НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДЕНО
ученым педагогическим советом
(протокол №06-22 от «22» июня 2022 г.)
Председатель педагогического совета
Директор _____ Л.Н. Цой

Рабочая программа профессионального модуля

ПМ.03 Защита информации техническими средствами

ППССЗ по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Объем дисциплины – 564 часа.

Якутск, 2022

Рабочая программа профессионального модуля разработана на основе Рабочая программа учебной дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**.** Укрупненная группа специальностей 10.00.00 Информационная безопасность.

Разработчики рабочей программы:	НПОУ «ЯКИТ»	Преподаватель	О.В. Крымова М.И. Нерлов
	(место работы)	(должность)	(инициалы, фамилия)

Обсуждено на заседании отделения «17» июня 2022 г. протокол №9/3

Председатель отделения — Зав. отделения — И.В. Пронин

Рассмотрено на заседании методического совета «20» июня 2022 г. протокол №5

Председатель МС — Заместитель директора по учебно-методической работе — «20» июня 2022 г.

Заместитель директора по учебно-методической работе — С.И. Томская — «20» июня 2022 г.

№ п/п	Прилагаемый к Рабочей программе документ, содержащий текст обновления	Решение отделения		Подпись заведующего отделения	Фамилия И.О. заведующего отделения
		дата	Протокол №		
1.	Приложение № 1				
2.	Приложение № 2				
3.	Приложение № 3				
4.	Приложение № 4				
5.	Приложение № 5				

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности (ВПД): Защита информации техническими средствами.

1.2. Место профессионального в структуре образовательной программы:

ПМ.03 «Защита информации техническими средствами» входит в профессиональный цикл, в профессиональные модули

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

В результате освоения профессионального модуля обучающийся должен иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
- установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

В результате освоения профессионального модуля обучающийся должен уметь:

- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации;
- применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять инженерно-технические средства физической защиты объектов информатизации

В результате освоения профессионального модуля обучающийся должен знать:

- порядок технического обслуживания технических средств защиты информации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;
- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики технических средств физической защиты;
- основные способы физической защиты объектов информатизации;
- номенклатуру применяемых средств физической защиты объектов информатизации.

Профессиональные (ПК) и общие (ОК) компетенции, которые актуализируются при изучении профессионального модуля:

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

1.4. Количество часов на освоение программы профессионального модуля:

Всего 564 часов, из них:

максимальной учебной нагрузки обучающегося (всего) – 564 часов;

обязательной аудиторной учебной нагрузки обучающегося (всего) – 382 часов;

самостоятельная работа обучающегося (всего) – 68 часов;

лабораторные занятия обучающегося (всего) – 234 часа;

учебной практики обучающегося (всего) – 36 часов;

производственная практика (по профилю специальности) – 72 часов;

промежуточная аттестация обучающегося (всего) – 6 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект),часов			
ОК.01 – ОК.10 ПК 3.1- ПК.3.5	Раздел 1 модуля. Техническая защита информации	212	170	108	-	18		42
ОК.01 – ОК.10 ПК 3.1- ПК.3.5	Раздел 2 модуля. Инженерно-технические средства физической защиты объектов информатизации	238	212	126	+	18		26
Учебная практика						36		
Производственная практика, часов							72	
Экзамен по профессиональному модулю		6						
ВСЕГО:		564	382	234		36	72	68

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	1,2
МДК.03.01 Техническая защита информации		212	1,2
Раздел 1. Концепция инженерно-технической защиты информации			1,2
Тема 1.1. Предмет и задачи технической защиты информации	Содержание	4	1,2
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации.		1,2
	Тематика лабораторных работ	7	1,2
	Основные параметры системы защиты информации.		1,2
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание	3	1,2
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации..		1,2
	Тематика лабораторных работ Классификация способов и средств защиты информации	6	1,2
Раздел 2. Теоретические основы инженерно-технической защиты информации			1,2
Тема 2.1. Информация как предмет защиты	Содержание	3	1,2
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.		1,2
	Тематика лабораторных работ	6	1,2
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		1,2

Тема 2.2. Технические каналы утечки информации	Содержание	3	1,2
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		1,2
	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Тема 2.3. Методы и средства технической разведки	Содержание	4	1,2
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.		1,2
	Тематика лабораторных работ	6	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Раздел 3. Физические основы технической защиты информации			1,2
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	3	1,2
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей		1,2
	Тематика лабораторных работ	7	1,2
	Измерение параметров физических полей		1,2
Тема 3.2. Физические процессы при подавлении опасных	Содержание	4	1,2
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		1,2

сигналов	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Раздел 4. Системы защиты от утечки информации			1,2
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание	4	1,2
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.		1,2
	Тематика лабораторных работ	7	1,2
	Защита от утечки по акустическому каналу		1,2
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание	4	1,2
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		1,2
	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Промежуточная аттестация по МДК.03.01			1,2
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание	4	1,2
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.		1,2
	Тематика лабораторных работ	6	1,2
	Защита от утечки по виброакустическому каналу		1,2
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание	4	1,2
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура		1,2

	применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Тематика лабораторных работ	7	1,2
	Определение каналов утечки ПЭМИН		1,2
	Защита от утечки по цепям электропитания и заземления		1,2
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание	4	1,2
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.		1,2
	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание	4	1,2
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		1,2
	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание	4	1,2
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		1,2
	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Раздел 5. Применение и эксплуатация технических средств защиты информации			1,2
Тема 5.1. Применение технических средств	Содержание	4	1,2
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты		1,2

защиты информации	информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Тема 5.2. Эксплуатация технических средств защиты информации	Содержание	4	1,2
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.		1,2
	Тематика лабораторных работ	7	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Примерные виды самостоятельной работы при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		42	1,2
Учебная практика Виды работ: Измерение параметров физических полей. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации.		18	1,2
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		238	1,2

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты			1,2
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание	9	1,2
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.		1,2
	Тематика лабораторных работ	14	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	10	1,2
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.		1,2
	Тематика лабораторных работ	14	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты			1,2
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание	10	1,2
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.		1,2
	Тематика лабораторных работ	14	1,2
	Монтаж датчиков пожарной и охранной сигнализации		1,2
Тема 2.2. Система контроля и управления доступом	Содержание	12	1,2
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация		1,2

	средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.		
	Тематика лабораторных работ	14	1,2
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя		1,2
	Рассмотрение принципов устройства, работы и применения средств контроля доступа		1,2
Тема 2.3. Система телевизионного наблюдения	Содержание	9	1,2
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.		1,2
	Тематика лабораторных работ	14	1,2
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		1,2
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание	9	1,2
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.		1,2
	Тематика лабораторных работ	14	1,2
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		1,2
Тема 2.5 Система воздействия	Содержание	9	1,2
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.		1,2
	Тематика лабораторных работ	14	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты			1,2
Тема 3.1 Применение инженерно-технических средств	Содержание	9	1,2
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом.		1,2

физической защиты	Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.		
	Тематика лабораторных работ	14	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Содержание	9	1,2
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.		1,2
	Тематика лабораторных работ	14	1,2
	Тематика учебных занятий формируется образовательной организацией самостоятельно		1,2
Примерные виды самостоятельной работы при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования …		26	1,2
Учебная практика по разделу 2 модуля Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления.		18	1,2

Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по инженерно-технической защите информации.		
Производственная практика профессионального модуля Виды работ Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	72	1,2
Экзамен по профессиональному модулю	6	1,2
Всего	564	1,2

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета:

- автоматизированные рабочие места обучающихся;
- компьютеры, объединенные в локальную вычислительную сеть;
- проектор;
- экран;
- акустическая система;
- учебно-наглядные пособия:
- схемы;
- таблицы;
- учебные презентации.
- Раздаточный дидактический материал: учебные карточки с заданиями; дидактический материал для выполнения практических работ.

Технические средства обучения:

- компьютеры, объединенные в локальную вычислительную сеть;
- мультимедиа проектор;
- интерактивная доска.
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности в виде: ПАК Соболь (имеется в наличии) – 1шт.

Учебно-методические материалы и образы виртуальных машин для развертывания учебных стендов по следующим темам: "Защита серверов и рабочих станций" (Основы применения системы защиты Secret Net Studio, Secret Net LSP и ПАК "Соболь") – от 16 до 32 академических часов; "Защита сетевого периметра" (Основы применения АПКШ "Континент" версий 3.9, 4 для организации сетевой защиты) – от 16 до 32 академических часов; "Организация доступа удаленных пользователей к веб-ресурсам защищаемой корпоративной сети по протоколу TLS" (Основы применения СКЗИ "Континент TLS" для организации удаленного доступа) – от 8 до 16 академических часов; "Защита средств

виртуализации" (Основы применения vGate для защиты виртуальных инфраструктур) – 8–12 академических часов

Оснащение лаборатории Информационных технологий, программирования и баз данных:

- рабочие места на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»;
- Дистрибутивы программного комплекса Vipnet;
- Дистрибутивы программного комплекса InfoWatch TrafficMonitor
- Дистрибутивы Linux операционных систем;
- Дистрибутивы антивирусных программных комплексов;
- Академическая подписка Office 365 A1 для преподавателей и студентов;
- программное обеспечение: дистрибутивы операционных систем; правочная правовая система «Гарант»; ПО Oracle VirtualBox; антивирусная программа;
- Прикладное программное обеспечение, в том числе: Академическая подписка Office 365 A1 для преподавателей и студентов;

Бесплатное ПО: LibreOffice - офисный пакет с открытым исходным кодом, являющийся ответвлением от проекта OpenOffice.org и претендующий на роль бесплатной альтернативы пакету офисных приложений Microsoft Office. В состав программы входят текстовый редактор Writer, табличный процессор Calc, мастер презентаций Impress, векторный графический редактор Draw, редактор формул Math и модуль управления базами данных Base; GIMP - свободно распространяемый растровый графический редактор, программа для создания и обработки растровой графики и частичной поддержкой работы с векторной графикой (Аналог Adobe Photoshop); Inkscape - Свободно распространяемый векторный графический редактор, удобен для создания как художественных, так и технических иллюстраций. (аналог Adobe Illustrator, Corel Draw и MicrosoftVisio)

- специализированное программное обеспечение: EclipseIDEforJavaEEDevelopers, .NETFrameworkJDK 8, MicrosoftSQLServerExpressEdition, MicrosoftVisioProfessional, MicrosoftVisualStudio Community, SQLServerManagementStudio, MicrosoftSQLServerJavaConnector, AndroidStudio, Cisco Packet Tracer (на правах сетевой академии Cisco), Oracle VirtualBox, Пакет All Products Pack IDE от JetBrains (Академическая лицензия).
- программные и программно-аппаратные средства обнаружения вторжений (Secret Net Studio);

− средства уничтожения остаточной информации в запоминающих устройствах: ПО низкоуровневого форматирования информации;

− Установочные комплекты Secret Net Studio, Secret Net LSP и vGate с набором учебных лицензий на 3 года бесплатно для развертывания в учебном классе;

Выход в электронно-информационную образовательную среду колледжа (порядок доступа к элементам ЭИОС и отдельным информационным базам и системам): https://moodle.yakit.ru

3.2. Информационное обеспечение обучения

Основные источники:

1. 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, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/497433U

2. 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, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: 8TUhttps://urait.ru/bcode/495525U8T

3. 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, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: 8TUhttps://urait.ru/bcode/497433U8T

4. Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: 8TUhttps://urait.ru/bcode/494562U8T

5. 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, 2022. — 161 с. — (Профессиональное

образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: 8TUhttps://urait.ru/bcode/495525U8T

Дополнительные источники:

1. 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, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
Умения:	
– применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации.	Лабораторные занятия, домашняя работа, тестирование
Знания:	
– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.	Домашняя работа, тестирование