Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Кабардино-Балкарский государственный университет
им. Х.М. Бербекова»
Колледж информационных технологий и экономики

СОГЛАСОВАНО

Директор института информатики и проблем регионального управления КБНЦ РАН
_____/Т.Х.Иванов /
«03» ____04____ 2019 г.

УТВЕРЖДАЮ

Зам.директора по учебно-производственной работе колледжа информационных технологий и экономики
_____/А.А. Гажев/
«03» _____04_____ 2019 г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

(ПП.03 по профилю специальности)

ПМ.03 Защита информации техническими средствами

Программа подготовки специалистов среднего звена специальности

10.02.05 – Обеспечение информационной безопасности в автоматизированных системах

Среднее профессиональное образование

Квалификация выпускника
Техник по защите информации

Очная форма обучения

Нальчик, 2019

Рабочая программа производственной практики по профессиональному модулю разработана на основании Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. № 1553, учебного плана по программе подготовки специалистов среднего звена.

Разработчик: Тлупов З.А., преподаватель

Рабочая программа учебной дисциплины рассмотрена и одобрена на заседании ЦК «Программирование и информационная безопасность»

Протокол № 6 от «20» 06 2019 г.

Председатель ЦК _____ Е. К. Эдгулова

Согласовано

Научная библиотека КБГУ,
отдел комплектования _____ Губжокова Н.А.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

Производственная практика ПМ.03 Защита информации техническими средствами.

1.1 Область применения программы

Программа производственной практики является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности Защита информации техническими средствами.

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

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

1.3 Цели и задачи производственной практики

Производственная практика является обязательным компонентом профессионального модуля «Защита информации техническими средствами» для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, обуславливающим умения и навыки для профессиональной деятельности выпускника.

В результате прохождения практики студент 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 по учебному плану производственной практики:

Общее количество часов производственной практики – 432 ч.

ПП по профессиональному модулю ПМ.03 – 108 ч.

Промежуточная аттестация по производственной практике в форме **дифференцированного зачета.**

2. 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.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

Код ПК	Код и наименование профессиональных модулей, код и наименование МДК	Количество часов на производственную практику по ПМ и соответствующим МДК	Виды работ	Наименование тем производственной практики	Количество часов по темам	Уровень освоения
1	2	3	4	5	6	7
ПК 3.1 ПК 3.2 ПК 3.3	**ПМ.03 Защита информации техническими средствами**					
ПК 3.4 ПК 3.5	**МДК.03.01 Техническая защита информации**	**54**	- Ознакомление с организацией работы на предприятии или в структурном подразделении. - Ознакомление с должностными и функциональными обязанностями. - Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации. - Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения. - Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам. - Применение нормативно право-	**Тема 1. Системы защиты от утечки информации.** 1. Системы защиты, применяемые в организации от утечки информации по акустическому каналу. 2. Системы защиты, применяемые в организации от утечки информации по проводному каналу. 3. Системы защиты, применяемые в организации от утечки информации по вибрационному каналу. 4. Системы защиты, применяемые в организации от утечки информации по электромагнитному каналу. 5. Системы защиты, применяемые в организации от утечки информации по телефонному каналу 6. Системы защиты, применяемые в организации от утечки информации по электросетевому каналу 7. Системы защиты применяемые в организации от утечки информации по оптическому каналу	27	3
				Тема 2. Применение и эксплуатация технических средств защиты информации. 1. Применение технических средств защиты информации по месту практики. 2. Эксплуатация технических средств защиты информации применяемых по месту практики.	27	3

			вых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.			
	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	**54**		**Тема 1. Инженерно-технических средств физической защиты применяемые по месту практики** 1. Построения системы охранной сигнализации. 2. Система контроля и управления доступом. 3. Система телевизионного наблюдения. 4. Система сбора, обработки, отображения и документирования информации.	27	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. Нормативно правовые акты, нормативно методические документы по обеспечению защиты информации техническими средствами.	27	3
	Всего часов	**108**			**108**	

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).

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению практики

Реализация программы производственной практики (по профилю специальности) профессионального модуля предполагает наличие в производственной организации следующего оборудования:

- инструменты и приборы для установки, монтажа и наладки технических средств защиты информации;
- комплект измерительного оборудования;
- персональный компьютер и программное обеспечение общего и профессионального назначения
- специализированная мебель;
- комплект нормативных документов.

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 информационной безопасности : учебное пособие / И. М. Ажмухамедов, О. М. Князева ; под редакцией Т. С. Кулакова. — СПб. : Интермедия, 2017. — 264 с. — ISBN 978-5-4383-0160-8. — 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. —

Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/73732.html

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

3. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
4. 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.
5. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
6. 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
7. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
8. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
9. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
10. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
11. 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
12. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
13. 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
14. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
15. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
16. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
17. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
18. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
19. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
20. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
21. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
22. 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.
23. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищен-

ном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
24. 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.
25. 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.
26. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
27. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
28. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
29. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
30. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
31. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
32. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
33. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
34. 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

4.3. Общие требования к организации производственной практики

Производственная практика проводится на предприятиях, учреждениях, имеющих опыт и практику применения информационных технологий.

В период практики студенты выступают в качестве дублеров техников.

В случае несоответствия базы практики требованиям программы студент обязан своевременно поставить в известность руководителя практики.

Студенты образовательных учреждений среднего профессионального образования при прохождении производственной (профессиональной) практики в организациях **обязаны**:

- полностью выполнять задания, предусмотренные программой производственной (профессиональной) практики;
- соблюдать действующие в организациях правила внутреннего трудового распорядка;
- изучать и строго соблюдать нормы охраны труда и правила пожарной безопасности;
- предоставить руководителю практики от колледжа график своей работы и адрес организации.

Руководители практики от предприятия:

- несут личную ответственность за проведение практики;
- организуют практику в соответствии с программой;
- предоставляют места практики, обеспечивающие наибольшую эффективность ее прохождения;
- организуют, обучение студентов до начала практики правилам техники безопасности, с проверкой их знаний в области охраны труда в установленном данном предприятии порядке;
- обеспечивают выполнение согласованных с учебным заведением графиков прохождения практики по структурным подразделениям предприятия;
- предоставляют студентам возможность пользоваться литературой, технической документацией.

Руководитель практики от учебного заведения:

- устанавливает связь с руководителем практики от предприятия и совместно с ними составляет рабочие программы практики, графики, согласованные с руководителем практики от предприятия;
- разрабатывает тематику индивидуальных заданий и проверяет их выполнение, оказывает студентам методическую помощь;
- осуществляет контроль за правильностью использования студентов в период практики и выполнения программы практики;
- оказывает методическую помощь студентам при выполнении ими индивидуальных заданий;
- оценивает результаты выполнения практикантами программы практики;
- осуществляет постоянный контроль за ходом и организацией практики.

4.4. Кадровое обеспечение практики

Требования к квалификации кадров, осуществляющих руководство практикой:

Руководителями практики могут быть педагогические кадры, имеющие высшее образование, соответствующее профилю модуля.

Имеющие опыт деятельности в организациях соответствующей профессиональной сферы.

Преподаватели должны получать дополнительное профессиональное образование по программам повышение квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРАКТИКИ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Контроль и оценка результатов освоения программы производственной практики осуществляется преподавателем профессионального цикла – руководителем практики в процессе проведения консультаций, а также выполнения учащимися учебно-производственных заданий.

Критерии оценки практики:

1. Ведение документации.
2. Соблюдение сроков сдачи документации и прохождения практики.
3. Теоретическая подготовка – оценивается на основании отчета (реализации задач практики)
4. Профессиональная компетентность - оценивается на основании дневника (оценка работ руководителем практики от предприятия) и характеристики.
5. Творческие способности - оценивается качество решения практического задания.
   Социально-личностные качества - оценивается на основании характеристики.

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.	• Дневник производственной практики • Отчет по практике • Качество решения практического задания. **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	• Дневник производственной практики • Отчет по практике • Качество решения практического задания. **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 информации ограниченного доступа	• Дневник производственной практики • Отчет по практике • Качество решения практического задания. **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 информации	Владение методами измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	• Дневник производственной практики • Отчет по практике • Качество решения практического задания. **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	• Дневник производственной практики • Отчет по практике • Качество решения практического задания. **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	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**

компетенции)		
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	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
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	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
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)	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
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	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
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,	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
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	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
ОК 8. Использовать средства физической	- эффективность выполнения правил ТБ во время учебных за-	• Дневник производственной практики

культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	нятий, при прохождении учебной и производственной практик;	• Отчет по практике • Качество решения практического задания
ОК 9. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	• Дневник производственной практики • Отчет по практике • Качество решения практического задания
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	• Дневник производственной практики • Отчет по практике • Качество решения практического задания