АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

УТВЕРЖДАЮ
ДИРЕКТОР АНО ПО «БИТ»
_____ В.В. СЕРГЕЕВ
«_____» _____ 20____ ГОДА
М.П.

ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА
МДК.03.01 Техническая защита информации

Калининград
2022г.

Программа учебной дисциплины МДК.03.01 «Техническая защита инормации» 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: АВТОНОМНАЯ 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 ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «МДК.03.01. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

1.1. Место дисциплины в структуре основной профессиональной образовательной программы.

Программа междисциплинарного курса «МДК.03.01. Техническая защита информации» 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.03.01. Техническая защита информации», 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	Использовать информационные технологии в профессиональной

9.	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, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.	**ЛР 3**
Принимающий семейные ценности своего народа, готовый	**ЛР 4**

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.	
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	− установки, монтажа и настройки технических средств защиты информации;

опыт	− 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	− 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
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.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Обязательная учебная нагрузка	174
в том числе:	
теоретическое обучение	78
практические занятия	66
самостоятельная работа	18
Экзамен.	**12**

2.2. Тематический план и содержание учебной дисциплины «Техническая защита информации».

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем в часах	Уровень освоения	Осваива-емые ком петенци и
1	2	3		
Раздел 1.		**50**		
Введение	**Содержание учебного материала**	**2**		
	Виды, источники и носители защищаемой информации. Предмет и задачи дисциплины. Структура дисциплины, ее роль и место в системе профессиональной подготовки.	2	1	ОК 01 ОК 03 ЛР 01-12
Тема 1.1. Общие положения.	**Содержание учебного материала**	**14**		
	Понятие об информации и методах ее хищения. Акустическая информация, электронная информация, оптическая информация. Параметры информации, как смысловой аспект.	2 2	1	ОК 01 ОК 02 ЛР 01-12
	Нормативно-правовая база защиты информации. Роль и место правового обеспечения.	2	1	ОК 04 ЛР 01-12
	Общегосударственные документы по обеспечению информационной безопасности.	2	2	ПК 1.1. ЛР 01-12
	Основные этапы и процедуры добывания информации технической разведкой.		2	ПК 2.1. ЛР 01-12

	Организация защиты информации. Организационные и технические мероприятия по защите информации.		2	ПК 3.3. ЛР 01-12
	Классификация иностранной технической разведки. Основные понятия о промышленном шпионаже. Закон и промышленный шпионаж. Основные способы ведения информационной разведки и промышленного шпионажа.		1	ПК 5,3.
	Практические занятия:	**4**		
	ПР-1. Применение прав и обязанностей субъектов в области защиты информации.	2	1	ОК 01 ЛР 01-12
	ПР-2.Стандарт безопасности ISO/IEC 15408..	2		
	Лабораторная работва.	**2**		
	ЛР-1. Расчет параметров информационной безопасности.	2	1	ОК 02 ЛР 01-12
Тема 1.2. Задачи и требования к способам и средствам технической защиты.	**Содержание учебного материала**	**10**		
	Основные понятия и определения. Классификация. Основные параметры по информационной безопасности.	2	1	ОК 04 ЛР 01-12
	Принцип защиты информации техническими средствами. Общие требования к приборам.	2	1	ОК 05 ЛР 01-12
	Общая характеристика методов перехвата информации, копирования, уничтожения, искажения, блокирования, подавления информации.	2	2	ОК 10 ЛР 01-12
	Лабораторные работы:	**4**		
	ЛР-2. Исследование электромеханических приборов вибрационной помехи.	2 2		ПК 3.3. ЛР 01-12

	ЛР-3. Исследование информационных сигналов по осциллографу сканирующего приемного устройства аппаратно-программного комплекса «LAB-2000».			ПК 5,3. ЛР 01-12
Тема 1.3. Теория защиты информации техническими средствами.	**Содержание учебного материала**	**24**	Е	
	Классификация технической разведки. Способы ведения информационной разведки.	2 2	1	ОК 01 ОК 02 ЛР 01-12
	Визуально-оптическая информация. Акустическая информация. Вибрационная информация.	2	1	ОК 04 ЛР 01-12
	Прием и анализ электромагнитных излучений ультрафиолетового, видимого и инфракрасного диапазонов от объектов информации,	2	2	ПК 1.1. ЛР 01-12
	Спектрозональная фотосъемка. Инфракрасная разведка. Тепловизионные приборы и приборы ночного видения.	2 2	2	ПК 2.1. ЛР 01-12
	Прием и анализ электро-магнитного излучения (ЭМИ), создаваемыми различными радиоэлектронными средствами передачи информации..		1	ПК 3.3. ЛР 01-12
	Радиолокационная разведка (РЭР). Принцип действия и область применения.		1	ПК 5,3. ЛР 01-12
	Лазерная разведка. Принцип модуляции отраженного луча. Строчно-кадровая развертка. Аппаратура точного наведения лазерного луча. Условия эффективного перехвата.		1	ПК 5.3. ЛР 01-12
	Практические занятия:	**6**		

	ПР-3.Анализ оптической информации телеохранной информации.	2	1	
	ПР-4.Анализ уровня электро-магнитного излучения..	2		
	ПР-5.Анализ уровня инфрокрасного излучения в помещении..	2		
	Лабораторные работы:	**6**		
	ЛР-4. Исследование спектра речевого сигнала.	2	1	
	ЛР-5. Исследование инфракрасного сигнала от объекта информации.	2	1	
	ЛР-6. Измерение уровня электро-магнитного излучения объекта информации.	2	1	
Промежуточная аттестация по учебной дисциплине				
Раздел 2. Теоретические аспекты технической защиты информации.		**36**		
Тема 2.1. Понятие и особенности технических каналов утечки информации.	**Содержание учебного материала**	**12**		
	Структура, классификация и основные характеристики технических каналов утечки информации. Каналы утечки информации, обрабатываемой техническими средствами передачи информации (ТСПИ).	2 2	1 1	ОК 05 ОК 09
	Физическая природа побочных электромагнитных излучений (ПЭМИ). Элементарный электрический излучатель. Элементарный магнитный излучатель.	2	2	ПК 3.1 ПК 3.3
	Электромагнитные каналы утечки информации. Наводки электромагнитных излучений. Параметрический канал утечки информации.		1	ПК 5.3. ЛР 01-12
	Лабораторные работы:	**6**		
	ЛР-7. Исследование уровня побочного электромагнитного излучения персонального компьютера.	2		
	ЛР-8. Измерение ПЭМИН в канале утечки средств передачи информации.	2 2		
	ЛР-9. Наводки электромагнитных излучений в канале электросвязи.			
Тема 2.2.	**Содержание учебного материала**	**20**		

Технические каналы утечки речевой.	Краткие сведения по акустике. Линейные характеристики звукового поля. Плоская и сферическая волна. Акустические и электрические уровни.	2	2	ОК 02 ОК 04
	Звуковые сигналы. Частотный диапазон и спектр звукового сигнала. Понятность и разборчивость речи.			ОК 09
	Звуковое поле и звуковой фон в помещении. Звуковой резонанс. Звуковые характеристики помещения. Звукопроницаемость и звукоизоляция помещений.	2	1	ОК 10
	Акустические источники утечки речевой информации. Порошковые, электродинамичекие, конденсаторные, электретные, пьезоэлектрические, электромагнитные микрофоны.	2	1	ПК 2.1 ПК 3.1
	Комбинированные, направленные линейчатые, трубчатые, щелевые, фазированные микрофоны. Микрофоны с параболическим рефлектором.	2	2	ПК 3.3
	Основные характеристики направленных микрофонов. Неравномерность воспроизводимых частот, осевая чувствительность, ширина полосы воспроизводимых частот, диаграмма направленности, индекс направленности и коэффициент направленного действия, коэффициент сигнал/шум.		1	ПК 5.3 ЛР 01-12
	Микрофонный эффект радио-электронных элементов.			
	Практические занятия:	**6**		
	ПР-6. Определение полосы воспроизводимых частот электретного микрофона.	2 2		
	ПР-7. Снятие диаграммы направленности порошкового микрофона.	2		
	ПР-8. Определение уровня звукоизоляции служебного помещения.			
	Лабораторные работы:	**6**		
	ЛР-10. Исследование спектра речевого сигнала.	2		
	ЛР-11. Исследование уровня акустической волны.	2		

	ЛР-12. Исследование уровня разборчивости акустического речевого сигнала.	2		
Тема 2.3. Защита информации от утечки по техническим каналам связи.	**Содержание учебного материала**	**4**		ОК 04
	Экранирование электромагнитного поля. Электромагнитное экранирование и развязывающие цепи. Фильтрация информационных сигналов.	2	1	ОК 05
	Подавление емкостных и индуктивных паразитных связей. Заземление технических средств. Пространственное и линейное зашумление.		1	ОК 09
	Средства выявления каналов утечки информации. Индикаторы электромагнитного поля. Анализаторы спектра, частотомеры. Сканирующие радиоприемники. Нелинейные локаторы. Металлодетекторы. Демодуляторы, демаскираторы.	2	1 2	ПК 3.1 ПК 3.3
	Способы предотвращения утечки информации через ПЭМИН ПК. Особенности слаботочных линий и сетей как каналов утечки информации. Безопасность оптоволоконных кабельных систем. Рекомендуемые схемы подключения анализаторов и детекторов поля.			ПК 5.3 ЛР 01-12
Раздел 3. Физические основы технической защиты информации.		**10**		
Тема 3.1. Физика утечки информации по побочным каналам.	**Содержание учебного материала.**	**6**		ОК 01
	Параметрические каналы утечки информации. Виброакустика. Утечка информации через виброакустическую среду. Технические каналы утечки теле – видео информации.	2 2	2	ОК 02 ОК 04 ПК 3.1.
	Оптико-электронные технические каналы утечки речевой информации.	2	2	ПК 3.3 ПК 5.3
	Лабораторные работы:	**4**	1	ЛР 01-12
	ЛР-13. Определение уровня побочного излучения в канале электросвязи.	2 2		
	ЛР-14. Определение уровня побочного излучения в канале виброакустики.			

Тема 3.2. Физические процессы при подавлении средств перехвата информации.	**Содержание учебного материала.**	**10**		ОК 01
	Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.	2	1	ОК 02 ОК 04
	Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра.	2	1	ОК 09 ОК 10
	Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра. Противодействие методам скрытого видеонаблюдения	2	2	ПК 2.1 ПК 3.1.
	Лабораторные работы:	**4**		ПК 3.3
	ЛР-15. Определение частоты и типа модуляции для подавления несанкционированного радиоприема информации.	2	1	ПК 5.3 ЛР 01-12
	ЛР-16. Исследование демаскирующих параметров объекта в инфракрасном диапазоне электромагнитных волн.	2	1	
Раздел 4. Системы защит от утечки информации.		**10**		
	Содержание учебного материала.	**14**		
Тема 4.1. Акустический канал.	Система защиты от утечки информации по акустическому каналу. Система регистрации речи «TEL-32». Область применения, технические характеристики, настройка.	2	1	ОК 01 ОК 02 ОК 04
Тема 4.2. Виброакустический канал.	Система защиты речевой информации в телефонных каналах электросвязи. Четырех канальный прибор защиты телефонной линии «SI-2010». Технические данные прибора.	2 2	2 1	ОК 05 ОК10
	Прецизионный генератор виброакустического шума «SPP-14».			ПК 2.1
Тема 4.3. Телефонный канал электросвязи.	Система защиты от радио микрофонов и портативных диктофонов. Система обнаружения различных электронных устройств скрытого съема информации «СРМ-700-М».	2	1	ПК 3.1.
Тема 4.4. Выносные микрофоны.	**Лабораторные работы:**	**6**		ПК 3.3
	ЛР-17. Исследование электромагнитного поля портативного диктофона.	2 2	1 1	ПК 5.3

	ЛР-18. Измерение уровня маскирующего виброакустичекого шума.	2		ЛР 01-12
	ЛР-19. Измерение уровня маскирующего цифрового шума.			
Раздел 5. Эксплуатация технических средств и систем защиты информации.		**30**		
Тема 5.1. Применение технических средств на объектах защиты.	**Содержание учебного материала.**	**10**		ОК 01
	Система охранно-тревожной сигнализации.	3		ОК 02
	Система контроля и управления доступом.		2	ОК 04
	Телевизионные системы удаленного наблюдения.	4		ПК 1.1
	Система пожарной сигнализации.		2	ПК 3.1.
	Периметральная охранная система.	3		ПК 3.3
	Радио техническая система.		2	ПК 5.3
				ЛР 01-12
Тема 5.2. Аттестация объектов информатизации по требованиям безопасности информации.	**Содержание учебного материала.**	**18**		
	Методы испытания от утечки по каналу ПЭМИН.	2		
	Порядок проведения контроля защищенности помещения от утечки акустической речевой информации.	2	1 1	ОК 01 ОК 02
	Контроль технических средств и систем на наличие акустоэлектрических преобразований.	2		ОК 04 ОК 05
	Практические занятия:	**12**		ОК 09
	ПР-9. Измерение отношений «сигнал/шум» в контрольных точках выделенных помещений.	2	1	ОК 10
	ПР-10. Оценка эффективности мер защиты информации по электромагнитному излучении.	2	1	ПК 2.1
	ПР-11. Испытание пожарного извещателя системы сигнализации «Астра» по уровню инерции, дифференциалу и порогу срабатывания.	2	1	ПК 3.1. ЛР 01-12
	ПР-12. Испытание учебной аудитории на защищенность помещения от утечки акустической речевой информации.	2	1	ПК 3.3
	ПР-13. Испытание компьютерного класса на утечку информации по	2	1	

	каналу ПЭМИН.		1	ПК 5.3 ЛР 01-12
	ПР-14. Составление протокола измерений уровня электромагнитного излучения в учебной аудитории.	2		
Самостоятельная работа обучающихся.	**Тематика самостоятельных работ.**	**10**		
	Основные операции технического обслуживания средств технической защиты информации. Расконсервация оборудования. Развертывание в помещении. Укомплектование датчиками и приборами питания. Предварительная настройка и прогон функциональных возможностей. Профилактика, диагностика неисправностей, текущий ремонт.	2 2		ПК 3.3 ПК 5.3 ЛР 01-12
	Система контроля и управления допуском (СКУД). Принципы построения системы. Порядок допуска сотрудников и клиентов на охраняемые объекты. Планы размещения и маршруты следования.	2		ПК 3.3 ПК 5.3 ЛР 01-12
	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.	2		
	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.	2		ПК 3.3 ПК 5.3 ЛР 01-12
Самостоятельные работы		18		
Промежуточная аттестация по учебной дисциплине в форме экзамена		**12**		
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 следующим 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 локатор 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 защиты информации.
* 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 связи.
* 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,

** интерактивная доска,

** проектор.

3.2. Информационное обеспечение обучения.

3.2.1. Основные источники.

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

2. Нестеров С.А Информационная безопасность. Учебник и практикум. М. Юрайт * 2019.

3. Краковский Ю.М. Информационная безопасность и защита информации. Учебный курс. М. Издательский центр «МарТ», 3-е издание. 2017.

4. Герасименко В.Г. Методы защиты акустической речевой информации от утечки по техническим каналам. 2-е издание. М. «Факел». 2018.

5. 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. Горбатов В.С. Контроль защищенности информации в помещениях. Лабораторный практикум. М. 2017.

3. Каторин Ю.Ф. Энциклопедия промышленного шпионажа. Санкт-Петербург, «ПОЛИГОН», 2019.

4. Научно-производственный центр «НЕЛК». Технические системы защиты информации. Каталог – 2019. М. издательская фирма «НЕЛК».

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

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

7. Катаранов В.А. Цифровые устройства и микропроцессоры. Учебное пособие. Электронное издание М. Академия, 2016.

8. Рогозин Ю.Н. Инженерно-техническая защита информации Лабораторный практикум. М. Издательство МГИУ. 2016.

3.2.3. Дополнительные электронные источники.

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. «СОФТ».

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ.

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: - элементной базы, компонентов и принципы работы типовых устройств защиты информации; - элементной базы, принципа работы типовых извещателей; - требований к монтажу и правила эксплуатации систем охранно-пожарной сигнализации; - основных сведений о методах измерении специальных электрических величин; - принципа действия звуковых радиоволновых, оптических, инфракрасных извещателей.	Демонстрация знаний принципов работы типовых электронных приборов, цифровых устройств, их элементной базы, а также принципа действия основных типов электроизмерительных приборов.	Оценка знаний в ходе тестирования, проведения практических и лабораторных работ.
Умения: - читать монтажные, сборочные, электрические схемы типовых устройств защиты информации; - выполнять проект развертывания измерительной аппаратуры для регистрации мест электромагнитного излучения; - производить расчет параметров безопасности информации; - выполнять подбор типовых первичных датчиков для систем	Умение проводить расчеты типовых параметров приборов и устройств защиты информации. Умение самостоятельно проводить измерения специальных параметров параметров по аттестации объектов информации по требованиям безопасности информации.	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий и лабораторных работ, экзамен.

защиты информации; - снимать показания с электронных измерительных приборов и устройств; - проводить измерения по контролю утечки информации.		

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, демонстрировать весь спектр его способностей, интересов, склонностей, знаний и умений.