

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»
Московский приборостроительный техникум

РАБОЧАЯ ПРОГРАММА

Учебная практика УП.03.01 Учебная практика

Профессиональный модуль ПМ.03 Защита информации техническими средствами

Код, специальность 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

СОГЛАСОВАНА:
Цикловой методической
комиссией
«10.02.05
Профессиональных
модулей»

Протокол № 6-21/22 ЗК
от «15» января 2022 года

Разработана на основе Федерального государственного
образовательного стандарта по специальности среднего
профессионального образования
специальность: 10.02.05 Обеспечение информационной
безопасности автоматизированных систем
квалификация: техник по защите информации

**Председатель цикловой
методической комиссии**



Подпись Инициалы Фамилия
М.А. Молотков

Заместитель директора по учебной работе



Подпись Инициалы Фамилия
Д.А. Клопов

УТВЕРЖДЕНА:
Директор техникума



Подпись Инициалы Фамилия
А.В. Чурилов

Составители (авторы):

Прищеп Михаил Сергеевич, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова
Молотков Максим Алексеевич, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова

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

СОГЛАСОВАНО: 
представитель работодателя

Рецензент: _____

Ф.И.О., ученая степень, звание, должность, наименование

СОДЕРЖАНИЕ

	Стр.
1. Паспорт программы практики.....	4
2. Результаты практики	9
3. Структура и содержание практики.....	10
4. Условия реализации программы практики	14
5. Контроль и оценка результатов освоения практики.....	17

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Область применения программы

Рабочая программа учебной практики является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, квалификация: техник по защите информации в части освоения основного вида профессиональной деятельности Защита информации техническими средствами

1.2. Цели и задачи учебной практики:

Формирование у обучающихся первоначальных практических профессиональных умений в рамках модулей ППССЗ по основным видам деятельности для освоения методов и приемов практического применения прикладных программных продуктов для программного обеспечения компьютерных систем

1.3. Требования к результатам освоения учебной практики

В результате прохождения учебной практики по виду профессиональной деятельности обучающихся 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

1.4 Количество часов на освоение рабочей программы учебной практики:

Всего - 108 часов, в том числе:

В рамках освоения ПМ.03 – 108 часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ.03 по основному виду деятельности Защита информации техническими средствами необходимых для последующего освоения ими профессиональных компетенций по специальности

Код	Наименование результата освоения практики
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.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Код ПК	Код и наименование профессионального модуля	Количество часов по ПМ	Виды работ	Наименования тем учебной практики	Количество часов по темам
1	2	3		4	5
ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5.	ПМ.03 Защита информации техническими средствами	108	<ul style="list-style-type: none"> – 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. – Монтаж различных типов датчиков. – Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. – Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации. – Рассмотрение системы контроля и управления доступом. – Рассмотрение принципов работы системы видеонаблюдения и ее 	<p>Раздел 1 модуля. Применение технической защиты информации</p> <p>Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации</p>	<p>54</p> <p>54</p>

			<p>проектирование.</p> <ul style="list-style-type: none"> – Рассмотрение датчиков периметра, их принципов работы. – Выполнение звукоизоляции помещений системы шумления. – Реализация защиты от утечки по цепям электропитания и заземления. – Разработка организационных и технических мероприятий по заданию преподавателя; – Разработка основной документации по инженерно-технической защите информации. 		
	ВСЕГО часов	108			108

3.2. Содержание учебной практики

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов
1	2	3
ПМ.03 Защита информации техническими средствами		108
Раздел 1 модуля. Применение технической защиты информации	<p>Содержание</p> <p>Измерение параметров физических полей.</p> <p>Определение каналов утечки ПЭМИН.</p> <p>Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</p> <p>Установка и настройка технических средств защиты информации.</p> <p>Проведение измерений параметров побочных электромагнитных излучений и наводок.</p> <p>Проведение аттестации объектов информатизации.</p>	54
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации	<p>Содержание</p> <p>Монтаж различных типов датчиков.</p> <p>Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.</p> <p>Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.</p> <p>Рассмотрение системы контроля и управления доступом.</p> <p>Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.</p> <p>Рассмотрение датчиков периметра, их принципов работы.</p> <p>Выполнение звукоизоляции помещений системы зашумления.</p> <p>Реализация защиты от утечки по цепям электропитания и заземления.</p> <p>Разработка организационных и технических мероприятий по заданию преподавателя;</p> <p>Разработка основной документации по инженерно-технической защите информации.</p>	54

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

- **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	15
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 (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок		
9	Лабораторный стенд "Защита информации от утечек по акустиковибрационным каналам", ТЗИ-АКУСТОВБР (1 штука) Средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.);		
10	ПЗ-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, оснащенные 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, Mozilla 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,	14
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 3ds Max, AutoCAD 2019, Mozilla Firefox, Google Chrome, Explorer

- **Лаборатория информационных технологий, программирования и баз данных**

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	10 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	13
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, CorelDraw, Mozilla Firefox, Microsoft Edge, Google Chrome

4.2 Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

Печатные издания не используются. ПМ полностью обеспечен электронными изданиями.

4.2.1 Печатные издания

ОСНОВНЫЕ не используются

ДОПОЛНИТЕЛЬНЫЕ не используются

4.2.2 Электронные издания

1. [Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.](http://znanium.com/catalog/product/560580) Технические средства и методы защиты информации. 7-е изд., испр. 2017.
<http://znanium.com/catalog/product/560580>
2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с.
<https://znanium.com/catalog/product/536932>
3. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности (1-е изд.), М. Академия, 2017
<https://academia-library.ru/catalogue/4831/293834/>

4.2.3 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 июня 1995 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.

4.2.4 Электронные ресурсы:

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» <http://www.ict.edu.ru>
9. Сайт Научной электронной библиотеки www.elibrary.ru

4.2.5 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"

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляются руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий. В результате освоения учебной практики в рамках профессиональных модулей обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 3.1 Осуществлять установку,	Демонстрировать умения и	оценка процесса и

монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	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	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	оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	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	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

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	наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка при выполнении работ по учебной практике
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
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, применять стандарты антикоррупционного поведения.	- 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	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	

поддержание необходимого уровня 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.	