МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Саратовский государственный технический
университет имени Гагарина Ю.А.»

Профессионально-педагогический колледж

УТВЕРЖДАЮ
Директор ППК СГТУ имени Гагарина Ю.А.
_____Л.И. Рожкова
30 июня 2021 г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

специальность

10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рабочая программа рассмотрена
на заседании методической комиссии
рекламы, информационной безопасности и
компьютерных сетей
протокол № 11 от «09» июня 2021 г.
Председатель МК _____ М.А. Ястребова

Саратов 2021

Рабочая программа разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»,утверждѐнного приказом Министерства образования и науки РФ от 09.12.2016 г. № 1553.

Разработчики программы:

Комзолова А.А. – преподаватель высшей квалификационной категории ППК СГТУ имени Гагарина Ю.А.

Таланова Ю.В. – преподаватель высшей квалификационной категории ППК СГТУ имени Гагарина Ю.А.

Рецензенты:

ВнутреннийБондарьА.Г –преподаватель высшей квалификационной категории ППК СГТУ имени Гагарина Ю.А.

ВнешнийМилевский А.А. –генеральный директор ООО «Инфо-Эксперт»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Область применения программы

Рабочая программа производственной (преддипломной) практики является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

Цели и задачи производственной (преддипломной) практики:

Цели практики - углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, проверка его готовности к самостоятельной трудовой деятельности. Кроме того, целью производственной (преддипломной) практики является сбор материалов для дипломного проектирования, практическая работа совместно с разработчиками профессионалами по созданию программного продукта, который будет являться одной из основных частей завершенного дипломного проекта.

Количество часов на освоение программы производственной (преддипломной) практики:

Всего – 144 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Результатом производственной (преддипломной) практики является закрепление первоначального практического опыта и развитие профессиональных (ПК) и общих (ОК) компетенций:

Код	Наименование результата обучения
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
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 ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

3.1.Тематический план производственной (преддипломной) практики

Код ПК	Код и наименования профессиональных модулей	Количество часов	Наименования разделов практики	Количество часов по разделам
1	**2**	**3**	**4**	**5**
ОК 1-10		12	Организационные вопросы оформления на предприятии	6
			Знакомство со структурой и характером деятельности предприятия	6
ОК 1-10 ПК 1.1-1.4	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	114	Тема 1. Формирование требований Тема 2 Разработка концепции ИС Тема 3 Техническое задание Тема 4. Эскизный проект Тема 5 Технический проект Тема 6 Рабочая документация	114
ОК 1-10 ПК 2.1-2.6	ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами			
ОК 1-10 ПК 3.1-3.5	ПМ. 03 Защита информации техническими средствами			
ОК 1-10	**Подготовка отчета по практике**	12		12
Промежуточная аттестация в форме дифференцированного зачета				6
Итого				**144**

3.2. Содержание производственной (преддипломной) практики

Наименование тем практики	Виды работ	Объем часов	Формируемые компетенции
1	2	4	5
Организационные вопросы оформления на предприятии	**Содержание**	6	ОК 1-10
	Организационные вопросы оформления на предприятии, установочная лекция, инструктаж по охране труда и технике безопасности, распределение по рабочим местам *Изучить инструкции по охране труда, инструкции по технике безопасности и пожарной безопасности, схемы аварийных проходов и выходов, размещения пожарного инвентаря.* *Изучить инструкции по охране труда при работе с вычислительной техникой*		
Знакомство со структурой и характером деятельности предприятия	**Содержание**	6	ОК 1-10
	Ознакомиться с производственно - хозяйственной деятельностью предприятия (организации) *Составить характеристику предприятия*		
Тема 1. Формирование требований	1. Обследование объекта и подготовительная работа с экспертами 2. Обоснование необходимости создания или модификации ИС в защищенном исполнении 3. Формирование требований к пользователям ИС	24	ОК 1-10 ПК 1.1-1.4 ПК 2.1-2.6 ПК 3.1-3.5
Тема 2 Разработка концепции ИС	**Содержание**	24	
	1. Изучение объекта с точки зрения функциональной и организационной структуры 2. Изучение объекта с точки зрения организации и содержания документооборота 3. Проведение необходимых научно-исследовательских работ 4. Разработка вариантов концепции ИС 5. Выбор варианта концепции ИС, удовлетворяющего требованиям пользователей		

Наименование тем практики	Виды работ	Объем часов	Формируемые компетенции
Тема 3 Техническое задание	**Содержание** 1. Разработка и утверждение плана технического задания на создание или модификацию ИС в защищенном исполнении 2. Детализация разделов плана технического задания на создание или модификацию ИС в защищенном исполнении 3. Утверждение технического задания на создание ИС в защищенном исполнении	30	
Тема 4. Эскизный проект	1. Обоснование предварительных проектных решений по отдельным частям ИС 2. Обоснование предварительных проектных решений по ИС в целом 3. Разработка предварительных проектных решений по отдельным частям ИС в защищенном исполнении 4. Разработка предварительных проектных решений по ИС в целом 5. Разработка документации на ИС в целом и на ее отдельные части	12	
Тема 5 Технический проект	1. Разработка проектных решений по отдельным частям ИС в защищенном исполнении 2. Разработка проектных решений по ИС в целом	12	
Тема 6 Рабочая документация	1. Разработка рабочей документации на внедрение ИС 2. Разработка документации по техническому сопровождению ИС в период эксплуатации 3. Разработка документации по обучению пользователей работе с ИС 4. Формирование справочной интерактивной поддержки ИС 5. Создание или адаптация Интернет-ресурса поддержки ИС	12	
Подготовка отчета по практике	Работа в колледже с руководителем практики, формирование отчета, сдача его на проверку руководителю.	12	ОК 1-10
Промежуточная аттестация в форме дифференцированного зачета		6	
Итого		**144**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает проведение производственной практики на предприятиях/организациях на основе прямых договоров, заключаемых между образовательным учреждением и каждым предприятием/организацией, куда направляются обучающиеся.

Информационное обеспечение обучения

Нормативно правовые акты:

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

13. 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.
14. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
17. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
18. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
19. 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.
20. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.
№ 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
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 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
39. 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.
40. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
41. 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.
42. 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.
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.

Основные печатные источники:

51. Батаев А.В. Операционные системы и среды (2-е изд., стер.) учебник.- М.: Академия, 2018
52. Фуфаев Э.В. Базы данных (11-е изд.) учеб. пособие.- М.: Академия, 2017
53. Костров Б.В. Сети и системы передачи информации (1-е изд.) учебник.- М.: Академия, 2017
54. Кравченко В.Б. Эксплуатация автоматизированных (информационных) систем в защищѐнном исполнении (1-е изд.) учеб. пособие.- М.: Академия, 2018
57. Баричев С.Г.,Гончаров В.В.,Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.
59. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с
60. Лавровская О.Б. Технические средства информатизации. Практикум (1-е изд.) учеб. пособие.- М.: Академия, 2018
62. Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

Периодические издания:

63. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
64. Журналы Защита информации. Инсайд: Информационно-методический журнал
65. Информационная безопасность регионов: Научно-практический журнал
66. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
67. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Электронные источники:

68. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
69. Информационный портал по безопасности www.SecurityLab.ru.
70. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
71. Российский биометрический портал www.biometrics.ru
72. Сайт журнала Информационная безопасность http://www.itsec.ru –
73. Сайт Научной электронной библиотеки www.elibrary.ru

74. Справочно-правовая система «Гарант» » www.garant.ru

75. Справочно-правовая система «Консультант Плюс» www.consultant.ru

76. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

77. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

78. Федеральный портал «Российское образование www.edu.ru

Общие требования к организации образовательного процесса

Обязательным условием допуска к преддипломной практике является освоение учебного материала и учебной практики для получения первичных, профессиональных умений и навыков, производственной (по профилю специальности) практики, освоенных профессиональных и общих компетенций, в рамках профессиональных модулей:

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ПМ. 03 Защита информации техническими средствами

Аттестация по итогам практики проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.

При прохождении производственной (преддипломной) практики устанавливается продолжительность рабочего времени 36 часов в неделю.

По окончании производственной (преддипломной) практики в соответствии с учебным планом проводится аттестация в форме дифференцированного зачета.

Результатом прохождения производственной (преддипломной) практики должна являться разработанная практическая часть выпускной квалификационной работы (дипломного проекта), содержание которой соответствует одному из видов профессиональной деятельности.

Кадровое обеспечение образовательного процесса

Производственная (преддипломная) практика проводится преподавателями дисциплин профессионального цикла, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины (модуля).

Организацию и руководство производственной (преддипломной) практикой осуществляют руководители практики от образовательного учреждения и от организации.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Результаты (освоенные профессиональные компетенции)	**Формы и методы контроля и оценки результатов обучения**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении. ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении. ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. 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	Отчет в виде предоставленных документов по видам работ практики, отчет-презентация, аттестационный лист по практике, дневник, характеристика

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.	
Результаты (освоенные общие компетенции)	**Формы и методы контроля и оценки**
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.	Отчет в виде предоставленных документов по видам работ практики, отчет-презентация, аттестационный лист по практике, дневник, характеристика

5.2. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Показатели и критерии оценивания компетенций

Показатели и критерии оценивания компетенций отражены в комплекте контрольно оценочных средств. (Приложение 1)

Контрольные и тестовые задания

Перечень вопросов, контрольные и тестовые задания, необходимые для оценки знаний, умений, навыков характеризующих формирование компетенций представлены в комплекте контрольно-оценочных средств. (Приложение 1)

Методические материалы

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков характеризующих формирование компетенций представлены в методических рекомендация по выполнению практических работ. (Приложение 2)