МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАБАРДИНО – БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ.Х.М.БЕРБЕКОВА»

Колледж информационных технологий и экономики

СОГЛАСОВАНО
Председатель Федерального
государственного бюджетного
научного учреждения «Федеральный
научный центр «Кабардино-Балкарский
научный центр Российской Академии наук»»
_____ З.В. Нагоев
«10» 06 2021 г.

УТВЕРЖДАЮ
Зам.директора по учебно-
производственной работе колледжа
информационных технологий и
экономики
_____ Гажев А.А.
«10» 06 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

(УП.03 Учебная практика)

ПМ.03 Защита информации техническими средствами

Программа подготовки специалистов среднего звена

10.02.05 - Обеспечение информационной безопасности автоматизированных систем

Среднее профессиональное образование

Квалификация выпускника
Техник по защите информации

Очная форма обучения

Нальчик, 2021 г.

Рабочая программа учебной практики по профессиональному модулю ПМ.03 Защита информации техническими средствами разработана на основании федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (базовая подготовка), утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. №1553., учебного плана по специальности Обеспечение информационной безопасности автоматизированных систем.

Разработчик:
Тлупов З.А., преподаватель

Рабочая программа профессионального модуля обсуждена и утверждена на заседании ЦК программирования и информационной безопасности

Протокол № 10 от « 10 » 06 2021 года.

Председатель ЦК _____ Эдгулова Е.К.

Содержание

I. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРКТИКИ
ПМ.03 Защита информации техническими средствами.

1.1. Область применения программы

Рабочая программа учебной практики – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности (ВПД): Защита информации техническими средствами. и соответствующих профессиональных компетенций (ПК3.1-ПК 3.5).

1.2. Место программы учебной практики в структуре программы подготовки специалистов среднего звена:

Рабочая программа учебной практики входит в профессиональный модуль ПМ.03 Защита информации техническими средствами.

1.3. Цели и задачи учебной практики – требования к результатам освоения практики.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной практики 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.

1.4. Количество часов на освоение учебной практики: – 72 ч.

II. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРАКТИКИ

Результатом освоения программы практики является овладение обучающимися видом 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.

III. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

Код ПК	Код и наименование профессиональных модулей, код и наименование МДК	Количество часов на учебную практику по ПМ и соответствующим МДК	Виды работ	Наименование тем учебной практики	Количество часов по темам	Уровень освоения
1	2	3	4	5	6	7
ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4	**ПМ.03 Защита информации техническими средствами**	**72**			**72**	
ПК 3.5	**МДК.03.01 Техническая защита информации**	**36**	1. Инструктаж по технике безопасности. 2. Назначение. Функциональная схема лаборатории технических средств защиты информации. 3. Монтаж различных типов датчиков. 4. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 5. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для	**Тема 1. Физические основы технической защиты информации.** 1. Утечки информации по каналам побочных электромагнитных излучений и наводок. 2. Физические процессы при подавлении опасных сигналов.	10	3
				Тема 2. Системы защиты от утечки информации. 1. Системы защиты от утечки информации по акустическому каналу. 2. Системы защиты от утечки информации по проводному каналу. 3. Системы защиты от утечки информации по вибрационному каналу 4. Системы защиты от утечки информации по электромагнитному каналу 5. Системы защиты от утечки информации по телефонному каналу 6. Системы защиты от утечки информации по электросетевому каналу 7. Системы защиты от утечки информации по оптическому каналу	16	3

			защиты ин- формации. 6. Рассмотрение системы контроля и управления доступом. 7. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 8. Рассмотрение датчиков периметра, их принципов работы.	**Тема 3. Эксплуатация технических средств защиты информации.** 1. Назначение технических средств защиты информации. 2. Эксплуатация технических средств защиты информации.	10	3
	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	**36**	10. Выполнение звукоизоляции помещений системы зашумления. 11. Реализация защиты от утечки по цепям электропитания и заземления. 12. Разработка организационных и технических мероприятий по заданию преподавателя; 13. Разработка основной документации по инженерно- технической защите информации.	**Тема 1. Компоненты комплекса инженерно- технических средств физической защиты** 1. Разновидность, назначение и построение систем обнаружения. 2. Периферийное оборудование систем контроля и управления доступом. 3. Оборудование систем телевизионного наблюдения. 4. Элементы систем сбора, обработки, отображения и документирования информации	18	3
				Тема 2. Эксплуатация инженерно-технических средств физической защиты. 1. Монтаж, обслуживание и эксплуатация технических средств защиты информации. 2. Монтаж, обслуживание и эксплуатация средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения. 3. Монтаж, обслуживание и эксплуатация средств защиты информации от несанкционированного съёма и утечки по техническим каналам. 4. Разработка основной документации по инженерно- технической защите информации.	18	3
	Всего часов	**72**			**72**	

Для характеристики уровня освоения учебного материала используются следующие обозначения: 2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

IV. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы учебной практики предполагает наличие:
- лаборатории технических средств защиты информации.

Оборудование кабинета и рабочих мест лаборатории **технических средств защиты информации**:

- аппаратные средства аутентификации пользователя;
- средства защиты информации от утечки по акустическому (виброаккустическому) ка- налу и каналу побочных электромагнитных излучений и наводок;
- средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.);
- стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов.

4.2. Информационное обеспечение обучения

Основные печатные источники:

1. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации / составители И. А. Денисов. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/61529.html
2. Ажмухамедов, И. М. Основы организационно-правового обеспечения информацион- ной безопасности : учебное пособие / И. М. Ажмухамедов, О. М. Князева ; под редакацией Т. С. Кулакова. — СПб. : Интермедия, 2017. — 264 с. — ISBN 978-5-4383-0160-— Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. URL: http://www.iprbookshop.ru/73643.html
3. Учебно-методическое пособие по выполнению курсового проекта по дисциплине Методы и средства защиты информации / составители А. Н. Руднев. — М. : Московский технический университет связи и информатики, 2016. — 29 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/61496.html
4. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно- методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 с. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/77317.html

Дополнительные печатные источники:

1. Горев, А. И. Обработка и защита информации в компьютерных системах : учебно- практическое пособие / А. И. Горев, А. А. Симаков. — Омск : Омская академия МВД России, 2016. — 88 с. — ISBN 978-5-88651-642-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72856.html
2. Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 368 с. — ISBN 2227-8397. —

3. Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/73732.html
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
7. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
8. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
9. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
10. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
11. 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 об- мена».
12. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
13. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правиельства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
14. 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.
15. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
16. 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.
17. 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.
18. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
19. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
20. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
21. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

22. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
23. 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 не декларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
24. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
25. 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
26. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
27. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
28. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
29. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
30. 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
31. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
32. 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
33. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита ин- формации. Процессы формирования и проверки электронной цифровой подписи"
34. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
35. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
36. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
37. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
38. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищен- ном исполнении. Общие требования. Госстандарт России, 2000.
39. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

40. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
41. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищен- ном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
42. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищен- ном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
43. 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.
44. 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.
45. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
46. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
48. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
49. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
50. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
51. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
52. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
53. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
54. программное обеспечение: специализированное программное обеспечение для про- верки защищенности помещений от утечки информации по акустическому и вибро-акустическому каналам, специальных исследований средств вычислительной техники;
55. 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

V. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ.

В результате освоения учебной практики студент должен знать и уметь:

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	Правильность выполнения установки и монтажа технических средств защиты информации; Правильность и точность настройки технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	− Накопительная оценка результатов выполнения практических работ на учебной практике. − Качество решения практических заданий. − Оценка защиты отчета по учебной практике. **Уметь** - применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Степень умения и уровень практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	− Накопительная оценка результатов выполнения практических работ на учебной практике. − Качество решения практических заданий. − Оценка защиты отчета по учебной практике. **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.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Качество выполнения работ по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки ин- формации ограниченного доступа	− Накопительная оценка результатов выполнения практических работ на учебной практике. − Качество решения практических заданий. − Оценка защиты отчета по учебной практике. **Уметь** - применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты ин- формации	Владение методами измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	− Накопительная оценка результатов выполнения практических работ на учебной практике. − Качество решения практических заданий. − Оценка защиты отчета по учебной практике. **Уметь** - применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявление знаний и умений в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	− Накопительная оценка результатов выполнения практических работ на учебной практике. − Качество решения практических заданий. − Оценка защиты отчета по учебной практике. **Уметь** - применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; - применять инженерно-технические средства физической защиты объектов информатизации.

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 1. 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	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике
ОК 2. 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	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике
ОК 4. 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)	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной

		практике
ОК 5. 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	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике
ОК 6. 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,	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике
ОК 7. 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	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике
ОК 9. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	− Накопительная оценка результатов выполнения практических работ на учебной практике − Качество решения практических заданий − Оценка защиты отчета по учебной практике

Критерии оценивания учебной практики

Дифференцированный зачет по учебной практике выставляется на основании отчета по выполненным за время практики работам. Оценивается их объем, качество выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

Оценка **«5»** ставится, если верно и рационально решено 90%-100% предлагаемых заданий, допустим 1 недочет, неискажающий сути решения.

Оценка **«4»** ставится при безошибочном решении 80% предлагаемых заданий.

Оценка **«3»** ставится, если выполнено 60% предлагаемых заданий, допустим 1 недочет.

Оценка **«2»** - решено менее 60% предлагаемых заданий.