Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет им. Г.В. Плеханова»
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

РАБОЧАЯ ПРОГРАММА

Дисциплина: ПМ.03 Защита информации техническими средствами

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация: Техник по защите информации

2019 г.

СОГЛАСОВАНА:

Цикловой методической комиссией «Профессиональных модулей 10.02.05»

Разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация: техник по защите информации

Протокол № 14-18/19-ЗК

от «03» июля 2019 года

Председатель цикловой методической комиссии

_____

М.А. Молотков

Заместитель директора по учебной работе _____ Д.А. Клопов

подпись

РАССМОТРЕННА И ОДОБРЕНА

_____

_____ _____ С.Г. Ахмадеев

подпись

УТВЕРЖДЕНА:

Директор техникума _____ А.В. Чурилов

подпись

Составители (авторы):

Молотков Максим Алексеевич, преподаватель ФГБОУ ВО «РЭУ им. Г.В. Плеханова»,

Прищеп Михаил Сергеевич, преподаватель ФГБОУ ВО «РЭУ им. Г.В. Плеханова»,

Кузнецов Павел Олегович, преподаватель ФГБОУ ВО «РЭУ им. Г.В. Плеханова»,

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации техническими средствами

1.1. Область применения рабочей программы

Программа профессионального модуля (далее - программа) - является частью программы подготовки специалистов среднего звена (далее - ППССЗ) в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

ФГОС по специальностям СПО и соответствующих профессиональных компетенций (ПК):

- ПК 2.1. - Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
- ПК 2.2. - Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
- ПК 2.3. - Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
- ПК 2.4. - Осуществлять обработку, хранение и передачу информации ограниченного доступа.
- ПК 2.5. - Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
- ПК 2.6. - Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2. Цель и планируемые результаты освоения профессионального модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

Иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

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

Уметь:

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

Знать:

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

- основные способы физической защиты объектов информатизации;
- номенклатуру применяемых средств физической защиты объектов информатизации.

1.3 Количество часов на освоение программы профессионального модуля:

всего – 613 часов, в том числе:

максимальной учебной нагрузки обучающегося – 595 часа, включая:

обязательной аудиторной учебной нагрузки обучающегося – 451 часов; самостоятельной работы обучающегося – 0 часов;

консультации – 6 часов;

промежуточная аттестация – 12 часов,

включая:

экзамен (Техническая защита информации, 6 семестр) - 8 часов
Экзамен по профессиональному модулю (8 семестр) - 4 часов

учебной и производственной практики – 180 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности Защита информации техническими средствами, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
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.
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное

	поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план 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	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов если предусмотрена рассредоточенная практика)
			Всего	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		
ПК 3.1- ПК.3.4 ОК 1– ОК10	МДК 03.01 Техническая защита информации	272	256	148	-	2	-	-	-
ПК 3.5 ОК 01–ОК10	МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	157	157	83	-	-	-		
ПК 3.1- ПК.3.5 ОК 1– ОК10	ПП.03.01 Производственная практика	72	72	-	-	-	-	-	72

**

ПК 3.1- ПК.3.5 ОК 1– ОК10	УП.03.01 Учебная практика	108	108	-	-	-	-	108	-
	консультации – 6 часов; промежуточная аттестация – 12 часов, включая: экзамен (Техническая защита информации, 6 семестр) - 8 часов экзамен по профессиональному модулю (8 семестр) - 4 часа								
	Всего:	613	593	231	-	2	-	108	72

3.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов	Уровень освоения
Раздел 1 модуля. Применение технической защиты информации			
МДК.03.01 Техническая защита информации		**272**	**-**
Раздел 1. Концепция инженерно-технической защиты информации		**10**	
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**4**	**1**
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.		
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**6**	
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.		
Раздел 2. Теоретические основы инженерно-технической защиты информации		**48**	**-**
Тема 2.1. Информация как предмет защиты	**Содержание**	**6**	**1**
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №1 Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		
Тема 2.2.	**Содержание**	**6**	**1**

Технические каналы утечки информации	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №2 Технические каналы утечки информации.		
Тема 2.3. Методы и средства технической разведки	**Содержание**	**6**	**1**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №3 Методы и средства технической разведки		
Раздел 3. Физические основы технической защиты информации		**34**	**-**
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**10**	**1**
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №4 Измерение параметров физических полей		
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**4**	**1**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №5 Физические процессы при подавлении опасных сигналов		
Раздел 4. Системы защиты от утечки информации		**112**	**-**
Тема 4.1. Системы защиты от утечки информации по	**Содержание**	**6**	**1**
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты		

акустическому каналу	информации от несанкционированной утечки по акустическому каналу.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа № 6 Защита от утечки по акустическому каналу		
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**6**	**1**
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №7 Системы защиты от утечки информации по проводному каналу		
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**6**	**1**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №8 Защита от утечки по виброакустическому каналу		
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**6**	**1**
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Тематика практических занятий и лабораторных работ	**12**	**2**
	Практическая работа №9. Определение каналов утечки ПЭМИН Защита от утечки по цепям электропитания и заземления		
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**6**	**1**
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.		

	Тематика практических занятий и лабораторных работ	**10**	**2**
	Практическая работа №10 Системы защиты от утечки информации по телефонному каналу		
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**6**	**1**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		
	Тематика практических занятий и лабораторных работ	**8**	**2**
	Практическая работа №11 Системы защиты от утечки информации по электросетевому каналу		
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**8**	**1**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		
	Тематика практических занятий и лабораторных работ	**8**	**2**
	Практическая работа №12 Системы защиты от утечки информации по оптическому каналу		
Раздел 5. Применение и эксплуатация технических средств защиты информации		**54**	**-**
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**12**	**1**
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
	Тематика практических занятий и лабораторных работ	**14**	**2**
	Практическая работа №13 Применение технических средств защиты информации		
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**10**	**1**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов		

	информатизации.		
	Тематика практических занятий и лабораторных работ	**16**	**2**
	Практическая работа №14 Эксплуатация инженерно-технических средств физической защиты		
	Самостоятельная работа	**2**	
Консультация **Промежуточная аттестация, включая:** **экзамен (Техническая защита информации, 6 семестр)** **диф. Зачет (8 семестр)** **другая форма аттестации (7 семестр)**			
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации			
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**157**	
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		**34**	**-**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**8**	**1**
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.		
	Тематика практических занятий и лабораторных работ	**6**	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно		
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**8**	**1**
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.		
	Тематика практических занятий и лабораторных работ	**12**	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно		
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		**81**	**-**
Тема 2.1 Система обнаружения	**Содержание**	**8**	**1**
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения		

комплекса инженерно-технических средств	безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.		
	Тематика практических занятий и лабораторных работ	**12**	**2**
	Монтаж датчиков пожарной и охранной сигнализации		
Тема 2.2. Система контроля и управления доступом	**Содержание**	**10**	**1**
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.		
	Тематика практических занятий и лабораторных работ	**9**	**2**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя		
	Рассмотрение принципов устройства, работы и применения средств контроля доступа		
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**8**	**1**
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.		
	Тематика практических занятий и лабораторных работ	**8**	**2**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**6**	**1**
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.		
	Тематика практических занятий и лабораторных работ	**6**	**2**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		
Тема 2.5 Система воздействия	**Содержание**	**6**	**1**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.		
	Тематика практических занятий и лабораторных работ	**8**	**2**

	Тематика учебных занятий формируется образовательной организацией самостоятельно		
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		**42**	**-**
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание**	**8**	**1**
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.		
	Тематика практических занятий и лабораторных работ	**10**	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно		
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**12**	**1**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.		
	Тематика практических занятий и лабораторных работ	**12**	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно		
Диф.зачет (8 семестра) **Другие формы аттестации (6 и 7 семестры)**			
Учебная практика **Виды работ:** - Измерение параметров физических полей. - Определение каналов утечки ПЭМИН. - Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. - Установка и настройка технических средств защиты информации. - Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. **Учебная практика по разделу 2 модуля** **1.** Монтаж различных типов датчиков. **2.** Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. **3.** Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для		**108**	***2***

защиты информации. **4.** Рассмотрение системы контроля и управления доступом. **5.** Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. **6.** Рассмотрение датчиков периметра, их принципов работы. **7.** Выполнение звукоизоляции помещений системы зашумления. **8.** Реализация защиты от утечки по цепям электропитания и заземления. **9.** Разработка организационных и технических мероприятий по заданию преподавателя. **10.** Разработка основной документации по инженерно-технической защите информации.		
Диф.зачет (6 семестр)		
Производственная практика профессионального модуля **Виды работ** **1.** Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; **2.** Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; **3.** Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; **4.** Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	**72**	***2***
Диф.зачет (7 семестр)		
Консультация – 6 часов Промежуточная аттестация – 12 часов, Включая: МДК.03.01 Техническая защита информации - экзамен (6 семестр) – 8 часов ПМ.03.Э Экзамен по профессиональному модулю (8 семестр) – 4 часа		
УП.03.01 Учебная практика	**72**	
ПП.03.01 Производственная практика	**108**	
ВСЕГО	**613**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (узнавание ранее изученных объектов, свойств);

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

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

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие:

- Лаборатория технических средств защиты информации

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	15 автоматизированных рабочих мест для обучающихся и 1 рабочее место для преподавателя с конфигурацией: Процессор Intel Core i5, оперативная память объемом 8 Гб, жесткий диск - 500 Гб, монитор 23", мышь, клавиатура;	Проектор 1 шт	29
2	столов 17 шт	коммутаторы 2 шт,	
3	стульев 29 шт		
4	сетевой шкаф 1шт		
5	доска 1 шт		
6	экран проектора 1шт		
7	стенды 1 шт		
8	Аппаратные средства аутентификации пользователя: Учебно-практический стенд «Системы контроля и управления доступом» ФЗИ-СКУД (1 штука) Средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок		
9	Лабораторный стенд "Защита информации от утечек по акустовибрационным каналам", ТЗИ-АКУСТОВБР (1 штука) Средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.);		
10	П3-34 Измеритель параметров электромагнитного поля. АП 3-34 Е УКВ (10 штук)		
11	Учебно-практический стенд «Системы видеонаблюдения» ФЗИ-VIDEO (1 штука)		
12	АССИСТЕНТ V1 (10 штук)		

	Стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов:		
13	Учебно-практический стенд «Системы контроля и управления доступом» ФЗИ-СКУД (1 штука)		

Программное обеспечение:

Windows 10 pro, Microsoft Office 2016, visio, 1С Предприятие; Visual Studio 2019; arduino, unity,php, Notepad++, XAMP, Pascal ABC.net, SQL Server, Adobe Photoshop, Adobe Illustrator, AutoCAD, Autodesk, ColerDraw, Mozila Firefox, Microsoft Edge, Google Chrome

- Лаборатория технических средств информатизации, или лаборатория информационных технологий и/или мастерская по наладке технологического оборудования по профилю выбираемой рабочей профессии

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	14 автоматизированных рабочих мест для обучающихся и 1 рабочее место для преподавателя с конфигурацией: Процессор Intel Core i5, оперативная память объемом 8 Гб, дискретная видеокарта, жесткий диск - 1 Тб, монитор 23", мышь, клавиатура;	проекторы - 1 шт,	32
2	Парты - 10 шт,		
3	стулья - 32 шт,		
4	стол преподавателя - 1 шт,		
5	доска маркерная - 1 шт,		
6	сетевой шкаф - 1 шт,		
7	Экран проектора – 1 шт		

Программное обеспечение:

Windows 10 pro,Microsoft Office 2016, Visio 2016,Visual Studio 2019, 1 С предприятие 8 (учебная версия), PascalABC.net, XAMPP, Unity,Python, notepad++, arduino,MongoDB, MySql, SqlServer,Adobe Photoshop, Adobe illustrator, Corel Draw, Autodesk 3d mask, autocad 2019,Mozila Firefox, Google Chrome, Explore

- Лаборатория информационных технологий, программирования и баз данных

№ п/п	**Оборудование**	**Технические средства**	**Количество рабочих**

		обучения	мест
1	9 автоматизированных рабочих мест для обучающихся и 1 рабочее место для преподавателя с конфигурацией: Процессор Intel Core i5, оперативная память объемом 8 Гб, дискретная видеокарта, жесткий диск - 1 Тб, монитор 23", мышь, клавиатура;	проектор 1	28
2	3 автоматизированных рабочих места для обучающихся с конфигурацией: Процессор Intel Core i7, оперативная память объемом 16 Гб, жесткий диск - 1 Тб, твердотельный накопитель - 256 Гб, монитор 23", мышь, клавиатура		
3	столов 11		
4	стульев 28		
5	шкафы 1		
6	маркерная доска 1		
7	стенды 1		

Программное обеспечение:

Windows 10 pro, Microsoft Office 2016, Visio 2016, Visual Studio 2019, 1С предприятие 8 (учебная версия), PascalABC.net, XAMPP, Unity, Python, notepad++, arduino, Android Studio, MySQL, T-SQL, SQL Server, Adobe Photoshop, Adobe Illustrator, AutoCAD, Autodesk, ColerDraw, Mozila Firefox, Microsoft Edge, Google Chrome

4.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. - Москва: Гор. линия-Телеком, 2016. - 616 с.: ISBN 978-5-9912-0084-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/560580
2. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...: Уч. пос./Новиков В.К. - Москва: Гор. линия-Телеком, 2015.- 176с. (О)ISBN 978-5-9912-0525-2, 500 экз. - Текст: электронный. - URL: https://znanium.com/catalog/product/536932
3. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2015.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений. https://znanium.com/bookread2.php?book=562922

Дополнительные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/ IEC 15408-2:2008). Росстандарт, 2013.

42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и

виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

Профессиональные базы данных и справочные системы

- Федеральная служба государственной статистики - https://rosstat.gov.ru/
- Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
- Информационно-справочная система "КонсультантПлюс"

4.3. Общие требования к организации образовательного процесса

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам):

Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии).

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях направление деятельности которых соответствует области профессиональной деятельности, указанной в пункте 1.5 настоящего ФГОС СПО, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности, указанной в пункте 1.5 настоящего ФГОС СПО, в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 процентов.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой Инженерно-педагогический состав:

Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии).

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях направление деятельности которых соответствует области профессиональной деятельности, указанной в пункте 1.5 настоящего ФГОС СПО, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности, указанной в пункте 1.5 настоящего ФГОС СПО, в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 процентов.

Мастера: не предусмотрены

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен по ПМ, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен по ПМ, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен по ПМ, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также	Проводить самостоятельные измерения параметров	тестирование, экзамен по ПМ, экспертное наблюдение выполнения

физических полей, создаваемых техническими средствами защиты информации	фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен по ПМ, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

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
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	учебной и производственной практикам Экзамен по ПМ
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	

физической подготовленности.		
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

Разработчики:

1. Молотков Максим Алексеевич, преподаватель ФГБОУ ВО «РЭУ им. Г.В. Плеханова»
2. Прищеп Михаил Сергеевич, преподаватель ФГБОУ ВО «РЭУ им. Г.В. Плеханова»
3. Кузнецов Павел Олегович, преподаватель ФГБОУ ВО «РЭУ им. Г.В. Плеханова»

Эксперты:

_____

(место работы) (занимаемая должность) (инициалы, фамилия)

_____

(место работы) (занимаемая должность) (инициалы, фамилия)