

**АВТНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»**

УТВЕРЖДАЮ
ДИРЕКТОР АНО ПО «БИТ»

В.В. СЕРГЕЕВ

«_____» _____ 20____ ГОДА
М.П.

**ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА
МДК.03.02 Инженерно-технические средства физической защиты
объектов информации**

Калининград
2022г.

Программа учебной дисциплины МДК.03.02 «Инженерно-технические средства физической защиты объектов информации» разработана на основе Федерального государственного образовательного стандарта (далее — ФГОС) по специальностям среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1553 и примерной основной образовательной программы СПО, разработанной ФУМО 2017 г.

Организация-разработчик: АУТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

Разработчик: _____

Михальков Алексей Николаевич,
преподаватель БИТ.

Рассмотрена
методической комиссией,
протокол № _____
от «___» _____ 2022 г.
председатель
_____ Т.В. Славинская

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ 4
УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ 9
ДИСЦИПЛИНЫ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 19**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ 21
УЧЕБНОЙ ДИСЦИПЛИНЫ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «МДК-03-02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

1.1. Место дисциплины в структуре основной профессиональной образовательной программы.

Программа междисциплинарного курса «МДК.03.02. Инженерно-технические средства защиты объектов информатизации» профессионального модуля «ПМ.03» является обязательной частью профессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

В результате изучения МДК студент должен освоить основной вид деятельности **ВД 3, Защита информации техническими средствами**, соответствующие ему общие и профессиональные компетенции.

Программой междисциплинарного курса «МДК.03.02. Инженерно-технические средства защиты объектов информатизации», наряду с другими дисциплинами обеспечивает формирование следующих общих и профессиональных компетенций.

1.1.1 Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
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.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере

1. 1.2. профессиональные компетенции

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации техническими средствами
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.

Общие требования к личностным результатам выпускников СПО

Личностные результаты реализации программы воспитания (дескрипторы)	Код личностных результатов реализации программы воспитания
Портрет выпускника СПО	
Осознающий себя гражданином и защитником великой страны.	ЛР 1
Готовый использовать свой личный и профессиональный потенциал для защиты национальных интересов России.	ЛР 2
Демонстрирующий приверженность к родной культуре,	ЛР 3

исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.	
Принимающий семейные ценности своего народа, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания.	ЛР 4
Занимающий активную гражданскую позицию избирателя, волонтера, общественного деятеля.	ЛР 5
Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение.	ЛР 6
Готовый соответствовать ожиданиям работодателей: проектно мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость.	ЛР 7
Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы; управляющий собственным профессиональным развитием; рефлексивно оценивающий собственный жизненный опыт, критерии личной успешности.	ЛР 8
Уважающий этнокультурные, религиозные права человека, в том числе с особенностями развития; ценящий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности».	ЛР 9
Принимающий активное участие в социально значимых мероприятиях, соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России; готовый оказать поддержку нуждающимся.	ЛР 10
Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением.	ЛР 11
Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.	ЛР 12

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none">– 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.
уметь	<ul style="list-style-type: none">– 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

<p>знать</p>	<ul style="list-style-type: none"> – 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.
--------------	--

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
--------------------	---------------

Обязательная учебная нагрузка	174
в том числе:	
теоретическое обучение	44
практические занятия	100
самостоятельная работа	18
Курсовая работа	6
Экзамен.	12

2.2. Тематический план и содержание междисциплинарного курса «МДК. 03.02. Инженерно-технические средства физической защиты объектов. информатизации».

Наименование разделов и тем профессионального модуля (ПМ).	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа.	Объем в часах	Уровень освоения	Осваиваемые компетенции
1	2	3	4	5
Раздел 1. Общие положения.		54		
Введение. Модель нарушителя.	Содержание учебного материала	4		
	Виды, источники и устройства физической защиты объектов информатизации. Структура дисциплины, ее роль и место в системе профессиональной подготовки.	4	1	ОК 01 ОК 03 ЛР 01-12
Тема 1.1. Цели и задачи инженерно-технических средств физической защиты объектов информатизации.	Содержание учебного материала.	18		
	Понятие об информации и объектах информатизации. Физические свойства и характеристики информационных сигналов.	2	1	ОК 01
	Нормативно-правовая база защиты объектов информатизации. Роль и место правового обеспечения физической защиты объектов информатизации.	2	1	ОК 02
	Жизненный цикл системы инженерно-технических средств физической защиты. Основные методы внедрения инженерно-технических средств по объектам информатизации.	2	1	ОК 04 ПК 1.1
	Основные этапы и маршруты проникновения к объектам информатизации. Групповые и одиночные маршруты проникновения на объекты.	2	1	ПК 2.1
Требования к инженерно-техническим средствам физической защиты	2	2	ПК 3.3	

	объектов информатизации по обеспечению информационной безопасности предприятия.			ПК 5,3 ЛР 01-12
	Практические занятия:	4		
	ПР-1. Прогноз маршрута проникновения на объект информатизации.	2	1	
	ПР-2. Контроль инженерно-технических средств по основным показателям защиты объекта.	2	1	
	Лабораторная работа.	4		ОК 01 ОК 03
	ЛР-1. Расчет параметров информационной безопасности объекта.	2	2	
	ЛР-2. Специальная проверка технических средств на возможность противодействия проникновению на объект информатизации.	2	1	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты объектов информатизации.	Содержание учебного материала	10		
	Основные понятия и определения. Классификация комплексов инженерно-технических средств. Основные параметры по информационной безопасности на объектах.	2	1	ОК 01
	Принцип построения интегрированных систем охраны информации на объектах.	2	1	ОК 02
	Общая характеристика методов хищения информации, копирования, уничтожения, искажения, подавления информации. Утечка информации по каналам ПЭМИН.	2	2	ОК 04 ЛР 01-12
	Лабораторные работы:	4		
	ЛР-3. Исследование акустических каналов хищения информации.	2	2	
	ЛР-4. Исследование технических средств на возможность утечки информации.	2	1	
Тема 1.3. Инженерные конструкции для	Содержание учебного материала	22		
	Классификация методов технической разведки. Способы ведения разведки на объектах информатизации.	2	1	ОК 04

предотвращения проникновения злоумышленника к источникам информации.	Обрывные сигнализационные устройства. Система «ТРЕПАНГ».	2	2	ПК 1.1. ПК 2.1 ПК 3.3 ПК 5.3 ЛР 01-12
	Пассивные и активные инфракрасные системы «ФОН» контроля движения.	2	2	
	Кабельные охранные системы территорий объекта. Система «КВАНТ».	2	2	
	Периметральные оптоволоконные кабельные системы физической защиты. Оптоволоконная система «ВОРОН».	2	2	
	Вибрационные кабельные системы для защиты сетчатых ограждений объекта. Система «ДЕЛЬФИН».	2	2	
	Радиотехнические системы сигнализации открытых территорий охраняемых объектов. Система «ВИАДУК», «МВС-22».	2	2	
	Практические занятия:	2		
	ПР-3. Анализ параметров пассивной ИК-системы контроля движения на объекте.	2	1	
	Лабораторные работы:	6		
	ЛР-5. Исследование спектра акустического речевого сигнала.	2	2	
ЛР-6. Исследование инфракрасного сигнала излучения на объекте информатизации.	2	2		
ЛР-7. Измерение уровня внешнего электро-магнитного излучения объекта информации.	2	1	ОК 01 ОК 03 ЛР 01-12	
Промежуточная аттестация по учебной дисциплине.				
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты.		78		
Тема 2.1. Система контроля и управления доступом на	Содержание учебного материала	16		
	Структура, классификация, принцип построения и характеристики комплекса СКУД. Электронные варианты системы СКУД.	2	1	ОК 01
	Интегрированная система контроля и управления доступом на объект	4	1	ОК 02

объекты информатизации.	информатизации. Система АРМ с биометрическим контроллером KF-100FC.			ОК 04 ЛР 01-12
	Акустические, ультразвуковые, оптические, фотоэлектрические охранные извещатели в интегрированной системе контроля и управления допуском.	6	1	
	Лабораторные работы:	4		
	ЛР-8. Исследование уровня защиты информации от побочного электромагнитного навязывания.	2	1	ОК 02
	ЛР-9. Измерение степени блокировки автоматизированного рабочего места при попытке проникновения к источнику информации.	2	1	ОК 04 ЛР 01-12
Тема 2.2. Система обнаружения проникновения на объект информатизации.	Содержание учебного материала	30		
	Система охранно-тревожной сигнализации «Астра».	2	1	ОК 01
	Система пожарной сигнализации «Гранит».	2	1	
	Телевизионные системы удаленного наблюдения «NoVuS»..	2	2	ОК 02
	Сейсмоакустическая охранная система «PSICON».	2	2	ОК 04 ПК 3.3 ЛР 01-12
	Периметральная охранная система «GUARDWIRE».	2	2	
	Радиоволновое устройство «ГАРУС» для обнаружения вторжения на объект.	2	2	
	Радиолучевая микроволновая техническая система «КРОКУС» для обнаружения перемещения на объекте информатизации.	2	2	
	Практические занятия:	10		
	ПР-4. Размещение датчиков охранно-пожарной системы сигнализации на объекте.	2	2	
	ПР-5. Определение уровня электромагнитного излучения детектором «D-008»	2	2	
	ПР-6. Поиск радио закладного устройства всеволновым радиоприемником «SONY FC-15K»	2	1	
ПР-7. Определение величины «мертвой зоны» датчик видео	2			

	наблюдения «ADEMCO»/			
	ЛР-8. Определение уровня сейсмоакустической среды служебного помещения.	2	1	
	Лабораторные работы:	6		
	ЛР-10. Исследование радиоволнового сигнала при вторжении на объект «МВС-22».	2	1	ОК 02
	ЛР-11. Исследование параметров радиотехнического извещателя «Acorus security».	2	1	ОК 04
	ЛР-12. Измерение уровня инфракрасного излучения активного извещателя по варианту блокировки объекта информатизации.	2	1	ЛР 01-12
Тема 2.3. Система удаленного видеонаблюдения.	Содержание учебного материала.	8		
	Телевизионные датчики и теле охранные системы. Промышленные телевизионные установки контроля и охраны объекта информатизации.	2	1	ОК 02
	Технические характеристики видеокамер охранного назначения. Наименования, классификация, форм-фактор камер охранного назначения.	2	2	ОК 04 ПК 3.3
	Встроенная функциональность камер охранного назначения. Механический ИК-фильтр, электронная функция «день / ночь», детекция движения, динамический диапазон.	2	2	ПК 5.3 ЛР 01-12
	Интеллектуальные функции анализа видеоизображения (VCA) системы «SAMSUNG-SAV» . Слежение за объектом, появление / исчезновение объекта, пересечение линии, автопатрулирование, коррекция аберраций.	2	2	
Тема 2.4. Система сбора, обработки, отображения и документирования	Содержание учебного материала	8		
	Система «HELK» - интегрированная система сбора, обработки, отображения и документирования информации на объекте.	4	2	ПК 3.3
	Оптико-электронная система сбора и обработки информации	2	2	ЛР 01-12

информации.	«NOVUS». Стандарт документирования информации.			
	Лабораторные работы:	2		
	ЛР-13. Функциональное исследование цифровой видеокамеры охранного видео наблюдения в режиме «День - ночь».	2	2	ОК 02
Тема 2.5. Система воздействия.	Содержание учебного материала.	16		
	Высокочастотное навязывание в канале конфиденциальной информации на средство несанкционированного доступа в автоматизированных системах.	2	2	ОК 04
	Инфракрасное воздействие на средства перехвата на объекте информатизации в диапазоне оптического спектра.	2	2	ПК 1.1.
	Демаскирующее воздействие в оптическом диапазоне электромагнитного спектра.	2	1	ПК 2.1
	Противодействие методам скрытого видеонаблюдения и фотосъемки.	2	1	ПК 3.3
	Лабораторные работы:	4		
	ЛР-14. Определение частоты и типа модуляции для подавления несанкционированного радиоприема информации.	2	2	ПК 5.3 ЛР 01-12
	ЛР-15. Исследование демаскирующих параметров на объекте в инфракрасном диапазоне электромагнитных волн.	2	1	
	Практические работы:	4		
	ПР-9. Применение метода акустического воздействия на технические средства акустического перехвата информации.	2	1	ПК 3.3 ЛР 01-12
ПР-10. Применение метода высокочастотного воздействия на технические средства перехвата информации по радио каналу..	2	1	ПК 3.3 ЛР 01-12	
Раздел 3. Проектирование и эксплуатация инженерно-технических средств физической защиты.		34		
	Содержание учебного материала.	10		
Тема 3.1. Управление	Система управления от утечки информации по акустическому каналу. Система регистрации речи «TEL-32». Область применения,	3	1	ОК 04

системой ИТС физической защиты.	технические характеристики, настройка.			ПК 1.1. ПК 2.1 ПК 3.3 ПК 5.3 ЛР 01-12
	Система управления средствами мультиплексирования и скремблирования речевой информации в телефонных каналах электросвязи. Четырех канальный прибор защиты телефонной линии «SI-2010». Прецизионный виброакустический генератор «SPP-14».	3	1	
	Практические работы:	4		
	ПР-11. Применение типового метода измерения прямого акустоэлектрического преобразования в реальных условиях.	2		
	ПР-12.. Осуществление технического контроля по эффективности мер защиты информации.	2		
Тема 3.2. Эксплуатация комплекса инженерно-технических средств физической защиты.	Содержание учебного материала.	22		
	Этапы проведения работ по обеспечению надежности инженерно-технических средств. Основные операции проведения технического обслуживания инженерно-технических средств. Процедура тест-прогона, анализ результатов, дефектовка, текущий ремонт.	6	1	
	Лабораторные работы:	6		
	ЛР-16. Определение номинальных параметров датчика перемещения охранной сигнализации на объекте информатизации.	2	1	
	ЛР-17. Инструментальный расчет защищенности служебного помещения от утечки речевой конфиденциальной информации средствами PRD-130F.	2	1	
	ЛР-18. Скремблирование информации комплексом «LAB-2000».	2	2	
	Практические занятия:	10		
	ПР-13. Измерение отношений «сигнал/шум» в контрольных точках выделенных помещений на объектах информации.	2	2	
	ПР-14. Оценка эффективности мер защиты информации по электромагнитному излучению.	2	1	
	ПР-15. Испытание пожарного извещателя системы сигнализации	2	2	

	«Астра» по уровню инерции, дифференциалу и порогу срабатывания.			
	ПР-16. Испытание учебной аудитории на защищенность помещения от утечки акустической речевой информации. Определение степени звукоизоляции.	2	2	
	ПР-17. Исследование компьютерного класса на утечку информации по электрическому каналу ПЭМИН.	2	1	
Раздел 4. Курсовой проект.		30		
Тематика курсовых работ	Содержание учебного материала.			
	Расчет основных показателей качества системы охранно-пожарной сигнализации «Рубеж-2М» объекта информатизации.			
	Вариант структуры построения системы сбора и обработки информации на объекте информатизации.			
	Проект системы контроля и управления доступом служебного офиса.			
	Разработка требований по защите информации от несанкционированного доступа к информации.			
	Разработка требований к инженерно-техническим средствам для физической защиты автоматизированных рабочих мест на объекте.			
	Вариант развертывания радиолучевой системы обнаружения вторжения «Гарус» на слабопересеченной местности.			
Самостоятельная работа обучающихся.	Тематика самостоятельных работ.	12		
	Основные операции технического обслуживания средств технической защиты информации. Расконсервация оборудования. Развертывание в помещении или на местности. Укомплектование системы датчиками и приборами питания. Предварительная настройка и прогон функциональных возможностей. Профилактика, диагностика неисправностей, текущий ремонт.	3		
	Система контроля и управления допуском (СКУД). Принципы построения системы. Порядок допуска сотрудников и клиентов на	3		

	охраняемые объекты. Планы размещения и маршруты следования.		
	Пожарная тактика и охранная тактика применения приборов охранно-пожарной сигнализации и управления серии «Гранит». Указания мер безопасности. Схемы внешних и внутренних соединений. Порядок установки. Проверка технического состояния. Подготовка к работе.	3	
	Схема размещения периметральных средств на местности. Примеры охраны открытых территорий. Рекомендации по рельефу местности и погодным условиям. Особенности применения радиоволновых технических средств защиты объекта. Радиолучевая система обнаружения. Вибрационная кабельная система.	3	
Экзамен по программе дисциплинарного курса		12	
Самостоятельные работы		18	
Всего:		174	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

- кабинет «Основы теории защиты и передачи информации», оснащенный для реализации программы учебной дисциплины специфическим оборудованием;

- кабинет «Технические средства защиты информации».

3.2. Оборудование кабинетов должно иметь следующие приборы технической защиты информации и средства измерения:

* 5 - 7 компьютеров обучающихся с архитектурой физического уровня и 1 компьютер преподавателя. Аппаратное обеспечение: одна сетевая плата, процессор не ниже Core-i3, оперативная память объемом не менее 2 Гб; HD 500 Gb, программное обеспечение: операционные системы Windows, пакет офисных программ.

* Аппаратно-программный комплекс «Lab-2000», обеспечивающий функции аппаратуры передачи данных, генерации аналоговых сигналов, генерации цифровых сигналов, спектрографа, осциллографа, маскиратора, коммутатора, репитера.

* Генераторы низкой частоты, генераторы стандартных сигналов (ГСС), генераторы высокой частоты, шумогенератор, сейсмоакустический генератор, осциллограф, спектрограф, индикаторы электромагнитного излучения, частотомеры, сканирующие приемные устройства, нелинейный локализатор на 2-ю гармонику,

* Учебный стенд телевизионной системы охранного видеонаблюдения.

* Учебный макет системы контроля и управления доступом.

* Специфическая измерительная аппаратура регистрации побочного электромагнитного излучения и наводок (ПЭМИН).

* Средства охранно-тревожной и пожарной сигнализации.

* Учебный комплект звуковых, ультразвуковых, инфракрасных, пьезоэлектрических и оптических извещателей технических средств воздействия.

* Типовой состав соединительных проводов и кабелей для монтажа и наладки сети охранно-тревожной и пожарной сигнализации.

* Комплекс измерительной аппаратуры для определения соотношения «сигнал / шум», волнового сопротивления, коэффициента затухания, сопротивления линий связи.

* Аппаратура радиоволновой охранной системы защиты территорий.

* Измерительная аппаратура для проведения аттестации объектов информатизации по требованиям безопасности информации.

* Пример проектной документации.

* Необходимое лицензионное программное обеспечение для обеспечения безопасности информации.

* Технические средства обучения:

** компьютеры с лицензионным программным обеспечением для обеспечения курсовых работ по учебной дисциплине;

** интерактивная доска, проектор.

3.2. Информационное обеспечение обучения.

3.2.1. Основные источники.

1. Зайцев А.П. Инженерно-технические средства и методы защиты информации. Учебник. М. «Горячая линия – Телеком». 2017.

3. Рогозин Ю.Н. Инженерно-техническая защита информации Лабораторный практикум. М. Издательство МГИУ. 2017.

4. Хореев А.А. Способы и средства защиты информации. Учебное пособие. 3-е издание. МО РФ. 2017.

3.2.2. Дополнительные печатные источники.

1. Садердинов.А.А. Информационная безопасность предприятия. Учебное пособие. 3-е издание. М, корпорация «Дашков и К°». , 2017.

2. Гедсберг Ю.М. Охранное телевидение. М. Горячая линия – Телеком. 2017.

3. Соболев А.Н. Физические основы технических средств обеспечения информационной безопасности. Учебное пособие. М. «Гелиос АРВ». 2017.

4. Краковский Ю.М. Информационная безопасность и защита информации. Учебный курс. М. Издательский центр «МарТ», 3-е издание. 2016.

5. Каторин Ю.Ф. Энциклопедия промышленного шпионажа. Санкт-Петербург, «ПОЛИГОН», 2016.

6. Научно-производственный центр «НЕЛК». Инженерно-технические системы защиты информации. Каталог – 2016. М. издательская фирма «НЕЛК».

3.2.3. Дополнительные электронные источники.

1. ЭБС – ipr.books. Доступ к электронной библиотечной системе для сотрудников техникума и студентов осуществляется при помощи авторизации бесплатно.

DVD. Mary Lynn Garcia. The design and evaluation physical protection systems. М. Гарсиа. Проектирование систем физической защиты.

CD. Монтаж и настройка систем охранной и пожарной сигнализации. Изготовитель М. «СФТ».

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ.

Результаты обучения	Критерии оценки	Формы и методы оценки
<p>Знания:</p> <ul style="list-style-type: none"> - элементной базы, компонентов и принципы работы типовых устройств физической защиты объектов; - элементной базы, принципа работы типовых извещателей; - требований к монтажу и правила эксплуатации систем видеонаблюдения и охранно-пожарной сигнализации; - основных сведений о методах измерении специальных электрических величин; - принципа действия звуковых радиоволновых, оптических, инфракрасных извещателей. 	<p>Демонстрация знаний принципов работы типовых инженерно-технических средств физической защиты объектов информатизации, а также принципа действия основных типов датчиков перемещения и излучения.</p>	<p>Оценка знаний в ходе тестирования, тест-опросов, проведения практических и лабораторных работ.</p>
<p>Умения:</p> <ul style="list-style-type: none"> - читать монтажные, сборочные, электрические схемы типовых инженерно-технических устройств защиты объектов информатизации; - выполнять проект развертывания систем и комплексов средств регистрации проникновения на объект; - производить расчет параметров безопасности объектов информатизации; 	<p>Умение проводить расчеты типовых параметров систем и устройств физической защиты объектов информатизации. Умение самостоятельно проводить измерения специальных параметров по аттестации объектов информации на требования безопасности</p>	<p>Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий и лабораторных работ, экзамен.</p>

<ul style="list-style-type: none"> - выполнять подбор типовых первичных датчиков для систем защиты объектов; - проводить анализ работы средств защиты объектов; - проводить измерения по контролю утечки информации. 	<p>информации.</p>	
---	--------------------	--

Личностные результаты обучающихся фиксируются через сформированность личностных универсальных учебных действий, определяемую по трём основным блокам:

- сформированность основ гражданской идентичности личности;
- готовность к переходу к самообразованию на основе учебно-познавательной мотивации, в том числе готовность к выбранному направлению профильного образования;
- сформированность социальных компетенций, включая ценностно-смысловые установки и моральные нормы, опыт социальных и межличностных отношений, правосознание.

В соответствии с требованиями Стандарта достижение личностных результатов не выносится на итоговую оценку обучающихся, а является предметом оценки эффективности воспитательно-образовательной деятельности техникума. Оценка этих достижений проводится в форме, не представляющей угрозы личности, психологической безопасности и эмоциональному статусу учащегося, и может использоваться исключительно в целях оптимизации личностного развития обучающихся.

Комплексная характеристика общих, профессиональных, личностных результатов составляется на основе Портфолио ученика. Цель Портфолио - собрать, систематизировать и зафиксировать результаты развития ученика, его усилия и достижения в различных областях, продемонстрировать весь спектр его способностей, интересов, склонностей, знаний и умений.