение траектории собственного профессионального и личностного развития; - реализация собственного профессионального и личностного развития; - определение актуальности нормативно-правовой документации в профессиональной деятельности.	
ОК 04.Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- организация работы коллектива и команды; - эффективное взаимодействие с коллегами, руководством; - эффективное взаимодействие с клиентами.	
ОК 05.Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей	- грамотное изложение своих мыслей на государственном языке с учетом особенностей социального и культурного контекста;	

социального и культурного контекста.	- правильное оформление документов по профессиональной тематике на государственном языке.	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- понимание значимость своей специальности; - описание значимости своей специальности; - презентация структуры профессиональной деятельности по специальности; - проявление гражданско-патриотической позиции; - демонстрация осознанного поведения на основе традиционных общечеловеческих ценностей; - применение стандартов антикоррупционного поведения.	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- содействие сохранению окружающей среды; - содействие ресурсосбережению; - осуществление эффективных действий в чрезвычайных ситуациях; - соблюдение норм экологической безопасности; - определение направлений ресурсосбережения в рамках профессиональной деятельности по специальности	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- использование физкультурно-оздоровительной деятельности для укрепления здоровья, достижения жизненных и профессиональных целей; - применение рациональных приемов двигательных функций в профессиональной деятельности; - использование средств профилактики перенапряжения характерными для данной специальности	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- применение средств информационных технологий для решения профессиональных задач; - использование современного	

	программного обеспечения	
ОК 10.Пользоваться профессиональной документацией на государственном и иностранном языках.	- понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые); - понимание текста на базовые профессиональные темы; - участие в диалогах на знакомые общие и профессиональные темы; - построение простых высказываний о себе и о своей профессиональной деятельности; - краткое обоснование и объяснение своих действий (текущих и планируемых); - написание простых связных сообщений на знакомые или интересующие профессиональные темы	
ОК.11 Использовать знания финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	- выявление достоинств и недостатков коммерческой идеи; - презентация идеи открытия собственного дела в профессиональной деятельности; - оформление бизнес-плана; - расчет размера выплат по процентным ставкам кредитования; - определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности; - презентация бизнес - идеи; - определение источников финансирования	

4.2. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по профессиональному модулю

Показатели и критерии оценивания компетенций

Показатели и критерии оценивания компетенций, описание шкал оценивания содержатся в приложении 1.

Контрольные и тестовые задания

Контрольные задания содержатся в приложении 1.

Методические материалы

Методические материалы, определяющие процедуры оценивания знаний,

умений, характеризующих формирование компетенций, содержатся в приложении 1.

Приложение 1

Контрольно-оценочные средства

для проведения промежуточной аттестации по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

1.1. Форма промежуточной аттестации: Экзамен квалификационный (8 семестр).

1.2. Система оценивания результатов выполнения заданий

Оценивание результатов выполнения заданий промежуточной аттестации осуществляется на основе следующих принципов:

достоверности оценки – оценивается уровень сформированности знаний, умений, практического опыта, общих и профессиональных компетенций, продемонстрированных обучающимися в ходе выполнения задания;

адекватности оценки – оценка выполнения заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания;

надежности оценки – система оценивания выполнения заданий должна обладать высокой степенью устойчивости при неоднократных оценках уровня сформированности знаний, умений, практического опыта, общих и профессиональных компетенций обучающихся;

комплексности оценки – система оценивания выполнения заданий должна позволять интегративно оценивать общие и профессиональные компетенции обучающихся;

объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений преподавателей, осуществляющих контроль или аттестацию.

При выполнении процедур оценки заданий используются следующие основные методы:

- метод экспертной оценки;
- метод расчета первичных баллов;
- метод расчета сводных баллов;
- метод агрегирования.

Результаты выполнения заданий оцениваются в соответствии с разработанными критериями оценки.

Используется сто бальная шкала оценкидля оценивания результатов обучения.

Перевод сто бальной шкалы учета результатов в пяти бальную оценочную шкалу:

Оценка	**Количество баллов, набранных за выполнение теоретического и практического задания**
Оценка 5 «отлично»	90-100
Оценка 4 «хорошо»	76-89
Оценка 3 «удовлетворительно»	50-75
Оценка 2 «неудовлетворительно»	≤ 49

1.3. Контрольно-оценочные средства

1.3.1Задание:

1. Тестирование
2. Практическое задание

Примерное задание «Тестирование»

1. К аспектам информационной безопасности не относится:
а) Доступность
б) Целостность

в) Конфиденциальность
г) Защищенность
2. Один из методов защиты информации на компьютере
а) полное отключение системного блока
б) отключение жесткого диска
в) защита паролем
г) копирование информации.
3. Какого метода разграничения доступа не существует:
а) разграничение доступа по спискам
б) разграничение доступа по уровням секретности и категориям
в) локальное разграничение доступа
г) парольное разграничение доступа
4. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:
а) Авторизация
б) Обезличивание
в) Деперсонализация
г) Аутентифика́ция
д) Идентификация
5. Несанкционированный доступ к информации это:
а) Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
б) Работа на чужом компьютере без разрешения его владельца
в) Вход на компьютер с использованием данных другого пользователя
г) Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
д) Доступ к СУБД под запрещенным именем пользователя
6. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ:
а) Информация составляющая государственную тайну
б) Информация составляющая коммерческую тайну
в) Персональная
г) Конфиденциальная информация
д) Документированная информация
7. Владельцем информации второй категории является…
а) Простые люди
б) Государство
в) Коммерческая организация
г) Муниципальное учреждение
д) Некоммерческая организация
8. Для защиты от злоумышленников необходимо использовать:
а) Системное программное обеспечение
б) Прикладное программное обеспечение
в) Антивирусные программы
г) Компьютерные игры
д) Музыку, видеофильмы
9. Свойство вируса, позволяющее называться ему загрузочным – способность …
а) заражать загрузочные сектора жестких дисков
б) заражать загрузочные дискеты и компакт-диски
в) вызывать перезагрузку компьютера-жертвы
г) подсвечивать кнопку Пуск на системном блоке.
10. Какие файлы заражают макро-вирусы?
а) исполнительные;
б) файлы документов Word и элект. таблиц Excel;
в) графические и звуковые;

г) html документы.
11. Руткит – это:
а) Программа для скрытого взятия под контроль взломанной системы
б) Вредоносная программа, маскирующаяся под макрокоманду
в) Разновидность межсетевого экрана
г) Программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю.
12. Основные меры по защите информации от повреждения вирусами:
а) проверка дисков на вирус
б) создавать архивные копии ценной информации
в) не пользоваться "пиратскими" сборниками программного обеспечения
г) передавать файлы только по сети.
13. Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
а) Подсистема сканирования
б) Подсистема управления
в) Подсистема обнаружения вирусной активности
г) Подсистема устранения вирусной активности
14. Где нужно установить все необходимые параметры для задания пароля при загрузке ОС?
а) В настройках учётной записи.
б) В Bios.
в) Нельзя установить пароль при загрузке ОС.
г) В настройках общего доступа к диску.
15. Биометрические системы защиты - это...
а) системы аутентификации, использующие для удостоверения личности людей их биометрические данные.
б) физические и биологические системы защиты.
в) системы аутентификации, использующие для удостоверения личности людей пароль на основе фамилии, имени или даты рождения.
г) программы для взлома пароля на основе биометрический данных.
16. Как происходит идентификация по радужной оболочке глаза?
а) Изображение самого глаза выделяется из изображения лица, после чего на него накладывается специальная маска штрих-кодов. В результате будет получена матрица, которая индивидуальна для каждого человека.
б) Изображение самого глаза выделяется из изображения лица, после чего полученная информация преобразуется в цифровой код и сравнивается с той, которая находится в памяти компьютера.
в) Изображение самого глаза выделяется из изображения лица, после чего учитывается простая геометрия: размеры и форма, уголки глаз, расположение ресниц и т. д.
17. Межсетевой экран (Брандмауэр, firewall) – это…
а) Комплекс аппаратных средств
б) Комплекс программных средств
в) Комплекс аппаратных или программных средств
г) Комплекс аппаратных и программных средств
18. Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:
а) SSL
б) SET
в) HTTP
г) IPSec
19. Каковы преимущества частных сетей?
а) информация сохраняется в секрете
б) удаленные сайты могут осуществлять обмен информацией незамедлительно
в) удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ

г) низкая стоимость
20. В чем особенность работы VPN?
а) шифровании трафика
б) аутентификации систем
в) создании канала связывающего две системы
21. Из каких структурных единиц состоит шифропроцессор
а) вычислитель
б) блок управления
в) буфер ввода-вывода
22. Криптостойкость – это…
а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
б) свойство гаммы
в) все ответы верны
23. Основные современные методы шифрования:
а) алгоритма гаммирования
б) алгоритмы сложных математических преобразований
в) алгоритм перестановки
24. В чем суть метода перестановки
а) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
б) замена алфавита
в) все правильные
25. Для чего использовался DES-алгоритм из-за небольшого размер ключа
а) закрытия коммерческой информации
б) шифрования секретной информации
в) нет правильного ответа
26. Плюсы программных шифраторов:
а) цена
б) гибкость
в) быстродействие
27. Что требуется для восстановления зашифрованного текста
а) ключ
б) матрица
в) вектор
28. Когда появилось шифрование
а) четыре тысячи лет назад
б) две тысячи лет назад
в) пять тысяч лет назад
29. Первым известным применением шифра считается
а) египетский текст
б) русский
в) нет правильного ответа
30. Какую секретную информацию хранит Windows
а) пароли для доступа к сетевым ресурсам
б) пароли для доступа в интернет
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

Примерное практическое задание:

Ситуация 1
Сотрудники компании АО «Сигнал» имеют возможность во внерабочее время пользоваться персональными компьютерами. Многие из них приводят сюда своих детей школьного возраста для работы на компьютерах, те пользуются принесёнными с собой флеш-картами.

Система антивирусного контроля имеется, но на протяжении более чем полугода она не обновлялась.

Задание.

1. Перечислите нарушения регламента информационной безопасности, которые допущены в компании АО «Сигнал».
2. Опишите последствия от выявленных нарушений информационной безопасности в компании АО «Сигнал».
3. Какие меры по защите информации следует предпринять руководству компании АО «Сигнал»?
4. Разработайте предложения по защите информации с использованием программных и (или) программно-аппаратными средств, в том числе и средств криптографической защиты.

1.3.2. Критерии оценки

Критерии оценки задания «Тестирование»

Максимальное количество баллов за выполнение задания «тестирование» – **30 баллов.**

Оценка за задание «Тестирование» определяется простым суммированием баллов за правильные ответы на вопросы. Один верный ответ равен 1 баллу.

Ответ считается правильным, если:

- при ответе на вопрос закрытой формы с выбором ответа выбран правильный ответ;
- при ответе на вопрос открытой формы дан правильный ответ;
-при ответе на вопрос на установление правильной последовательности установлена правильная последовательность;
-при ответе на вопрос на установление соответствия, если сопоставление произведено верно для всех пар.

Критерии оценки практического задания

№	Критерии оценки	Баллы за критерии оценки
Задание 1		
	Перечислить нарушения регламента информационной безопасности, которые допущены на предприятии	**Максимальный балл – 10 баллов**
	Критерии оценки:	
1	Проведен анализ информационной безопасности (ИБ) ситуации	2
2	Верно определены нарушения регламента ИБ	2
3	Верно указаны структурные элементы регламента ИБ, в которых обнаружены нарушения	2
4	Верно определены свойства информации и информационной инфраструктуры, на которые было оказано воздействие	2
5	Перечислены нормативные акты регулирующие аспекты ИБ предприятия	2
Задание 2		
	Описать последствия от выявленных нарушений информационной безопасности на предприятии	**Максимальный балл – 12 баллов**
	Критерии оценки:	
1	Описаны возможные внутренние последствия, которые несут нарушения ИБ предприятия	4
2	Описаны возможные внешние последствия, которые несут нарушения ИБ предприятия	4
3	Указаны методики и системы мониторинга последствий от выявленных нарушений ИБ	4

	Задание 3	
	Указать меры по защите информации следует предпринять руководству предприятия	**Максимальный балл – 14 баллов**
	Критерии оценки:	
1	Для каждого вида нарушения ИБ предприятия предложены 1-2 меры защиты информации	4
2	Меры защиты обоснованы исходя из рода деятельности предприятия	2
3	Описаны правила ИБ на рабочем месте «нарушителя»	4
4	Указан уровень доступа «нарушителя» к информационной системе	4
	Задание 4	
	Разработать предложения по защите информации с использованием программных и (или) программно-аппаратными средств	**Максимальный балл – 34 баллов**
	Критерии оценки:	
1	Указаны методы защиты оборудования	2
2	Указано аппаратное обеспечение ИБ	4
3	Указано программное обеспечение ИБ	4
4	Разработаны правила пользования электронной почтой	4
5	Разработаны правила управления сетью	4
6	Разработаны правила хранения и передачи данных	4
7	Разработана схема комплексной защиты	6
8	Описан общий принцип работы схемы защиты	6
	ИТОГО	**70**

1.4. Материально-техническое обеспечение для проведения промежуточной аттестации

Аттестация проводится в лаборатории программных и программно-аппаратных средств защиты информации

1.5. Учебно-методическое и информационное обеспечение для проведения промежуточной аттестации

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/

8.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». - Режим доступа: http://www.consultant.ru/

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. - Режим доступа: http://www.consultant.ru/

10. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/

11. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

12. Приказ ФАПСИ 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». - Режим доступа: http://www.consultant.ru/

13. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

14. 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. – Режим доступа: http://docs.cntd.ru/

15. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

16. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/

17. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/

18. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/

19. 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. – Режим доступа: http://docs.cntd.ru/

20. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/

21. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/

22. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/

23. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/

24. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

25. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/

26. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

27. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/

28. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

29. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

30. 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. – Режим доступа: http://docs.cntd.ru/

31. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

33. 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. – Режим доступа: http://docs.cntd.ru/

34. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

35. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

36. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0

37. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

38. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное

образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

39. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности / учеб. пособие для студ. учреждений сред. проф. образования / Е.Б. Белов, В.Н. Пржегорлинский. - 2-е изд., испр. и доп. - М. : Издательский центр «Академия», 2020. – 336 с. В пер. ISBN 978-5-4468-8456-8

40. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Костров Б.В. Сети и системы передачи информации : учебник/ Б.В. Костров, В.Н. Ручкин : (2-е изд.) (в электронном формате) 2019. https://academia-library.ru

42. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

43. Бубнов А.А. Основы информационной безопасности : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. - 3-е изд., стер. - М. : Издательский центр «Академия», 2020. – 256 с. В пер. ISBN 978-5-4468-8682-1

Дополнительные учебные издания

44. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

46. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

47. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

48. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

49. 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. – Режим доступа: http://docs.cntd.ru/

50. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

51. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

52. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/

53. 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. -

Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

54. Сайт журнала Информационная безопасность - Режим доступа: http://www.itsec.ru
55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/
56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/
57. Федеральный портал. Российское образование. - Режим доступа:http://www.edu.ru

Методические указания для обучающихся по освоению профессионального модуля

58. Методические указания для обучающихся по выполнению практических работ.
59. Методические указания для обучающихся по выполнению заданий самостоятельной работы.
60. Методические указания для обучающихся по выполнению лабораторных работ.
61. Методические рекомендации по подготовке и защите курсовых работ (проектов).
62. Методические указания по выполнению заданий практики.