Департамент образования Белгородской области
Областное государственное автономное профессиональное образовательное учреждение «Белгородский индустриальный колледж»

РАБОЧАЯ ПРОГРАММА
Профессионального модуля ПМ.03
«Программно-аппаратные и технические средства защиты информации»

для специальности

10.02.01 Организация и технология защиты информации.

г. Белгород, 2021 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальностям среднего профессионального образования (далее – СПО) 10.02.01 Организация и технология защиты информации.

Рассмотрено
предметно-цикловой комиссией
Протокол заседания № ____
От «____»_____ 202__ г.
Председатель цикловой комиссии
_____/

Утверждаю
Зам. директора по УР
_____/ Выручаева Н.В.
« » _____ 20 г.

Рассмотрено
предметно-цикловой комиссией
Протокол заседания № ____
От «____»_____ _____ 202__ г.
Председатель цикловой комиссии
_____/

Рассмотрено
предметно-цикловой комиссией
Протокол заседания № ____
От «____»_____ 202__ г.
Председатель цикловой комиссии
_____/

Организация - разработчик:
ОГАПОУ «Белгородский индустриальный колледж»

Составитель:
Ченская Ирина Борисовна, преподаватель первой категории специальных дисциплин ОГАПОУ «Белгородский индустриальный колледж»

Рецензент:
Глухова Л.А. - преподаватель высшей категории ОГАПОУ «Белгородский индустриальный колледж»

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.01 «Организация и технология защиты информации» в части освоения основного вида профессиональной деятельности (ВПД**):** Программно-аппаратные и технические средства защиты информации и соответствующих профессиональных компетенций (ПК):

1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.
2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.
3. Проводить регламентные работы и фиксировать отказы средств защиты.
4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Рабочая программа профессионального модуля может быть использована в области программирования компьютерных систем при наличии основного общего, среднего (полного) общего образования. Опыт работы не требуется.

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

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

иметь практический опыт:

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

уметь:

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

знать:

- виды, источники и носители защищаемой информации;
- источники опасных сигналов;
- структуру, классификацию и основные характеристики технических каналов утечки информации;
- классификацию технических разведок и методы противодействия им;
- методы и средства технической защиты информации;
- методы скрытия информации;

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

владеть:
- профессиональной терминологией:
- навыками внедрения и эксплуатации современных средств программно-аппаратной защиты информации;
- способами выявления и нейтрализации программ разрушающего действия;
- навыками разработки и использования межсетевых экранов и систем обнаружения и предотвращения вторжений.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

максимальной учебной нагрузки обучающегося – 652 часа, включая:
обязательной аудиторной учебной нагрузки обучающегося – 436 часов;
самостоятельной работы обучающегося – 216 часов;
учебной практики – 216 часов;
производственной практики – 144 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности Программно-аппаратные и технические средства защиты информации, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1	Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах
ПК 3.2	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов
ПК 3.3	Проводить регламентные работы и фиксировать отказы средств защиты
ПК 3.4	Выявлять и анализировать возможные угрозы информационной безопасности объектов.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения

	информационной безопасности
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10	Применять математический аппарат для решения профессиональных задач.
ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов *(макс. учебная нагрузка и практики)*	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов *(если предусмотрена рассредоточенная практика)*
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1-3.4	**Раздел 1. Технология применения технических методов и средств защиты информации**	**366**	**244**	124		**122**			
ПК 3.1-3.4	**Раздел 2. Технология использования программно-аппаратных средств защиты информации**	**288**	**192**	116		**96**			
	В том числе:								
ПК 3.1-3.4	**Учебная практика**	**216**						216	
ПК 3.1-3.4	**Производственная практика** (по профилю специальности)	**144**							144
	Всего:	**654**	**436**	240		**212**		**216**	

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

3.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
Раздел ПМ 1. Технология применения технических методов и средств защиты информации			**244**	
МДК 03.01. Технические методы и средства, технологии защиты информации			**244**	
Тема 1.1. Основные свойства информации как предмета защиты	**Содержание учебного материала**		**4**	
	1	Введение.		2
	2	Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты		2
Тема 1.2. Демаскирующие признаки объектов защиты	**Содержание учебного материала**		**4**	
	1	Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.		2
	2	Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков		2
Тема 1.3. Источники и носители конфиденциальной информации	**Содержание учебного материала**		**2**	
	1	Понятие об источниках, носителях и получателях информации. Классификация источников информации. Виды носителей информации (люди, физические поля, электрические сигналы и материальные тела)		2
Тема 1.4. Источники опасных сигналов	**Содержание учебного материала**		**6**	
	1.	Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства и системы		2
	2.	Побочные электромагнитные излучения и наводки. Акустоэлектрические преобразователи, их виды и принципы работы		2
Тема 1.5. Способы несанкционированного доступа к источникам информации	**Содержание учебного материала**		**2**	
	1.	Понятие о разведывательном контакте и его условиях. Принципы доступа к источникам информации без физического проникновения к контролируемую зону		2
Тема 1.6. Способы и средства перехвата сигналов	**Содержание учебного материала**		**4**	
	1.	Задачи, решаемые при перехвате сигналов. Структура средств перехвата и их функции.		2
	2.	Принципы определения координат источников радиоизлучений и анализа сигналов		2

Тема 1.7. **Способы и средства подслушивания акустических сигналов**	**Содержание учебного материала**		**12**	
	1.	Структура и характеристики технических средств подслушивания.		2
	2.	Принципы работы и характеристики диктофонов для скрытной записи. Классификация и характеристики закладных устройств.		2
	3.	Варианты камуфлирования закладных устройств. Способы и средства лазерного подслушивания и ВЧ-навязывания		2
Тема 1.8. **Технические каналы утечки информации**	**Содержание учебного материала**		**20**	
	1.	Характеристики каналов утечки информации. Типовая структура технического канала утечки информации.		2
	2.	Оптические каналы утечки информации		2
	3.	Радиоэлектронные каналы утечки информации		2
	4.	Акустические каналы утечки информации		2
	5.	Материально-вещественные каналы утечки информации		2
Тема 1.9. **Концепция технической защиты информации**	**Содержание учебного материала**		**10**	
	1.	Применение комплекса радиоконтроля спектр МК		2
	2.	Применение нелинейного радиолокатора NR-м		2
	3.	Применение детектора поля ST-007 и Мозайка ПК+		2
Тема 1.10. **Способы и средства инженерной защиты и технической охраны**	**Содержание учебного материала**		**24**	
	1.	Модели злоумышленников. Уровни физической безопасности объектов охраны. Показатели эффективности инженерно-технической охраны объектов		2
	2.	Способы и средства инженерной защиты объектов.		2
	3.	Способы и средства обнаружения злоумышленников и пожара		2
	4.	Способы и средства видеоконтроля. Структура системы видеоконтроля		2
	5.	Способы и средства нейтрализации угроз		2
	6.	Средства управления системой охраны. Автоматизированные интегральные системы охраны объектов, их структура и тенденция развития		
Тема 1.11. **Способы и средства защиты информации на предприятии**	**Содержание учебного материала**		**20**	
	1.	Способы и средства противодействия наблюдению в оптическом диапазоне волн. Особенности маскировки в видимом и ИК-диапазонах света		2
	2.	Способы и средства противодействия радиолокационному и гидроакустическому наблюдению. Способы активного подавления сигналов радиолокаторов		2
	3.	Способы и средства информационного скрытия акустических сигналов и речевой информации. Сущность способов технического закрытия, их сравнительный анализ.		2
	4.	Способы и средства энергетического скрытия акустических сигналов. Основные звукопоглощающие материалы и способы их применения. Способы оценки энергетических и информационных показателей безопасности речевой информации		2
	5.	Способы и средства предотвращения утечки информации с помощью закладных устройств. Классификация средств обнаружения, локализации и подавления закладных устройств.		2
Тема 1.12.	**Содержание учебного материала**		**12**	

Организационные и технические меры по технической защите информации в организации	1.	Краткая характеристика государственной системы защиты информации. Основные руководящие и нормативные документы по организации технической защиты информации в организации, их сущность		2
	2.	Сущность организационных и технических мер по защите информации в организации. Задачи и виды контроля эффективности защиты информации		2
	3.	Виды моделей угроз информации: путей физического проникновения злоумышленника к источнику и каналов утечки. Методические рекомендации по моделированию каналов утечки. Формы представления результатов моделирования. Рекомендации по оценке угроз безопасности информации		2
	Практические занятия, семинары		**124**	4
	1.	Классификация устройств защиты информации. Изучение типовых методов работы.	4	
	2.	Система защиты информации от несанкционированного доступа Страж NT 3.0. СЗИ СтронгДиск Про	4	
	3.	Изучение генераторов низкой/высокой частоты, импульсного генератора	6	
	4.	Организация охраны и защиты выделенного помещения	4	
	5.	Изучение виртуального цифрового осциллографа. Тестеры	6	
	6.	Защищенные соединения. Удаленное управление инженерно-техническими средствами	6	
	7.	Изучение и обнаружение закладных аудиоустройств. Подавители диктофонов, генераторы белого и речеобразного шума.	6	
	8.	Изучение и обнаружение закладных аудиоустройств. Дифференциальный адаптер проводных линий ДАПЛ	4	
	9.	Изучение радиолокаторов	8	
	10.	Съем и защита информации по электросети. Сетевые помехоподавляющие фильтры и генераторы	4	
	11.	Съем и защита информации по телефонной сети. Устройства защиты от прослушивания проводных телефонных линий. Устройства защиты от прослушивания сотовых телефонов.	4	
	12.	Съем и защита информации по телефонной сети. Блокираторы и подавители сигнала сети сотовых телефонов. ГШ-1000У (генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации)	4	
	13.	Съем и защита информации в вычислительной сети. Устройства защиты от утечки по каналам ПЭМИН. Устройства «зашумления» локальных компьютерных сетей.	4	
	14.	Съем и защита информации в вычислительной сети. Блокираторы Bluetooth и WiFi. Многофункциональный поисковый прибор ПИРАНЬЯ-Р	4	
	15.	Съем и защита информации по радиоканалу. Подавители радиомикрофонов и видеопередатчиков. Комплексные устройства защиты переговоров	4	
	16.	Применение комплекса радиоконтроля спектр МК	4	

	17.	Применение нелинейного радиолокатора NR-м	4	
	18.	Применение детектора поля ST-007 и Мозайка ПК+	4	
	19.	Охранная сигнализация на основе емкостного датчика	4	
	20.	Ультразвуковая охранно-пожарная сигнализация, основанная на эффекте Доплера	4	
	21.	Охранная сигнализация на основе датчиков разрушения стеклянных полотен	4	
	22.	Охранная сигнализация на основе пироэлектрического преобразователя	4	
	23.	Радиоразведка и противодействие в радиодиапазоне. Устройства виброакустической защиты переговоров.	4	
	24.	Сравнительный анализ скремблеров.	4	
	25.	Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу	4	
	26.	Обновление AVP	4	
	27.	Маскировка объектов наблюдения (на основе графических редакторов программного обеспечения ПЭВМ)	4	
	28.	Энергетическое скрытие речевой информации (с использованием звуковой карты и звукового редактора ПЭВМ)	4	
Самостоятельная работа при изучении раздела ПМ 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ и подготовка к их защите. Подготовка рефератов, устных сообщений и мультимедийных презентаций по индивидуальным темам.			**120**	
Примерная тематика внеаудиторной самостоятельной работы: Информация. История возникновения информационной безопасности Приборы наблюдения в оптическом диапазоне Устройства защиты информации Средства инженерной защиты источников информации Технологии удаленного сбора информации Факторы, влияющие на эффективность обнаружения и распознавания объектов наблюдения и основные характеристики средств наблюдения Способы и средства наблюдения. Средства перехвата сигнала Способы перехвата сигналов. Закладные устройства Проводные линии как канал утечки информации Способы и средства подслушивания акустических сигналов Каналы утечки информации Съем и защита информации Применение Спрут-мини-А, Гром, Шумомер Универсальный анализатор проводных коммуникаций ULAN				

Информационный портрет объекта защиты Радиоконтроль. Виброакустические средства Соната – ИПЗ. Видеоконтроль Способы и средства защиты информации на предприятии Генератор радиопомех Оптимизация проекта системы (предложений) защиты информации Организационные и технические меры по технической защите информации в организации				
Раздел ПМ 2. Технология использования программно-аппаратных средств защиты информации			**192**	
МДК 03.02. Программно-аппаратные средства защиты информации			**192**	
Тема 1.1 Методы и средства защиты информации в компьютерных системах и сетях	**Содержание учебного материала**		**18**	
	1	Способы несанкционированного доступа к информации и защиты от него в компьютерных системах.		2
	2	Способы идентификации и аутентификации субъектов компьютерных систем		4
	3	Аутентификация пользователей при локальном и удаленном доступе к компьютерным системам		4
	4	Дискреционное, мандатное и ролевое разграничение доступа к объектам компьютерных систем		2
	5	Аудит событий безопасности в компьютерных системах		2
	6	Методы и средства защиты информации в сети Интернет		4
Тема 1.2. Средства защиты информации в операционных системах	**Содержание учебного материала**		**18**	
	1	Архитектура подсистемы безопасности операционной системы Windows		2
	2	Разграничение прав пользователей операционной системы Windows		4
	3	Разграничение доступа к объектам в операционной системе Windows		2
	4	Аудит событий безопасности в операционной системе Windows		2
	5	Разграничение прав пользователей и доступа к файлам в операционных системах семейства Unix		2
	6	Аудит событий безопасности в операционных системах семейства Unix.		2
	7	Средства защиты информации в серверах AS/400		4
Тема 1.3. Программно-аппаратные средства криптографической защиты информации	**Содержание учебного материала**		**22**	
	1	Принципы построения и использования криптографического интерфейса приложений операционной системы Windows (CryptoAPI)		2
	2	Создание, хранение и распространение криптографических ключей с помощью CryptoAPI		2
	3	Использование CryptoAPI для шифрования и расшифрования данных		4
	4	Использование CryptoAPI для получения и проверки хеш-значений и электронной цифровой подписи		4
	5	Применение CryptoAPI в приложениях пакета Microsoft Office и шифрующей файловой системе Windows		4
	6	Аппаратные средства криптографической защиты данных		4
	7	Криптографические средства операционных систем		2
Тема 1.4. Методы и средства защиты от вредоносных программ и	**Содержание учебного материала**		**18**	
	1	Вредоносные программы и их классификация		6
	2	Методы обнаружения и удаления вредоносных программ		4

несанкционированного копирования информации	3	Принципы построения систем защиты от копирования		2
	4	Методы защиты от копирования инсталляционных дисков		2
	5	Методы настройки устанавливаемого программного обеспечения на характеристики компьютера		2
	6	Методы защиты программ от изучения		2
	Практические занятия, семинары		**86**	4
	1.	Криптографическая защита информации		
	2.	Меры противодействия несанкционированному доступу		
	3.	Идентификация и аутентификация пользователей		
	4.	Ограничение доступа на вход в систему. Разграничение доступа		
	5.	Регистрация событий (аудит).		
	6.	Система защиты корпоративной информации «Secret Disk»		
	7.	Создание защищенных логических дисков		
	8.	Работа с защищенными дисками		
	9.	Хранение секретной информации на съемных носителях		
	10.	Система защиты информации от несанкционированного доступа «Страж NT»		
	11.	Запуск и регистрация в системе защиты		
	12.	Создание пользователей		
	13.	Реализация мандатной модели разграничения доступа		
	14.	Реализация дискреционной модели разграничения доступа		
	15.	Создание замкнутой программной среды		
	16.	Контроль целостности		
	17.	Организация учета съемных носителей информации		
	18.	Регистрация событий		
	19.	Гарантированное удаление данных		
	20.	Средства организации виртуальных частных сетей		
	21.	Задачи, решаемые VPN. Туннелирование в VPN		
	22.	Уровни защищенных каналов. Защита данных на канальном уровне		
	23.	Организация VPN средствами протокола PPTP		
	24.	Установка и настройка VPN		
	25.	Анализ защищенности передаваемой информации		
	26.	Защита данных на сетевом уровне		
	27.	Использование протокола IPSec для защиты сетей		
	28.	Проверка защиты трафика		
	29.	Настройка политики межсетевого экранирования с использованием протокола		
	30.	Организация VPN средствами СЗИ StrongNet		
	31.	Установка защищенного соединения		
	32.	Защита на транспортном уровне		
	33.	Получение сертификатов открытых ключей		
	34.	Организация защищенного обмена электронной почтой		
	35.	Система защиты информации «Secret NET 7»		
	36.	Создание учетных записей пользователей		

	37.	Реализация дискреционной и мандатной модели разграничения доступа		
	38.	Режим замкнутой программной среды		
	39.	Контроль целостности		
	40.	Регистрация событий		
	41.	Печать штампа		
	42.	Гарантированное удаление данных		
	43.	Настройка механизма шифрования		
	Лабораторные работы		**30**	
	1	Установка операционной системы Windows на виртуальной машине		
	2	Работа с редактором реестра		
	3,4	Управление дисками из командной строки		
	5	Аудит в Windows. Просмотр журнала аудита		
	6	Работа с вредоносными программами		
	7	Принципы защиты файрволом типа 3+ (Kerio PF)		
	8	Принципы построения VPN сети (VipNet)		
	9,10	Принципы защиты отдельных сервисов с помощью туннелирования трафика (ZeBeDee)		
	11, 12	Принципы защиты программно-аппаратным комплексом SecretNet		
	13	Принципы защиты программно-аппаратным комплексом Dallas Lock		
	14,15	Освоение принципов документального оформления структуры и работы защищенных (Digital Security Office)		
Самостоятельная работа при изучении раздела ПМ 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Разбор вопросов по темам занятий. Работа с источниками и поиск информации в сети Интернет. Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите. Подготовка рефератов, устных сообщений и мультимедийных презентаций по индивидуальным темам.			96	
Примерная тематика внеаудиторной самостоятельной работы: Методы и средства ограничения доступа к компонентам ЭВМ Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания Защита программных средств от исследования Классификация средств исследования программ Защита программ от несанкционированного копирования Методы, затрудняющие считывание скопированной информации методы, препятствующие использованию скопированной информации Основные функции средств защиты от копирования Основные методы защиты от копирования Методы противодействия динамическим способам снятия защиты программ от копирования Характеристика и классификация компьютерных вирусов Характеристика средств нейтрализации компьютерных вирусов Полностью контролируемые компьютерные системы Основные элементы и средства защиты от несанкционированного доступа				

Системы защиты информации от несанкционированного доступа Аппаратно-программные средства криптографической защиты информации Комплекс «КРИПТОН-ЗАМОК» для ограничения доступа к компьютеру Система защиты данных CRYPTON SIGMA Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания Виды мероприятий по защите информации Современные системы защиты ПЭВМ от несанкционированного доступа к информации Уязвимость компьютерных систем Политика безопасности в компьютерных системах. Оценка защищенности Идентификация пользователей КС-субъектов доступа к данным Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей Протоколы идентификации с нулевой передачей знаний Схема идентификации Гиллоу-Куискуотера Средства и методы ограничения доступа к файлам Система разграничения доступа к информации в КС Концепция построения систем разграничения доступа Организация доступа к ресурсам КС, обеспечение целостности и доступности информации в КС		
УП 03.01 Учебная практика **Виды работ:** Участие в планировании и организации работ по обеспечению защиты объекта: Участие в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации Участие в разработке программ и методик организации защиты информации на объекте Осуществлять планирование и организацию выполнения мероприятий по защите информации Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности Ведение учета, обработки, хранения, передачи, использование различных носителей конфиденциальной информации Обеспечение техники безопасности при проведении организационно-технических мероприятий Участие в организации и проведении проверок объектов информатизации, подлежащих защите Контроль соблюдения персоналом требований режима защиты информации Участие в оценке качества защиты объекта Организация и технология работы с конфиденциальными документами: Участие в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации Участие в организации и обеспечение технологии ведения делопроизводства с учетом конфиденциальности информации Организация документооборота, в том числе электронного, с учетом конфиденциальности информации Организация архивного хранения конфиденциальных документов Оформление документации по оперативному управлению средствами защиты информации Учет работ и объектов, подлежащих защите Подготовка отчетной документации, связанной с эксплуатацией средств контроля и защиты информации Документирование хода и результатов служебного расследования Использование нормативных правовых актов, нормативно-методических документов по защите информации Применение программно-аппаратных и инженерно-технических средств защиты информации: Применение программно-аппаратных и технических средств защиты информации на защищаемых объектах Настройка систем защиты информации	216	

Участие в эксплуатации систем и средств защиты информации защищаемых объектов Выявление и анализ возможных угроз информационной безопасности объектов Проведение регламентные работ и фиксация отказов средств защиты Проведение регламентных работ по проверке систем защиты информации Подбор и применение программно-аппаратных и технических средства защиты информации		
ПП 03.01 Производственная практика (по профилю специальности) **Виды работ:** Знакомство с рабочим местом. Изучение компьютерного парка организации Инструктаж по общим вопросам, охраны труда и техники безопасности, по режиму работы предприятия. Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия Знакомство с конструкторско-технологическим обеспечением производства СВТ и аппаратно-программных систем Знакомство с эксплуатацией микропроцессорных систем Знакомство с обслуживанием и ремонтом периферийных устройств Знакомство с работой сети Internet Обеспечение информационной и компьютерной безопасности на предприятии Выполнение работ по обслуживанию информационных систем Типы компьютерных сетей предприятия Сетевые операционные системы. Принципы построения компьютерных сетей из компьютеров на базе операционной системы Windows Методы защиты средств вычислительной техники Использование защищенных компьютерных систем Определение и инструментарий новых информационных технологии Нормативные документы по установке, эксплуатации и охране труда при работе с персональным компьютером, периферийным оборудованием и компьютерной оргтехникой: охрана труда, правила внутреннего распорядка, трудовой кодекс, должностная инструкция, требования противопожарной безопасности. Критерии безопасности документооборота. Основные требования к защищенному документообороту. Защита информации, тайна, средства защиты информации. Аппаратные и программные средства для защиты компьютерных систем от НСД. Основные технологии построения защищенных информационных систем.	144	
Всего	**1112**	

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

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лабораторий «Технических методов и средств, технологии защиты информации», «Программно-аппаратных средств защиты информации» с достаточным количеством компьютеризированных рабочих мест (по одной единице для каждого обучающегося), с возможностью администрирования программно-аппаратных комплексов.

Оборудование лабораторий и рабочих мест:
- автоматизированное рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- маркерная доска;
- компьютеры (рабочие станции);
- принтер;
- сканер;
- средства физической защиты информации;
- объекты видеонаблюдения;
- USB-накопители;
- наушники;
- локальная сеть;
- мультимедийный класс;
- комплект учебно-методической документации;
- комплект нормативно-правовой документации;
- лицензионное программное обеспечение.

Технические средства обучения:
-рабочее место преподавателя, оснащенное компьютером с лицензионным программным обеспечением, мультимедиапроектором и электронной доской.
- обучающие видеофильмы, презентации.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Креопалов В.В., Технические средства и методы защиты информации: учебно-практическое пособие – М.: Изд.центр ЕАОИ, 2011.
2. Д.А. Скрипник, Общие вопросы технической защиты информации – М.: Национальный Открытый Университет «ИНТУИТ», 2016.
3. Пролетарский А.В., Смирнова Е.В., Суворов А.М., Технологии защиты информации в компьютерных сетях – М.: Национальный Открытый Университет «ИНТУИТ», 2016.

4. Башлы П.Н., Бабаш А.В., Баранова Е.К., Информационная безопасность и защита информации– М.: РИОР, 2013.
5. Савельев И.А. Программно-аппаратная защита информации: Учебное пособие / И.А. Савельев; Финуниверситет, Каф. информационной безопасности - М.: Финуниверситет, 2014.
6. Федеральный закон «Об информации, информационных технологиях и о защите информации». Собрание законодательства Российской Федерации 08.07.2006г.
7. Мельников В.П. Информационная безопасность. М.: Издательский центр «Академия», 2011.
8. Румынина Л.А. Документационное обеспечение управления. М.,ОИЦ «Академия». 2011.
9. Постановление Правительства РФ от 16 апреля 2012 года № 313 “Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)”.
10. Савельев И.А. Программно-аппаратная защита информации: Учебное пособие; Финуниверситет, Каф. информационной безопасности - М.: Финуниверситет, 2014.
11. Грибунин В.Г., Чудовский В.В.Комплексная система защиты информации на предприятии – Спб.: «Академия», 2013.
12. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Практикум. Учебное пособие, Изд.: КноРус, 2016.
13. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие / ЭБС ZNANIUM - Москва: Издательство " ИНФА-М ", 2021.

Дополнительные источники:

1. Царегородцев А.В. Системы контроля доступа: Учебное пособие/ВГНА Минфина России - М.: ВГНА Минфина России, 2008.
2. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2009.

3. Биометрические системы безопасности/Ю.И.Лебеденко. – Тула: Издательство ТулГУ, 2012.
4. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие, имеется гриф МО РФ, 2011.
5. Шаханова М.В. Современные технологии информационной безопасности: учебно-методический комплекс. – Москва: Проспект, 2015.
6. Галатенко В.А., Основы информационной безопасности – М.: Национальный Открытый Университет «ИНТУИТ», 2016.
7. Грибунин В.Г., Чудовский В.В., Комплексная система защиты информации на предприятии – Спб.: «Академия», 2010.

Периодические издания:

1 «CHIP»;
2 «JET INFO»;
3 «Грани безопасности»;
4 «Защита информации. Конфидент».

Интернет ресурсы:

1. Википедия – свободная энциклопедия – ru.wikipedia.org;
2. Издание о высоких технологиях – cnews.ru;
3. Российский сайт корпорации Microsoft – www.microsoft.com/rus
4. Каталог образовательных Интернет-ресурсов: учебно-методические пособия – edu/ru/modules.php
5. Электронный учебник по информатике и информационным технологиям – ctc.msiu.ru
6. Центр информационной безопасности - bezpeka.com
7. Дидактические и методические разработки по основам информатизации – studfiles.ru
8. Справочные материалы по техническим средствам информатизации – intuit.ru
9. Российская научная библиотека – rsl.ru

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля «Программно-аппаратные и технические средства защиты информации» является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля «Программно-аппаратные и технические средства защиты информации».

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю модуля «Программно-аппаратные и технические средства защиты информации» и специальности «Организация и технология защиты информации».

Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального учебного цикла. Преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

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

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.	- определение требований к программному модулю; - разработка спецификаций программных модулей; - сравнение полученных спецификаций с заданными требованиями;	Экспертная оценка защиты лабораторных работ. Экспертная оценка выполнения практических занятий. Компьютерное тестирование по МДК. Оценка выполнения самостоятельной работы. Экспертная оценка выполнения практического задания по учебной практике. Экзамен квалификационный по модулю.
Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.	- анализ спецификаций программного продукта; - выбор языка программирования для разработки программного модуля; - демонстрация навыков использования средств разработки программных модулей; - моделирование структуры программы;	
Проводить регламентные работы и фиксировать отказы средств защиты.	- выявление ошибок в программных модулях; - выбор медов отладки программных модулей; - выбор специализированных средств для отладки программного продукта; - демонстрация навыков использования программных средств для отладки программного продукта	
Выявлять и анализировать возможные угрозы информационной безопасности объектов.	- разработка тестовых наборов и тестовых сценариев; - демонстрация устранения ошибок в программных модулях; - демонстрация использования методов тестирования программного обеспечения; - демонстрация навыков внесения изменения в программные модули для обеспечения качества программного обеспечения;	

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	-участие в работе студенческих научных обществ; - выступления на научно-практических конференциях; - участие во внеурочной деятельности связанной с будущей профессией/специальностью (конкурсы профессионального мастерства, выставки и т.п.) - высокие показатели производственной деятельности	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: - на лабораторных работах и практических занятиях (при решении ситуационных задач, при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.); - при выполнении работ на различных этапах производственной практики; - при проведении контрольных работ, зачетов, экзаменов по МДК, экзамена (квалифицированного) по модулю.
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- анализ профессиональных ситуации; - решение стандартных и нестандартных профессиональных задач	
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	- эффективный поиск необходимой информации; - использование различных источников, включая электронные при изучении теоретического материала и прохождении различных этапов производственной практики	
Использовать информационно-коммуникационные технологии в профессиональной	- использование в учебной и профессиональной деятельности различных видов программного обеспечения, в том числе	

деятельности.	специального, при оформлении презентации всех видов работ	
Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	взаимодействие: - с обучающимися при проведении деловых игр, выполнении коллективных заданий (проектов), - с преподавателями, мастерами в ходе обучения, - с потребителями и коллегами в ходе производственной практики	
Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	- самоанализ и коррекция результатов собственной деятельности при выполнении коллективных заданий (проектов); - ответственность за результат выполнения заданий	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- планирование и качественное выполнение заданий для самостоятельной работы при изучении теоретического материала и прохождении различных этапов производственной практики; - определение этапов и содержания работы по реализации самообразования	
Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- адаптация к изменяющимся условиям профессиональной деятельности; - проявление профессиональной маневренности при прохождении различных этапов производственной практики	
Применять математический аппарат для решения профессиональных задач.	– демонстрация способности формулировать задачи логического характера и применять для их решения средства математической логики	
Оценивать значимость документов, применяемых в профессиональной	– определение состава документируемой конфиденциальной	

деятельности.	информации	
Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	– использование системы электронного документооборота	