Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Амурский государственный университет»

РАБОЧАЯ ПРОГРАММА
по профессиональному модулю

ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Квалификация выпускника – техник по защите информации
Год набора 2021
Курс 2,3 Семестр 3,4,5,6
Общая трудоемкость дисциплины 782 (час.)

Составитель: Батурин Д.С.

2021г.

Рабочая программа профессионального модуля разработана в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденный приказом Минобрнауки РФ от 09.12.2016 г. № 1551

Рабочая программа обсуждена на заседании ЦМК социально-экономических дисциплин
«25» 05 20 21 г., протокол № 6
Председатель ЦМК _____Кирилюк Н.В.

СОГЛАСОВАНО
Зам. декана по учебной работе
_____ А.А. Санова
«23» 05 2021 г.

СОГЛАСОВАНО
Научная библиотека
_____
«24» 05 2021 г.

1. Область применения программы

Программа профессионального модуля ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты является частью образовательной программы в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа может быть использована в дополнительном профессиональном образовании.

2. Место учебной дисциплины в структуре основной образовательной программы: ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях сиспользованием технических средств защиты относится к дисциплинам профессиональныхмодулей, читается в 3, 4, 5, 6 семестрах в объеме 782 акад.часа. На компетенциях, формируемых на профессиональном модуле базируется прохождение производственной практики и производственной практики (преддипломной), а также подготовка и защита выпускной квалификационной работы.

3. Показателем освоения профессионального модуля:

Результатом освоения профессионального модуля является овладение профессиональными (ПК) и общими (ОК) компетенциями:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональ-ной документа-цией на государ-ственном и ино-странном языках

ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.

ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.

ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

ПК 3.4. Проводить отдельные работы по физической защите линий связи

информационно-телекоммуникационных систем и сетей.

В результате освоения учебной дисциплины обучающийся должен иметь практический опыт:

- выявление технических каналов утечки информации;
- использование основных методов и средств инженерно-технической защиты информации;
- диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;
- участие в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
- решение частных технических задач, возникающих при аттестации объектов, помещений, технических средств.

В результате освоения учебной дисциплины обучающийся должен уметь:

- применять технические средства защиты информации;
- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам;
- применят нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами.

В результате освоения учебной дисциплины обучающийся должен знать:

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;
- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам;
- номенклатуру применяемых средств охраны объектов, систем видеонаблюдения.

4. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Тематический план профессионального модуля

Код профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Консультации, часов	Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося			Производственная (по профилю специальности), ** часов	
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов			
1	2	3	4	5	6	7	8	9	10	
ПК 3.1-3.4	МКД.03. 01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	288	222	104	-	46	-	20	-	
ПК 3.1-3.4	МДК.03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей	266	198	94	-	46	-	22	-	
ПК 3.1-3.4	Учебная практика	36						-	-	
ПК 3.1-3.4	Производственная практика	144							144	
	Всего:	746	612	198	-	92	-	42	144	

4.2 Тематический план и содержание ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов	Уровень освоения
1	**2**		**3**	**4**
МКД.03. 01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты				
Раздел 1.	**Применение инженерно-технических средств обеспечения информационно безопасности**			
Тема 1.1. Объекты информационной защиты	**Содержание**			
	1	Введение	4	
	2	Средства информации ка предмета защиты техническими средствами.	4	**2**
	3	Демаскирующие признаки объектов защиты. Демаскирующие признаки сигналов, веществ. Носители и источники информации. Запись и съем информации с ее носителя.	6	**3**
	4	Источники угроз безопасности информации.	4	**3**
	5	Опасные сигналы и их источники.	4	**3**
	Практические работы			
	1	Классификация демаскирующих признаков.	4	**3**
	2	Основные виды угроз информации	4	**3**
Тема 1.2. Угрозы информационной безопасности	**Содержание**			
	1	Виды угроз безопасности информации, защищаемой техническими средствами. Органы добывания информации. Технология добывания информации.	4	
	2	Добывание информации без физического проникновения в контролируемую зону. Способы несанкционированного доступа к источнику информации. Способы и средства добывания	4	

		информации техническими средствами. Способы и средства перехвата сигналов. Классификация и структура технических каналов утечки информации. Акустические каналы утечки.		
	3	Оптические каналы утечки. Радиоэлектронные каналы утечки информации. Вещественные каналы утечки информации.	4	**3**
	Лабораторные работы			
	1	Работа остронаправленных микрофонов.	4	**3**
	2	Работа диктофонов со скрытой записью.	4	**3**
	3	Утечка информации по цепям.	4	**3**
	4	Типовая структура технических каналов утечки.	4	**3**
	5	Моделирование каналов утечки информации.	4	**3**
	6	Опасность электрических сигналов и радиосигналов в радиоэлектронном канале.	4	**3**
	7	Методы добывания информации о вещественных носителях.	4	**3**
Тема 1.3 Методы инженерно-технической защиты информации	**Содержание**			
	1	Концепция инженерно-технической защиты информации.	4	**3**
	2	Факторы обеспечения защиты информации от угроз воздействия утечки. Методы физической защиты информации. Способы и средства защиты информации от наблюдения. Методы противодействия радиолокальному и гидроакустическому наблюдению.	6	**3**
	3	Методы противодействия подслушиванию.	4	**3**
	4	Способы и средства предотвращения утечки информации через ПЭМИН. Способы предотвращения утечки информации по материально-вещественному каналу. Защита объектов от химической, радиационной и магнитометрической разведок, системы защиты от утечки информации по электросетевому каналу, моделирование объектов защиты и каналов утечки информации	4	**3**
	Практические работы			
	1	Типовые инженерные конструкции	4	**3**
	2	Способы и средства обнаружения злоумышленников и пожаров.	4	**3**
	3	Способы и средства видеоконтроля.	4	**3**
	4	Средства пожаротушения и тревожной сигнализации.	4	**3**
	5	Средства управления системой охраны.	4	**3**
	6	Маскировка в видимом и ИК диапазонах света.	4	**3**
	7	Активное подавление сигналов радиолокатора.	6	**3**

	8	Работа скремблеров и вокодеров.	4	**3**
	9	Энергетическое скрытие акустических сигналов: звукоизоляция и звукопоглощение.	4	**3**
	10	Применение генераторов акустического и вибрационного зашумления.	4	**3**
	11	Работа обнаружителей электромагнитного поля.	6	**3**
	12	Представление моделей объектов информационной безопасности.	6	**3**
	13	Определение путей проникновения злоумышленника к источнику информации.	4	**3**
	14	Типовые индикаторы каналов утечки.	4	**3**
	15	Комплексная система защиты.	4	**3**
Тема 1.4 Технические основы добывания и инженерно-технической защиты информации	**Содержание**			
	1.	Инженерно-техническая защита информации. Характеристика средств технической разведки. Возможности средств технической разведки.	4	**2**
	2	Акустические приемники. Диктофоны. Закладные устройства. Лазерные средства подслушивания.	4	**2**
	Лабораторные работы			
	1	Обнаружители и подавители диктофонов.	4	**2**
Тема 1.5Средства скрытого наблюдения	**Содержание**			
	1	Оптические системы. Визуально-оптические приборы. Фото и видео аппараты. Средства видеонаблюдения, видеоконтроля, видео охраны.	4	**2**
	Лабораторные работы			
	1	Структурная схема видеонаблюдения.	2	**2**
	2	Выбор оптимального устройства видеозаписи.	2	**2**
Тема 1.6 Средства перехвата сигналов	**Содержание**			
	1	Средства перехвата радиосигналов. Технические средства анализа сигналов.	4	**2**
	2	Средства определения координат источников радио сигналов и перехвата оптических и электрических сигналов. Определение координат источников радиоизлучений и анализа сигналов.	6	**3**
	3	Способы и средства уничтожения информации. Способы и средства стирания информации на магнитных носителях.	4	**2**
	4	Средства инженерной защиты. Инженерные конструкции.	4	**3**
	5	Ограждение территорий, зданий, помещений. Двери, окна, Ворота. Металлические сейфы,	4	**2**

		хранилища. Запирающие устройства.		
	6	Подходы к проектированию систем защиты информации. Принципы построения системы защиты информации.	4	**3**
	7	Методологические основы системы защиты информации. Методика определения состава защищаемой информации. Выявление каналов доступа к информации.	4	**2**
	8	Определение источников дестабилизирующего воздействия на информацию.	4	**3**
	9	Понятие модели объекта. Технологическое построение системы защиты информации. Кадровое обеспечение защиты информации. Кодекс корпоративного поведения. Нормативно-методическое обеспечение защиты информации. Управление системой защиты информации. Разработка системы ИТЗИ. Построение системы безопасности предприятия.	6	**3**
	Лабораторные работы			
	1	Комплексы обнаружения и пеленгации.	2	**3**
	2	Анализаторы телефонных линий.	2	**3**
	Самостоятельная работа		**46**	
	Систематическая проработка конспектов занятий, учебной литературы. Составление конспектов (таблиц, схем) по вопросам преподавателя. Подготовка к практическим работам. Написание рефератов. **Примерная тематика домашних заданий** **Написание рефератов по темам разделов:** «Направление комплексного проектирования систем защиты информации» «Основные проблемы реализации систем защиты информации» «Требования к КСЗИ» «Задачи стратегии защиты информации» «Верификация» «Дискреционный контроль доступа» «Биометрическая идентификация» «Биометрия по клавиатурному почерку» «Классификация признаков голоса и речи» «Средства высоконадежной биометрической аутентификации» «Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников» «Меры по защите информации внутри зоны» «Автоматическое обнаружение движущегося нарушителя» «Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведки»			

	«Контроль эффективности инженерно-технической защиты информации» «Пути оптимизации мер инженерно-технической защиты информации» Принципы оценки эффективности инженерно-технической защиты информации» «Источники опасных сигналов» «Типы побочных излучений и наводок, возможные «антенны»» «Помехи» «Физические основы побочных излучений и наводок» «Возможные наводки в аппаратуре» «Особенности распространения сигналов в помещениях» Ознакомление и литературой описывающей сканирующие приемники. Изучение инструкции сканера. Ознакомление с литературой описывающей нелинейные локаторы. Изучение инструкции нелинейного локаторы. Ознакомление с литературой и Интернет-ресурсами по теме космической и авиаразведки.			
	Консультации		**20**	
МДК.03.02 Физическая защита линий связи информационно-телекоммуникационных системах и сетях.				
Тема 1.1 Основные теории измерения	**Содержание**			
	1	Виды, методы и погрешности.	8	**2**
	2	Классификация измерительных приборов.	8	**2**
	Лабораторные работы			
	1	Инструктаж по технике безопасности при электрорадиоизмерениях.	8	
	2	Определение погрешности измерений.	8	
Тема 1.2 Измерение тока, напряжения и мощности	**Содержание**			
	1	Амперметры и вольтметры. Включение их в цепь.	8	
	Практические работы			
	1	Измерение параметров электрической цепи комбинированным прибором.	10	
	2	Измерение напряжений цифровым вольтметром.	10	
Тема 1.3. Приборы формирования стандартных	**Содержание**			
	1	Генераторы измерительные.	8	
	2	Генераторы шума.	8	

измерительных сигналов				
Тема 1.4 Исследование формы сигналов	**Содержание**			
	1	Универсальные осциллографы.	8	
	2	Способы отсчета напряжения и временных интервалов электрических сигналов.	8	
	Лабораторные работы			
	1	Исследование органов управления, включение и калибровки электронного осциллографа.	8	
	2	Изучение электронно-лучевых осциллографов со ждущей разверсткой.	8	
	3	Измерение параметров различных сигналов двухканальным осциллографом.	8	
Тема 1.5 Измерение параметров сигналов	**Содержание**			
	1	Методы измерения частоты и временных интервалов электрических сигналов.	8	
	Практические работы			
	1	Исследование технических характеристик, режимов работы и органов управления электронно-счётного частотомера.	12	
	2	Изучение Электронно-счётного осциллографа и применение их для измерения частоты сигналов.	12	
	3	Изучение затухающих электромагнитных колебаний.	10	
Тема 1.6 Измерение параметров и характеристик электрорадиотехнических цепей и компонентов.	**Содержание**			
	1	Измерение параметров с сосредоточенными параметрами.	8	
	2	Измерение АЧХ.	8	
	3	Измерение параметров полупроводниковых приборов.	8	
	Самостоятельная работа		46	
	Выполнение электрических расчетов Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя Проработка конспектов занятий, учебной и специальной технической литературы Написание отчетов Написание рефератов и подготовка сообщений по темам разделов			
	Консультации		22	
	Промежуточная аттестация		44	
	ИТОГО		267	
Учебная практика			36	

Виды работ:	Введение Изучение средств перехвата информации Микрофоны Акустические антенны Выбор типа микрофона и места его установки Изучение устройств подавления микрофонов Изучение устройств для перехвата речевой информации в проводных каналах Изучение оптико-акустической аппаратуры перехвата речевой информации Оптико-механические приборы Приборы ночного видения Средства скрытой фотосъемки Зоны подключения в линиях связи Перехват телефонных переговоров в зонах «А», «Б», «В», «Г», «Д», «Е» Изучение перехвата сообщений в каналах сотовой связи Методы поиска закладных устройств как физических объектов и электронных средств Панорамные приемники Аппаратура контроля и защиты линии связи Средства создания акустических и электромагнитных маскирующих помех Измерение токов, напряжений и сопротивлений, исследование двухполюсников с помощью мультиметра Прямые и косвенные однократные измерения Обработка и представление однократных измерений при наличии систематической погрешности Стандартная обработка результатов прямых измерений с многократным наблюдением Обработка результатов прямых измерений с многократным наблюдением при наличии грубых погрешностей Определение погрешности цифрового вольтметра сличения и прямых измерений Измерение мощности и силы постоянного электромагнитного тока Измерение постоянного напряжения методом компенсации Измерение переменного электрического напряжения Измерение частоты и периода электрических сигналов Терморезисторные измерительные преобразователи. Измерители температуры Емкостные измерительные преобразователи. Измерение размера Индуктивные измерительные преобразователи. Измерение перемещения Термоэлектрические измерительные преобразователи. Измерение температуры Пьезоэлектрические измерительные преобразователи. Измерение переменных ускорений		
Производственная практика		144	

Виды работ:	Выполнение подбора, настройки и применения технических средств защиты информации Использование средств охраны и безопасности объекта Организация и реализация технической охраны объектов Выполнение мероприятий по предотвращению несанкционированного доступа к информации Настройка системы защиты информации от съема и утечки по техническим каналам Изучение порядка применения нормативных правовых актов Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами Выявление технических каналов утечки информации Применение существующих способов выявления опасности целостности информации Анализ объектов информатизации предприятий, учреждений, организаций Анализ ресурсов обеспечения инженерно-технической защиты информации Изучение основных этапов проектирования системы защиты информации техническими средствами Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД Оформление технической и технологической документации		
	ИТОГО (с учетом практик)	782	

5. Образовательные технологии

Результаты освоения профессионального модуля достигаются за счет использования в процессе обучения современных инструментальных средств: лекции с применением мультимедийных технологий, практические занятия с использованием соответствующего оборудования.

При проведении занятий используются активные и интерактивные формы. В таблице приведено описание образовательных технологий, используемых в данном модуле.

Методы и формы организации обучения (ФОО)

МДК 03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

ФОО / Методы	Лекция	Пр.раб
Работа в команде		Тема 1.1. Объекты информационной защиты
Беседа	Тема 1.4 Технические основы добывания и инженерно-технической защиты информации	

МДК 03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей

ФОО / Методы	Лекция	Пр.раб
Работа в команде		Тема 1.1 Основные теории измерения
Беседа	Тема 1.4 Исследование формы сигналов	

6. Требования к минимальному материально-техническому обеспечению

Занятия по профессиональному модулю проводятся в учебной аудитории, компьютерном классе

Оснащения кабинета:Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, персональные компьютеры

Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, доска, мультимедиа-проектор, проекционный экран, ПК.

7. Учебно-методическое и информационное обеспечение дисциплины

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Гаврилов, М. В. Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Профессиональное

образование). — ISBN 978-5-534-03051-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449286

2. Зверева, В. П. Технические средства информатизации : учебник / В. П. Зверева, А. В. Назаров. - Москва : КУРС : ИНФРА-М, 2021. - 256 с. - (Среднее профессиональное образование). - ISBN 978-5-906818-88-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1214881

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356

Дополнительная литература

4. Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 c. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87882.html

5. Разработка и защита баз данных в Microsoft SQL Server 2005 : учебное пособие для СПО / . — Саратов : Профобразование, 2019. — 148 c. — ISBN 978-5-4488-0366-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86207.html

6. Аминев, А. В. Основы радиоэлектроники: измерения в телекоммуникационных системах : учебное пособие для среднего профессионального образования / А. В. Аминев, А. В. Блохин ; под общей редакцией А. В. Блохина. — Москва : Издательство Юрайт, 2020. — 223 с. — (Профессиональное образование). — ISBN 978-5-534-10395-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456593

7. Шишмарёв, В. Ю. Электрорадиоизмерения. Практикум : практическое пособие для среднего профессионального образования / В. Ю. Шишмарёв. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 234 с. — (Профессиональное образование). — ISBN 978-5-534-08588-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454371

8. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты: сб. учеб.- метод. материалов для специальностей: 10.02.04 «Обеспечение информационной безопасности в телекоммуникационных системах», / АмГУ, ФСПО; сост. С.А. Панов. – Благовещенск: Изд-во Амур. гос. ун-та, 2018.- 10 с.. Режим доступа: http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/10139.pdf

Перечень программного обеспечения

Операционная система MS Windows 7 Pro - DreamSparkPremiumElectronicSoftwareDeliveryRenewal по договору - Сублицензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года

Autodesk Product Design Suite Ultimate 2014-2017 AutoCAD - Электроннаялицензия Education Network license Multi-user 3000 concurrent users

"MS Visio 2010 - DreamSpark Premium Electronic Software Delivery Renewal подоговору – Сублицензионныйдоговор № Tr000074357/KHB 17 от 01 марта 2016 года"

Система защиты информации от несанкционированного доступа DallasLock - Договор о сотрудничестве с образовательным учреждением 127-17-153/1

Операционная система специального назначения «AstraLinuxSpecialEdition» РУСБ.10015-01 - Лицензионный договор № РБТ-14/1607-01-ВУЗ на предоставление права использования программы для ЭВМ

MaxPatrolEducation - Лицензионный договор № 003-17/EM

XSpiderEducation - Лицензионный договор № 005-17/EXОперационная система WindowsServer 2008 - DreamSparkPremiumElectronicSoftwareDeliveryRenewal по договору - Субли-цензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года, Операционная система MS Windows XP SP3 - DreamSparkPremiumElectronicSoftwareDeliveryRenewal по договору - Субли-цензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года

8. Контроль и оценка результатов освоения учебной дисциплины

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты (освоенные профессиональные компетенции)	**Формы и методы контроля и оценки**
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.	экспертная оценка выполнения практической работы
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.	экспертная оценка выполнения практической работы установке программного обеспечения
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения
ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.	Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения
Промежуточная аттестация	**Другие формы контроля, экзамен, дифференцированный зачет, экзамен по модулю**