АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03

ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

2017г.

Организация-разработчик: АНО ПО «Балтийский информационный техникум»

Разработчики

Балаклиевский Валерий Давидович, зам. Директора АНО ПО «БИТ»

Михальков Алексей Николаевич, преподаватель АНО ПО «БИТ»

Рассмотрена на заседании цикловой методической комиссии информационной безопасности 27 февраля 2017г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ .

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

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

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля «Защита информации техническими средствами» является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид профессиональной деятельности Защита информации техническими средствами и соответствующие ему профессиональные компетенции:

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, 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.

Содержание профессионального модуля состоит из набора разделов, каждый из которых соответствует конкретной профессиональной компетенции или нескольким компетенциям и направлен на развитие набора универсальных компетенций.

Дескрипторы сформированности компетенций по разделам профессионального модуля.

Спецификация ПК/ разделов профессионального модуля

Формируемые компетенции	*Название раздела*		
	Действия (дескрипторы)	*Умения*	*Знания*
Раздел модуля МДК 03.01 Физические основы защиты информации			
ПК3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими	*Решение задач на расчет механических, электрических и магнитных воздействий на объекты в случае несанкционированного доступа к информации*	*Рассчитывать степень безопасности объекта информации; рассчитывать диаграмму направленности и помехоустойчивость физических*	*Методы физического съема информации в телефонных, компьютерных и радиоканалах связи; принципы доступа к объектам информации через побочные*

средствами обработки информации ограниченного доступа.		*датчиков защиты информации.*	*электромагнитные излучения и наводки.*
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых ТСЗИ	*измерение параметров фоновых шумов, а также физических полей, создаваемых ТСЗИ*	*Рассчитывать по принятой методике фильтры звуковых частот в случае применения звуковых детекторов разбитого стекла; рассчитывать уровень акустического сигнала в точке размещения аудио преобразователя.*	*Базовые физические законы электромагнетизма, акустики, оптики, высокочастотных колебаний; физические принципы распространения в твердой, жидкой и газообразной средах акустических и высокочастотных волн.*
Раздел модуля МДК 0.02 Технические средства защиты информации и их эксплуатация			
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание ТСЗИ в соответствии с требованиями эксплуатационной документации.			
	установка, монтаж, настройка и техническое обслуживание ТСЗИ в соответствии с требованиями эксплуатационной документации.	*Осуществлять настройку, регулировку, восстановление работоспособности, прием и освоение компьютерного оборудования защиты информации.*	*Основные характеристики и функциональные возможности систем и отдельных ТСЗИ от утечки информации по различным каналам передачи информации.*
ПК 3.2 Осуществлять эксплуатацию ТСЗИ в соответствии с требованиями эксплуатационной документации.	*Выполнять работы по установке, настройке и обслуживанию ТСЗИ.*	*Выполнять полный комплекс задач администрирования операционных систем, систем управления базами данных, компьютерных сетей в части средств обеспечения*	*Номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.*

		информационной безопасности.	
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	*Применять системный подход к обеспечению информационной безопасности в различных сферах деятельности.*	*Планировать и организовывать комплекс мероприятий по защите информации.*	*Основы организационного обеспечения информационной безопасности.*

2. СТРУКТУРА и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	*Наименования разделов профессионального модуля*[*]	*Всего часов (макс. учебная нагрузка и практики)*	*Объем времени, отведенный на освоение междисциплинарного курса (курсов)*					*Практика*	
			Обязательные аудиторные учебные занятия			*внеаудиторная (самостоятельная) учебная работа*		*учебная, часов*	*производственная часов (если предусмотрена рассредоточенная практика)*
			всего, часов	*в т.ч. лабораторные работы и практические занятия, часов*	*в т.ч., курсовая проект (работа)*, часов*	*всего, часов*	*в т.ч., курсовой проект (работа)*, часов*		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
ПК3.1 – 3.5 ОК	*Раздел 1. Физические основы защиты информации*	*120*	*60*	*20*	-	*60*	-	*40*	*
	Раздел 2. Технические средства защиты информации и их эксплуатация	*220*	*120*	*70*		*100*			*100*
УП	*Учебная практика*	*72*							
ПП	*Производственная*	*144*							*108*

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

	практика								
	Всего:	***440***	***180***	***90***	***-***	***160***		***40***	***100***

2.2. Тематический план и содержание профессионального модуля «Защита информации техническими средствами»

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	***Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)***		***Объем часов***
1	***2***		***3***
Раздел 1. Физические основы защиты информации			***60***
Тема 1.1. Тема 1.1. Физические датчики и физические детекторы	***Содержание (указывается перечень дидактических единиц темы каждая из которых отражена в перечне осваиваемых знаний)***	***Уровень освоения***	
	1. Понятие о физических явлениях, - звук, свет, тепло, движение, давление, вибрация, электричество, проводимость, магнитное поле, - как физических основах защиты информации. Объекты и субъекты информации. Носители информации. Угроза информации. Атака на безопасность информации.	***1***[1]	***2***
	2. Понятие о физических датчиках для защиты информации. Понятие о физических детекторах. Понятие о чувствительности, «мертвой зоне» и помехозащищенности физических датчиков. Понятие о каналах и системах обработки и передачи информации. Плюс ПР-1 2 часа!	***2***	***2***
	Практическая работа № 1. Разработка формальной модели безопасности информации в компьютерном классе. Расчет степени безопасности локальной компьютерной сети.	***2***	***2***
Тема 1.2. Физика твердого тела.	1. Давление. Упругость твердого тела. Упругий удар твердых тел. Деформация твердого тела Вибрация твердого тела Датчики давления. Датчики деформации. Датчики встряски. Ударо-контактные датчики. Вибродатчики.	*2*	*2*

[1] *Здесь и далее места, в которых необходимо указать уровень освоения помечены «**»*

[2] *Здесь и далее указывается количество часов; рекомендации аналогичны приведенным в теме 1*

	2. Геометрия твердого тела. Форма твердого тела. Давление на изгиб. Давление на разрыв. Давление на опору. Сжатие. Контроль целостности объекта. Контроль формы объекта. Контроль присутствия объекта. Контроль положения объекта.	*2*	
	Лабораторная работа №1. Исследование параметров датчика давления при угрозе безопасности объекта информации.	2	***3***
	Самостоятельная работа № 1. Работа со специальной справочной литературой. Определение вероятности скрытой угрозы для компьютерного класса.		***3***
Тема 1.3. Движение и перемещение твердого тела.	1. Физика поступательного перемещения тел по горизонтальной поверхности. Прерывистое движение тел. Очень медленное и очень быстрое перемещение тел. Перемещение в замкнутом пространстве. Датчики движения. Датчики перемещения. Чувствительность датчиков. Помехозащищенность датчиков. Движение тел малых размеров.	*2*	***2***
	2. Вторичные явления перемещения твердого тела. Столкновение с препятствием. Следы перемещения. Аэроэффекты. Движение воздуха. Датчик соприкосновения. Контроль за движением воздуха.	*2*	***2***
	Лабораторная работа № 2. Исследование помехозащищенности датчика движения в замкнутом пространстве.	*2*	***3***
	Самостоятельная работа № 2. Работа со специальной справочной литературой. Типовой расчет зоны чувствительности датчика соприкосновения.	*1*	***3***
Тема 1.4. Тепловые явления	1. Нагревание, плавление, расширение, испарение. Явление запотевания. Температурные датчики для твердых тел. Температурные датчики контроля для помещений. Порог срабатывания и скорость срабатывания температурных датчиков. Диаграмма направленности.	*2*	***2***
	2. Движение объектов, излучающих тепло (человек, автомобиль, электроприборы). Диффузия. Тепловые потоки воздуха. Регистрация появления и перемещения тепловых потоков. Датчики теплового движения.	*2*	***3***

	3. Поглощение тепла. Остывание. Быстрая заморозка. Появление инея. Датчики внезапного скачка температур. Температурный дифференциал.	*2*	***3***
	Лабораторная работа № 3. Исследование динамических параметров температурного датчика.	*2*	***3***
	Самостоятельная работа № 3. Работа со специальной справочной литературой. Типовой расчет зоны чувствительности датчика контроля температуры воздуха для компьютерного класса.		***3***
Тема 1.5. Физика жидких и газообразных тел	1. Передача информации через воздушную и жидкостную среду. Атака на объект информации через воздушную и жидкостную среду. Гидро- и пневмо удары. Датчики давления и перемещения воздушной массы. Пневмо-датчики. Гидро-датчики.	*2*	***1***
	Практические занятия № 2. Конструктивное размещение пневмо-датчиков в замкнутом помещении компьютерного класса.	*2*	***2***
	Лабораторная работа № 4. Снятие диаграммы направленности пневмодатчика в условиях замкнутого помещения.	*2*	***3***
	Контрольная работа № 1	*2*	
Тема 2.1. Электрические и электромагнитные явления	1. Общие сведения об электрических цепях. Сопротивление цепи, проводимость цепи. Утечка токов. Терминология. Омические датчики.	*2*	
	2. Контакты в цепи. Ветви и узлы цепи. Параллельное соединение и соединение мостом. Электромагнетизм. Датчики электрического параметра. Мост Вина. Гер коны.. Электро-контактные датчики.	*2*	***1***

	3. Короткое замыкание в цепи. Обрыв электрической цепи. Параметры короткого замыкания и обрыва цепи. Схемы сравнения электрического параметра. Датчики сравнения. Компараторы. Контроль тока утечки. Электромагнитные датчики.	*2*	***3***
	4. Электрические цепи переменного тока. Реактивное сопротивление. Емкость и индуктивность в цепи переменного тока. Емкостные датчики. Индуктивные датчики.	*2*	***2***
	5. Переменный ток высокой частоты. Трансформаторы. Резонансные явления. Бесконтактная передача электрического тока. Индукционные датчики Трансформаторные датчики. Резонансные датчики.	*2*	***2***
	Лабораторная работа № 5. Исследование резонансного датчика.	*2*	***3***
	Самостоятельная работа № 4. Работа со специальной справочной литературой. Работа с каталогами. Изучение типовых схем индукционных датчиков для применения в компьютерном классе.		***3***
Тема 2.2. Волновые явления низкой частоты.	1. Звуковые явления. Инфразвук Ультразвук. Частота и длина волны звука. Распространение звука. Отражение звука. Эхо. Стоячие и бегущие волны. Звуковые детектора разбитого стекла. Эхо-датчики.	*2*	***2***
	2. Падающая и отраженная волна. Преломление звука. Наложение звука. Дифракция и интерференция звука. Тень от звука. Датчики пространства Датчики шума. Датчики нетипичного звука (фильтры).	*2*	***3***
	Практическая работа № 3. Разработка схемы конструктивного размещения инфразвукового датчика охраны объекта информации в замкнутом помещении компьютерного класса	*2*	***2***
	Самостоятельная работа № 5. Работа со специальной справочной литературой. Работа с каталогами. Изучение типовых схем звуковых детекторов разбитого стекла. Выбор детекторов с целью применения для охраны информации в компьютерном классе.		***3***

Тема 2.3. Волновые явления высокой частоты.	1. Радиоволны. Электромагнитные колебания, распространение радовали. Падающая и отраженная радио волна. Преломление радио волны. Дифракция и интерференция звука. Радиоволновые детекторы перемещения. Радио дальномеры. Радио зонды. Датчики радио отражения. Датчика целостности (стекла, объекта). Сенсорный эффект.	*2*	***1***
	2. Эффект Доплеров- Побочное электромагнитные излучения (ПЭМИ) и наводки. Радио накачка. Радио детекторы направления перемещения. Активная и пассивная ВЧ-накачка.	*2*	***2***
	Лабораторная работа №6. Исследование падиоволнового детектора. Снятие диаграммы направленности радиоволнового детектора.	*2*	***3***
	Самостоятельная работа № 6. работа со специальной справочной литературой. Работа с каталогами. Изучение типовых схем датчиков радио отражения.	*2*	
Тема 2.4. Волновые явления сверх высокой частоты.	1. Радиоволны. Свет. Инфракрасный диапазон света. Ультрафиолетовый диапазон света. Белый шум. Рассеянный свет, яркость света. Датчики яркости. Датчики плотности воздуха в помещении.	*2*	***1***
	2. оптические явления, фотоэффекты. Свечений тел в УФ-лучах. ИК-излучение источников тепла. Фото-датчики. Детекторы движения на ИК-лучах. Датчики перемещения тепловых потоков. Вторичное свечение. Опто-пары и опто-датчики. Линейный датчики пространства.	*2*	***2***
	Самостоятельная работа № 7. Работа со специальной технической литературой. Типовой расчет конструктивного размещения линейных датчиков в реальном компьютерном классе.	*1*	***3***
	Практическая работа № 4. Снятие диаграммы направленности фото-датчика. Определение чувствительности и ширины диаграммы направленности фото-датчика. Выявление «мертвой зоны» датчика.	*2*	***2***

Тема 3.1. Преобразование аудио информации.	1. Микрофоны аудио перехвата. Пассивные и активные микрофоны. Диаграммы направленности. Чувствительность. Физические методы защиты от аудио перехвата. Микрофоны порошковые (угольные), электродинамические, электростатические (конденсаторные), электретные, электромагнитные, пьезоэлектрические. Микрофоны с внешним управлением.	*2*	***2***
	2. Перезоват аудио информации в кабельных сетях. Перехват телефонных разговоров. Перехват компьютерного обмена информацией. Перехват информации с принтера и со сканера. Перехват информации в узлах связи, на коммутаторах, уплотнителях.	*2*	***2***
	3. Контактный и бесконтактный съем аудио информации на телефонных сетях. Подключение с компенсацией. Подключение с имитацией. Подключение с замещением. Высокочастотное навязывание. Съем информации с телефонного аппарата при не снятой трубке. Пассивный радио микрофон. Микрофон Термена.	*2*	***2***
	4. Съем информации в компьютерных сетях. Физические способы получения информации, обрабатываемой в компьютерных сетях. Контактный и бесконтактный съем компьютерной информации. Съем информации в режиме «Между строк». Съем в режиме «Замещения». Режим «Перехват завершения сеанса связи». Режим « Имитация сбоя». Режим «Отправка документа на печать». «Режим «Работа в Интернете».	*2*	***3***
	Самостоятельная работа № 8. По индивидуальному заданию выбор метода Защиты от несанкционированного доступа к аудио информации средствами активного направленного микрофона.		***1***
Тема 3.2. Физическая защита информации в радио сетях и сетях спутниковой (космической) связи.	1. Принцип передачи информации по каналам радио связи. Радиотелефонные каналы (зона «Е»). Широковещательные каналы радиосвязи. Ретрансляционные радио каналы. Радиорелейные каналы. Пейджинговые сообщения стандарта PPR2.1. Каналы сотовой связи. Мобильные каналы индивидуальной связи.	*2*	***2***
	2. Цифровые каналы связи. Методы частотного уплотнения. Методы кодирования цифровой информации. Методы идентификации пользователей. Спутниковые каналы связи. Методы доступа к спутниковым каналам информации.	*2*	***2***

	3.Стандартные протоколы защищенного канала. Уровни защищенных каналов, защита данных на канальном уровне; протоколы PPTP, L2F и L2TP. Защита данных на сетевом уровне - IPSec, назначение, характеристика, режим работы. Установление безопасной ассоциации, база данных политики безопасности, защита данных с помощью протокола AH, защита данных с помощью протокола ESP, защита на представительском уровне. Схемы взаимодействия предприятия с провайдером при организации VPH.	*2*	***2***
	Самостоятельная работа № 9. По индивидуальному заданию определение метода физической защиты от несанкционированного доступа к цифровой информации в каналах радио ретрансляционной связи.		***1***
Тема 3.3. Физическая защита информации при «нетрадиционных» методах перехвата.	1. Принцип (высокочастотного) ВЧ-навязывания. Принцип Л САР (лазерная система активной разведки). Гидроакустика (гидродатчики, гидрофоны). Гео-датчики. Магнитное поле Земли. Стихийные события. Магнитометры. Датчики внешнего магнитного поля. Магнитные уравновешенные датчики. Био-датчики. Рентгеновское излучение Сверх высокочастотное излучение. Искусственные помехи. Умышленная дезинформация. Имитация аварии. Блокирования датчиков. Ложные срабатывания датчиков. Защита датчиков.	*2*	***2***
	Самостоятельная работа № 10. Работа со специальной технической литературой. По индивидуальному заданию определение метода физической защиты от несанкционированного доступа к цифровой информации, осуществляемой методами Л САР (лазерная активная система разведки) в помещениях компьютерной обработки данных.		***3***
	Контрольная работа № 2. Физические явления, используемые для защиты информации при угрозе несанкционированного доступа.	*2*	***2***
Учебная практика раздела 1 ***Виды работ*** ***1*** Лабораторные и практические работы согласно тематического плана.			***

Раздел N2 *Технические средства защиты информации и их эксплуатация*			***120***
Раздел 1. Актуальность применения технических средств и методов защиты информации.	***Содержание***	***Уровень освоения***	
	Введение в дисциплину. Системный подход к ИТЗИ. Классификация и параметры системы защиты информации.	***2***	***8***
	Тема 1.1 Виды защищаемой информации, её свойства, демаскирующие признаки.	***2***	
	Тема 1.2 Источники и носители информации. Основные функциональные свойства ИТЗИ. Виды и источники угроз безопасности, опасные сигналы и их источники.		***2***
	Тема 1.3 Виды информационных сигналов в компьютерных системах и каналах связи. Аналоговые и цифровые способы передачи информации. Виды модуляции.		***2***
Раздел № 2. Структура, классификация и основные характеристики (ТКУИ). Пассивные и активные методы защиты от НСД.	Тема 2.1 Физические пути и каналы утечки информации. Классификация и структура ТКУИ. Акустические каналы утечки, направленные микрофоны.	***3***	***22***
	Тема 2.2 Электромагнитные каналы утечки информации. Побочное электромагнитное излучение и наводки (ПЭМИН). Классификация способов защиты.		***2***
	Тема 2.3 Активные методы защиты информации от утечки по каналам ПЭМИН.		***2***
	Тема 2.4 Пассивные методы защиты от ПЭМИН путём экранирования корпусов ПК, помещений, каналов связи. Основные характеристики экранов.		***2***

	Тема 2.5 Устройство и типы заземления. Применение оптоволоконных линий связи (ВОЛС) и ИК каналов для защиты от утечки информации.	***2***
	Тема 2.6 Электрические и параметрические каналы утечки информации. Физические пути утечки акустических информационных сигналов Специальные устройства съёма информации. Способы защиты.	***2***
	Тема 2.7 Источники бесперебойного питания. Типы, характеристики, структурные схемы.	***4***
	Тема 2.8 Защита информации по цепям электропитания. Сетевые фильтры. Устройства грозозащиты.	***4***
	Тема 2.9 Системы электропитания компьютерного оборудования современного предприятия.	***4***
Раздел № 3. Основы радиосвязи. Распространение радиоволн. Правила безопасности ведения переговоров с использованием радиосредств.	Тема 3.1 Основы радиосвязи, антенные устройства. Международный стандарт распределения диапазонов радиоволн.	***2***
	Тема 3.2 Особенности распространения радиоволн (РРВ). Рабочие частоты передачи сигналов в каналах утечки информации.	***2***

	Тема 3.3 Современные виды связи по радиоканалам. Задачи и структура государственной системы противодействия технической разведке. Организация ИТЗИ на предприятиях, нормативная база.	***2***
	Тема 3.4 Контрольная работа № 1. Тест по ИБП, ПЭМИН, радиосвязи, РРВ, ТКУИ.	***2***
Раздел № 4. Методы и средства защиты от наблюдения, подслушивания, перехвата. Защита от утечки акустической информации по техническим каналам	Тема 4.1 Классификация физических путей утечки акустической информации. Преобразователи сигналов - микрофоны, датчики. Их характеристики.	***2***
	Тема 4.2 Классификация радиозакладных устройств по 5 признакам. Способы внедрения РЗУ злоумышленниками. Контрольная работа № 2 – классификация РЗУ на примерах из прайс-листов технических средств.	***2***
	Тема 4.3 Технические средства поиска радиозакладок по электро-магнитному излучению. Индикаторы поля, частотомеры, радио сканеры. Их отличительные характеристики.	***4***
	Тема 4.4 Поисковые комплексы аппаратного и программно – аппа-ратного типа на примерах «Филин» «Oscor5000». Принцип корреляции в поисковых приёмниках.	***2***
	Тема 4.5 Основные задачи радиомониторинга. Методы и средства обнаружения, локализации закладных устройств, подавления опасных сигналов ПЭМИН.	***4***

	Тема 4.6 Практикум по поиску закладных устройств организационными методами и с применением поисковых средств.	***4***
	Тема 4.7 Технические средства съёма информации по виброакустическим каналам. Средства защиты от утечки информации по эти каналам.	***4***
Раздел № 5. Средства и методы зашиты от несанкционированного съёма речевой информации в телефонных линиях и каналах связи	Тема 5.1 Основы телефонии. Линии связи, распределительная сеть. Основные методы, применяемые злоумышленниками при несанкционированном доступе к информации в телефонной линии.	***4***
	Тема 5.2 Устройства защиты сигналов в телефонных каналах связи. Скремблеры. Принцип инверсии спектра сигнала.	***4***
	Тема 5.3 Скремблеры с перестановкой частотных полос спектра, временной перестановкой и способы защиты цифровой информации.	***4***
	Тема 5.4 Акустопреобразователи сигналов информации. Образование каналов утечки информации за счёт действия «микрофонного эффекта».	***4***

	Тема 5.5 Защитные устройства контроля за состоянием телефонных линий. Анализаторы и маскираторы сигналов. Устройства активной защиты в телефонии.	***4***
	Тема 5.6 Лабораторный практикум по исследованию каналов утечки информации в телефонных линиях.	***6***
	Тема 5.7 Лабораторный практикум по исследованию защитных устройств устанавливаемых в телефонные линии и каналы.	***6***
Раздел № 6. Методы и средства инженерной защиты и технической охраны объектов (территорий и помещений).	Тема 6.1 Средства инженерной защиты территорий и помещений. Классификация. Виды ограждений и типы сигнализации охраны. Металлодетекторы.	***6***
	Тема 6.2 Системы ограничения доступа в помещения. Структурная схема взаимодействия основных устройств. Методы идентификации личности по биометрическим и др. признакам	***4***
	Тема 6.3. Аналоговая система видеонаблюдения. Состав оборудования, типы видеокамер.	***2***
	Тема 6.4 Системы цифрового видеонаблюдения. Сравнение основных характеристик двух систем видеонаблюдения.	***2***
Раздел № 7. Организация охраны и безопасности объектов защиты.	Тема 7.1 Сигнальные цепи и каналы охраны. Контрольные панели, основные станции контроля, применяемые для охраны.	***2***

	Тема 7.2 Датчики охранно-пожарной сигнализации. Типы, классификация, характеристики.	***2***
	Тема 7.3 Комплексные системы охранно-пожарной сигнализации современных предприятий. Состав, назначение.	***2***
	Тема 7.4 Практическая работа по включению датчиков в охранно-пожарную систему. Работа с макетом охранной сигнализации.	***6***
	Тема 7.5 Системы сигнализации, использующие для передачи сигналов тревоги радиоканал.	***2***
Раздел № 8. Анализ угроз и классификация средств защиты информации по требованиям безопасности	Тема 8.1 Технический контроль эффективности защиты информации.	***4***
	Тема 8.2 Системный подход к инженерно-технической защите информации. Вопросы комплексной системы безопасности.	***4***
	Тема 8.3 Нормативно методическое обеспечение ИТЗИ. Моделирование объектов защиты от степени воздействия угроз безопасности.	***4***
	Тема 8.4 Деловая игра по обеспечению защиты информации виртуальной фирмы. Составление плана установки ИТЗИ в помещениях и на территории объектов.	***6***

Учебная практика Контрольная работа № 1 Классификация по 5 признакам радиозакладных устройств по данным из прайс-листов на РЗУ. Лабораторная работа по исследованию свойств направленного микрофона Практикум по поиску закладных устройств организационными методами и с применением поисковых средств, Контр. работа по РЗУ Лабораторный практикум по исследованию каналов утечки информации в телефонных линиях (Лаб.работы №№ 1,2,3,4) . Лабораторный практикум по исследованию защитных устройств устанавливаемых в телефонные линии и каналы (Лаб.работы №№ 4) . Практическая работа по включению датчиков в охранно-пожарную систему. Работа с макетом охранной сигнализации. Технический контроль эффективности защиты информации. Планирование комплексных мероприятий по защите информации службами безопасности предприятий. Деловая игра по обеспечению защиты информации виртуальной фирмы. Составление плана установки технических средств защиты информации в помещениях и на территории объектов. – ***Производственная практика*** Организация охраны и безопасности объектов защиты. Установка, монтаж, настройка и техническое обслуживание технических средств защиты информации. Проверка технического состояния, обслуживание и текущий ремонт, устранение отказов и восстановление работоспособности АИС в защищенном исполнении. Измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	
Всего	***216***

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

3.1. Материально-техническое обеспечение

Реализация профессионального модуля предполагает наличие учебного кабинета и лаборатории «Технические средства защиты информации».

Оборудование кабинета, лаборатории и рабочих мест:

Технические средства защиты информации:

- Лабораторные макеты в количестве 12 штук.
- Компьютеры на двух рабочих местах (видеонаблюдение и запись аудиоинформации с телефонного канала);
- проектор и кодопроектор;
- программное обеспечение общего и профессионального назначения;
- комплект учебно-методической документации.

3.2. Информационное обеспечение обучения

Основные источники (печатные):

1. В.И. Ярочкин «Информационная безопасность», М. Академический Проект, Фонд "Мир", 640 стр.
2. А.А. Торокин Инженерно-техническая защита информации. Москва «Гелиос АРВ».
3. Е.Б.Белов, В.П.Лось «Основы информационной безопасности» М. Горячая линия – Телеком г.
4. А.В. Пугин «Лабораторный практикум» часть 1 (по телефонии) БИТ .Н.
5. Соболев, В.М. Кириллов «Физические основы технических средств обеспечения информационной безопасности». Москва «Гелиос АРВ».

Дополнительные источники:

1. Под редакцией И.В. Василевского «Технические средства и методы защиты информации» Учебное пособие БИИТ.
2. Т.Л. Партыка «Информационная безопасность» Учебник Москва.
3. О.В.Головин «Радиосвязь»
4. В.И.Каганов «Радиотехнические цепи и сигналы».
5. А.А. Хорев, «Технические средства защиты информации» - часть 1 М.: МО РФ, 316 с.
6. А.В. Пугин «Методическое пособие по информационной безопасности» (Доктрина ИБ РФ)
7. Издательство БИТ «Сборник законодательных актов и нормативно-

правовых документов по защите информации»

8. С.Н. Сёмкин, Э.В. Беляков «Основы организационного обеспечения информационной безопасности объектов информатизации». Учебное пособие. Москва «Гелиос АРВ».

3.3. Организация образовательного процесса

Обучение по данному модулю основывается на знаниях и умениях, полученных при изучении общепрофессиональных дисциплин: электротехника, электроника и схемотехника, информатика, архитектура КС, информационные технологии. Обучение по модулю проводится в виде лекционных и практических занятий. Практические занятия проводятся в компьютерных классах и лабораториях, оснащенных соответствующим программным обеспечением и лабораторными установками. Время на изучение модуля – 180 часов, из них 90 часов практических занятий. В ходе проведения учебной практики студенты получают практические навыки по радиомонтажу. Время на отработку практических занятий в период учебной практики – 72 часа. В ходе проведения производственной практики студенты получают практические навыки согласно профессиональных компетенций, установленных ФГОС.

3.4. Кадровое обеспечение образовательного процесса

К педагогической деятельности в Техникуме допускаются лица, имеющие высшее образование, отвечающие требованиям квалификационных характеристик, определенных для соответствующих должностей педагогических работников. Образовательный ценз указанных лиц подтверждается документами государственного образца о соответствующем уровне образования и (или) квалификации.

1. ***Контроль и оценка результатов освоения профессионального модуля (по разделам)***

Результаты **(освоенные профессиональные компетенции)**	**Основные показатели оценки результата**	***Формы и методы контроля и оценки***

обеспечение процессов защиты информации и использованием необходимых видов, методов, средств и технологий защиты;	– качество и скорость настройки параметров функционирования аппаратного обеспечения; – качество и скорость установки и настройки основных компонентов системы защиты информации; – диагностирование простейших неисправностей оборудования ЗИ в случаях выхода из строя или повреждений; – качество проведения технического обслуживания аппаратных устройств.	*Текущий контроль в форме:* *- защиты практических занятий;* *- контрольных работ.* *Зачеты по учебной практике и по разделу профессионального модуля.* *Дифференцированный зачёт по профессиональному модулю.*
учет, обработка, хранение, передача, организация использования различных носителей конфиденциальной информации;	– демонстрация навыков работы с различными носителями информации; – качество и скорость настройки параметров функционирования периферийных устройств и компьютерной оргтехники; – диагностирование простейших неисправностей периферийных устройств и компьютерной оргтехники; – установка и замена расходных материалов для периферийных устройств и компьютерной оргтехники; – качество проведения технического обслуживания периферийных устройств и компьютерной оргтехники; – точность и грамотность оформления технологической документации. –	
выявление и блокирование каналов и методов несанкционированного доступа к информации, источников и способов дестабилизирующего воздействия на информацию;	– качество использования ресурсов локальных и глобальных компьютерных сетей; – управление файлами данных на локальных, съёмных запоминающих устройствах, а так же на дисках локальной компьютерной сети и в интернете; – качество распечатки, тиражирования и копирования документов на принтере и др. оргтехнике.	
установка и адаптация систем и средств обеспечения защиты информации;	– грамотность и точность работы в прикладных программах: текстовых и редакторах, базах данных, редакторе презентаций; – грамотность и точность работы с файловыми системами, различными форматами файлов, программами управления файлами; – скорость поиска информации в содержимом баз данных.	
осуществление контроля за качеством	– точность и грамотность настройки электронной почты, серверного и клиентского	

функционирования оборудования защищенных автоматизированных и телекоммуникационных систем, анализ качественных и количественных показателей функционирования оборудования, диагностика и устранение отказов, настройка и ремонт оборудования;	программного обеспечения; – скорость поиска информации с помощью технологий и сервисов интернета; – точность и грамотность ввода и передачи информации с помощью технологий и сервисов интернета;	
осуществление технической эксплуатации систем и средств обеспечения защиты информации на объектах профессиональной деятельности, предназначенных для сбора, обработки, хранения и передачи информации	– грамотность съёмки и передачи цифровых изображений с фото- и видеокамеры на компьютер; – грамотность и точность работы в мультимедийных и графических редакторах; – качество сканирования прозрачных и непрозрачных оригиналов;	
Обеспечивать общие меры по информационной безопасности.	– грамотность использования методов и средств защиты информации от несанкционированного доступа; – грамотность осуществления резервного копирования и восстановления данных; – точность ведения отчётной и технической документации.	

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

Результаты **(освоенные общие компетенции)**	**Основные показатели оценки результата**	***Формы и методы контроля и оценки***

Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	– демонстрация интереса к будущей профессии; – использование современных методов и средств информационных технологий при разработке информационных систем.	*Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы* *Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам* *Экзамен квалификационный*
Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	– применение методов ИТ при решении профессиональных задач; – выдвижение нестандартных идей при решении профессиональных задач. – оценка эффективности и качества выполнения;	
Планировать и реализовывать собственное профессиональное и личностное развитие	– решать стандартных и нестандартных профессиональных задач в области разработки технологических процессов изготовления деталей машин; – Владение методами влияния человека-оператора на функционирование информационных систем.	
Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	– эффективный поиск необходимой информации; – использование различных источников, включая электронные; – использование методов и средств организации, проектирования, разработки и применения систем, предназначенных для обработки информации.	
Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	– использование методов и средств информационных и телекоммуникационных технологий; – владение методами анализа информационных ресурсов.	
Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	– взаимодействие с обучающимися и преподавателями в ходе обучения – использование промышленных стандартизированных решений, опирающихся на современные информационно-коммуникационные технологии. – владение методами анализа проектных решений.	
Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в	– самоанализ и коррекция результатов собственной работы; – использование моделей администрирования сети и способов обеспечения безопасности информационных	

чрезвычайных ситуациях	систем.	
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
Использовать информационные технологии в профессиональной деятельности	– анализ инноваций в области разработки программного обеспечения; – использование структуры информационных систем, методов и средств информационных и телекоммуникационных технологий.	
Пользоваться профессиональной документацией на государственном и иностранном языках	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
Планировать предпринимательскую деятельность в профессиональной сфере	– самоанализ и коррекция результатов собственной работы; – использование моделей администрирования сети и способов обеспечения безопасности информационных систем.	