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
Профессионально-педагогического
колледжа СГТУ имени Гагарина Ю.А.
_____ Т.И. Кузнецова
«29» июня 2023 г.

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

специальность

10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рабочая программа рассмотрена
на заседании цикловой методической комиссии
информационной безопасности и компьютерных систем
протокол № 10 от «09» 06 2023 г.
Председатель ЦМК _____ М.А. Ястребова

Саратов 2023

Рабочая программа Производственной практики разработана в соответствии с Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем Министерства образования и науки РФ от 09.12.2016 г. N 1553.

Группа разработчиков:
Богданов В.Ю. - преподаватель Профессионально-педагогического колледжа СГТУ имени Гагарина Ю.А.
Хлебникова Ю.А. - преподаватель Профессионально-педагогического колледжа СГТУ имени Гагарина Ю.А.

Рецензенты:
Внутренний: Ястребова М.А. – преподаватель высшей квалификационной категории ППК СГТУ имени Гагарина Ю.А.
Внешний: Жордочкин А.В. - генеральный директор ООО «Ирис»

СОДЕРЖАНИЕ

Стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ **4**

2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ **6**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ **9**

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ **15**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

ПМ.03 Защита информации техническими средствами

1.1. Область применения рабочей программы

Рабочая программа Производственной практики является частью программы подготовки специалистов среднего звена (далее - ППССЗ) в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида деятельности Защита информации техническими средствами.

Производственная практика проводится при освоении обучающимися профессиональных компетенций в рамках профессионального модуля ПМ.03 Защита информации техническими средствами.

1.2. Место практики в структуре ППССЗ.

Производственная практика входит в Профессиональный цикл.

1.3. Цели и требования к результатам освоения практики

Производственная практика направлена на формирование у обучающихся профессиональных компетенций и общих компетенций в рамках профессионального модуля, реализуется в форме практической подготовки, организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

1.3.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.3.2. Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
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, 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.

1.3.3. В результате освоения программы практики обучающийся должен:

Иметь практический опыт	– выявлении технических каналов утечки информации; – применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; – проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; - проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
уметь	– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять инженерно-технические средства физической защиты объектов информатизации.

1.4. Количество часов на освоение программы практики:

Всего: 144 часа.

2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

2.1. Тематический план практики

Код (ПК, ОК)	**Код и наименование профессионального модуля**	**Количество часов практики**	**Наименования разделов практики**	**Количество часов по разделам, МДК**
1	2	3	4	5
ПК 3.1-3.5 ОК 01-11	ПМ.03 Защита информации техническими средствами	144	Инструктаж	**6**
			МДК 03.01 Техническая защита информации МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	**78** **48**
			Обобщение материалов, оформление дневника и отчета по практике.	**6**
			Промежуточная аттестация в форме дифференцированного зачета	**6**

2.2. Содержание практики

Наименование разделов, тем практики	Виды работ	Объем часов	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4	5
Инструктаж	1. Согласовать порядок выполнения заданий с руководителем практики от колледжа. 2. Пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности	6	1	ОК 01 ОК 04
Тема 1 Концепция технической защиты информации	1. Выявление технических каналов утечки информации 2. Применение технических средств защиты информации.	30	3	ОК 01-11 ПК 3.1
Тема 2 Эксплуатация и техническое обслуживание технических средств защиты информации	3. Участие в обслуживании и эксплуатации технических средств защиты информации, в том числе средств защиты информации от несанкционированного съёма и утечки по техническим каналам 4. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН). 5. Оценка защищенности информации от утечки по техническим каналам	48	3	ОК 01-ОК 11 ПК 3.2-3.4
Тема 3 Применение и эксплуатация инженерно-технических средств физической защиты	6. Участие в обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	48	3	ОК 01-11 ПК 3.5

	7. Организация отдельных работ по физической защите объектов информатизации 8. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.			
Обобщение материалов, оформление дневника и отчета по практике.		6	3	ОК 01-11 ПК 3.1-3.5
Промежуточная аттестация в форме дифференцированного зачета		6	3	ОК 01-11 ПК 3.1-3.5
Всего:		***144***		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

3.1. Требования к минимальному материально-техническому обеспечению практики

Практика может проводиться в организации, осуществляющей деятельность по профилю соответствующей образовательной программы, в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки, на основании договора. Требуется создание профильной организацией условий для реализации программы практики в форме практической подготовки, предоставления оборудования и технических средств обучения в объеме, позволяющем выполнять виды работ, определенные программой практики.

Типовое оборудование, технологическое оснащение рабочих мест, технические средства обучения.

Типовое лицензионное программное обеспечение.

Учебно-наглядные пособия, имеющиеся на предприятии.

Персональные компьютеры, имеющие выход в глобальную сеть Интернет, оснащен лицензионным программным обеспечением.

3.2. Учебно-методическое и информационное обеспечение реализации практики

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/

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». - Режим доступа: http://www.consultant.ru/

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. - Режим доступа: http://www.consultant.ru/

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

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21. - Режим доступа: http://www.consultant.ru/

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

13. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/

14. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

15. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

16. 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. – Режим доступа: http://docs.cntd.ru/

17. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

18. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/

19. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/

20. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/

21. 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. – Режим доступа: http://docs.cntd.ru/

22. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/

23. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/

24. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/

25. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/

26. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

27. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/

28. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

29. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/

30. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

31. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

33. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

34. 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. – Режим доступа: http://docs.cntd.ru/

35. 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. – Режим доступа: http://docs.cntd.ru/

36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

38. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

39. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

40. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0.

42. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД "ФОРУМ" : ИНФРА-М, 2021. - 416 с. - (Среднее профессиональное образование). ISBN 978-5-8199-0754-2

Дополнительные учебные издания

43. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

44. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

45. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

46. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

47. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

48. 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. – Режим доступа: http://docs.cntd.ru/

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

51. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/

52. 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. - Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

53. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) - Режим доступа: https://fstec.ru/

54. Информационно-справочная система по документам в области технической защиты информации - Режим доступа: https://fstec.ru/

55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/

56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/

57. Федеральный портал. Российское образование. - Режим доступа: http://www.edu.ru

58. Сайт Научной электронной библиотеки - Режим доступа: https://www.elibrary.ru/

Методические указания по выполнению заданий практики

59.Методические указания по выполнению заданий практики.

3.3. Общие требования к организации образовательного процесса

Образовательная деятельность при освоении профессионального модуля организуется в форме практической подготовки путем проведении практики, предусматривающей непосредственное выполнение обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Производственная практика проводится при освоении обучающимися профессиональных компетенций в рамках профессионального модуля ПМ.03 Защита информации техническими средствами и реализуется концентрированно, в рамках профессионального модуля. Производственная практика реализуется в профильных организациях, в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки.

Производственная практика ПП 03.01 реализуется в 8 семестре на 4 курсе (на базе 11 классов – 6 семестре, 3 курс) (в соответствии с учебным планом) после изучения МДК 03.01 Техническая защита информации, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации.

3.4. Кадровое обеспечение образовательного процесса

Для реализации программы Производственной практики назначается ответственное лицо, соответствующее требованиям трудового законодательства

Российской Федерации о допуске к педагогической деятельности, из числа работников Профильной организации.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ

4.1. Критерии оценки, формы и методы контроля и оценки результатов обучения

Код, наименование профессиональных компетенций	**Критерии оценки**	**Формы и методы контроля и оценки результатов обучения**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	- применение, техническое обслуживание, диагностика, устранение отказов, восстановление работоспособности, установка, монтаж и настройка инженерно-технических средств физической защиты и технических средств защиты информации;	**Текущий контроль:** собеседование по результатам выполненной работы, наблюдение за процессом выполнения заданий. выполнение письменной работы "Отчет по практике") **Промежуточная аттестация**: отчет по практике.
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	- применять технические средства для криптографической защиты информации конфиденциального характера; - применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	
ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	- проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	- проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;	

ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	- выявление технических каналов утечки информации; - применение средств охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	

Код, наименование общих компетенций	**Критерии оценки**	**Формы и методы контроля и оценки результатов обучения**
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	- распознавание задач в профессиональном и/или социальном контексте; - распознавание проблем в профессиональном и/или социальном контексте; - анализ задачи и/или проблемы; - выделение составных частей задачи и/или проблемы; - определение этапов решения задачи; - выявление информации, необходимой для решения задачи и/или проблемы; - осуществление эффективного поиска информации, необходимой для решения задачи и/или проблемы; - разработка плана действия решения задачи и/или проблемы; - определение необходимых ресурсов для решения задачи и/или проблемы; - владение актуальными методами работы в профессиональной и смежных сферах; - реализация составленного плана; - оценка результата и последствий своих действий (самостоятельно или с помощью наставника).	Текущий контроль успеваемости: - опрос устный; - выполнение заданий по практике. Промежуточная аттестация: в форме дифференцированного зачета. Метод проведения промежуточной аттестации: защита отчета по практике.
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- определение задач поиска информации, необходимых источников информации; - планирование процесса поиска необходимой информации; - осуществление поиска информации необходимой для выполнения задач профессиональной деятельности; - проведение анализа информации, необходимой для выполнения задач профессиональной деятельности; - осуществление интерпретации информации, необходимой для выполнения задач профессиональной деятельности; - структурирование получаемой информации; - выделение наиболее значимой в перечне информации;	

	- оценка практической значимости результатов поиска; - оформление результатов поиска.	
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	- планирование собственного профессионального развития; - построение траектории собственного профессионального и личностного развития; - реализация собственного профессионального и личностного развития; - определение актуальности нормативно-правовой документации в профессиональной деятельности.	
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- организация работы коллектива и команды; - эффективное взаимодействие с коллегами, руководством; - эффективное взаимодействие с клиентами.	
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- грамотное изложение своих мыслей на государственном языке; - правильное оформление документов по профессиональной тематике на государственном языке; - проявление толерантности в рабочем коллективе	
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	- понимание значимость своей специальности; - описание значимости своей специальности; - презентация структуры профессиональной деятельности по специальности; - проявление гражданско-патриотической позиции; - демонстрация осознанного поведения на основе традиционных общечеловеческих ценностей; - применение стандартов антикоррупционного поведения.	
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- содействие сохранению окружающей среды; - содействие ресурсосбережению; - осуществление эффективных действий в чрезвычайных ситуациях; - соблюдение норм экологической безопасности; - определение направлений ресурсосбережения в рамках профессиональной деятельности по специальности	
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе	- использование физкультурно-оздоровительной деятельности для укрепления здоровья, достижения жизненных и профессиональных	

профессиональной деятельности и поддержания необходимого уровня физической подготовленности	целей; - применение рациональных приемов двигательных функций в профессиональной деятельности; - использование средств профилактики перенапряжения характерными для данной специальности	
ОК 9. Использовать информационные технологии в профессиональной деятельности.	- применение средств информационных технологий для решения профессиональных задач; - использование современного программного обеспечения	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках	- понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые); - понимание текста на базовые профессиональные темы; - участие в диалогах на знакомые общие и профессиональные темы; - построение простых высказываний о себе и о своей профессиональной деятельности; - краткое обоснование и объяснение своих действий (текущих и планируемых); - написание простых связных сообщений на знакомые или интересующие профессиональные темы	
ОК.11 Использовать знания финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	- выявление достоинств и недостатков коммерческой идеи; - презентация идеи открытия собственного дела в профессиональной деятельности; - оформление бизнес-плана; - расчет размера выплат по процентным ставкам кредитования; - определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности; - презентация бизнес - идеи; - определение источников финансирования	

4.2. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Показатели и критерии оценивания компетенций

Показатели и критерии оценивания компетенций, описание шкал оценивания содержатся в приложении 1.

Методические материалы

Методические материалы содержатся в приложении 2.

Приложение 1

Контрольно-оценочные средства
для проведения промежуточной аттестации по практике
ПМ.03 Защита информации техническими средствами

1.1. Форма промежуточной аттестации: дифференцированный зачет (8 (6) семестр).

1.2. Система оценивания результатов выполнения заданий

Оценивание результатов выполнения заданий текущего контроля успеваемости, промежуточной аттестации обучающихся осуществляется на основе следующих принципов:

достоверности оценки – оценивается уровень сформированности знаний, умений, практического опыта, общих и профессиональных компетенций, продемонстрированных обучающимися в ходе выполнения задания;

адекватности оценки – оценка выполнения заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания;

надежности оценки – система оценивания выполнения заданий должна обладать высокой степенью устойчивости при неоднократных оценках уровня сформированности знаний, умений, практического опыта, общих и профессиональных компетенций обучающихся;

комплексности оценки – система оценивания выполнения заданий должна позволять интегративно оценивать общие и профессиональные компетенции обучающихся;

объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений преподавателей, осуществляющих контроль или аттестацию.

При выполнении процедур оценки заданий используются следующие основные методы:

метод экспертной оценки (привлечение к контролю и оценке специалистов предприятий и организаций);

метод расчета первичных баллов;

метод расчета сводных баллов.

Структура оценки результатов прохождения практики (отчет по практике):
- оценка отчета обучающегося о выполненной работе, содержащегося в документе «Отчет по практике»(оценивается результат выполнения заданий практики отдельно по каждой теме, определяется средний балл);
- оценка по защите практики;
- средний балл по итогам аттестации.

Используется пяти бальная шкала для оценивания результатов обучения:

Перевод пяти бальной шкалы учета результатов в пяти бальную оценочную шкалу:

Оценка	Количество баллов, набранных за выполнение теоретического и практического задания, средний балл по итогам аттестации
Оценка 5 «отлично»	4,6-5
Оценка 4 «хорошо»	3,6-4,5
Оценка 3 «удовлетворительно»	3-3,5
Оценка 2 «неудовлетворительно»	≤ 2,9

1.3. Контрольно-оценочные средства
Задание производственной практики

Наименование разделов, тем	Содержание задания	Объем часов	Коды компетенций, формированию которых способствует элемент программы
Инструктаж	- Согласование порядка выполнения заданий с руководителем практики от базы практики. - Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка предприятия/организации, являющейся базой практики. *Представить характеристику объекта практики. Использовать при составлении характеристики таблицу (Приложение А).*	6	ОК 01-04
Тема 1. Концепция технической защиты информации	**Вид работ: Выявление технических каналов утечки информации.** **Задание 1**. Структурировать защищаемую информацию предприятия. *В отчете предоставить перечень сведений, составляющих государственную, ведомственную или коммерческую тайну; перечислить источники информации на предприятии. Результат структурирования оформить в виде таблицы.* **Задание 2.** Предоставить план помещения предприятия, с его техническими характеристиками. *В отчете представить чертеж, выполненный в формате А4, с пояснением*	6 12	ОК 01-11 ПК 3.1

	элементов, расположенных на плане. На плане(ах) помещения(й) указать в масштабе места размещения ограждений, экранов, воздухопроводов, батарей и труб отопления, элементов интерьера и других конструктивных элементов, способствующих или затрудняющих распространение сигналов с защищаемой информацией, а также места размещения и зоны действия технических средств охраны и телевизионного наблюдения. Их параметры объединить в таблице.		
	Задание 3. Провести обследование объекта (предприятия) по выявлению возможных каналов утечки информации. *В отчете перечислить потенциальные каналы утечки информации для данного предприятия (с характеристикой каналов). Результат обследования оформить в виде таблицы.*	6	
	Вид работ: Применение технических средств защиты информации. **Задание 4.** Смоделировать способы физического проникновение злоумышленника к источникам информации предприятия: *В отчете предоставить сведения о возможных путях проникновения злоумышленника на данном предприятии к источникам информации (виды угроз см таблица В, Приложение В).* *Для каждой из угроз определить средства защиты, обеспечивающие защиту информации на предприятии, указать угрозы, которые не защищены. Результат обследования оформить в виде таблицы3.*	6	
Тема 2. Эксплуатация и техническое обслуживание технических средств защиты информации	**Вид работ: Участие в обслуживании и эксплуатации технических средств защиты информации, в том числе средств защиты информации от несанкционированного съёма и утечки по техническим каналам.** **Задание 5.** Проанализировать методы и средства технической защиты информации, применяемые на предприятии (в том числе с техническими средствами для криптографической защиты информации конфиденциального характера, техническими средствами для уничтожения информации и носителей информации, средствами защиты информации от несанкционированного	6	ОК 01-11 ПК 3.2

	съёма и утечки по техническим каналам): *В отчете перечислить основные методы и средства технической защиты информации на предприятии (с кратким их описанием). Предоставить сведения о средствах технической защиты информации применяемых на предприятии, с указанием их характеристик, количества и технического состояния (оформить в виде таблицы).*		
	Задание 6. Принять участие в диагностике и устранении отказов в робототехнических средств защиты информации (ТСЗИ). *В отчете перечислить сбои в работе технических средств защиты информации на предприятии (со слов руководителей практики или те с которыми Вы столкнулись на предприятии).* *Перечислить возможные неисправности оборудования (ТСЗИ) исходя из данных других предприятий, использующих такие же ТСЗИ (или из статистических данных о работоспособности и возможных неисправностях оборудования). Описать алгоритмы устранения перечисленных сбоев и отказов.*	12	
	Задание 7. Принять участие в разработке предложений (рекомендаций) по более эффективной работе технических средств защиты информации, средств защиты информации от несанкционированного съёма и утечки по техническим каналами технических средств для уничтожения информации и носителей информации, способных обеспечивать полный и надёжный контроль над безопасностью предприятия. *В отчете перечислить основные рекомендации, предложения.*	6	
	Вид работ: Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН).		ОК 01-11, ПК 3.3
	Задание 8. Принять участие в поиске и измерение сигналов ПЭМИН и сигналов наводок ПЭМИН в линии электропитания. Производить расчеты показателей защищенности. *В отчете описать методику поиска и измерения сигналов излучений и наводок, методику оценки защищенности конфиденциальной информации от утечки*	12	

	по каналам ПЭМИН. Сделать вывод о защищенности объекта защиты.		
	Вид работ: Оценка защищенности информации от утечки по техническим каналам. **Задание 9.** Принять участие в проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Производить расчеты показателей защищенности. *В отчете описать методику измерений параметров фоновых шумов и физических полей, методику оценки защищенности конфиденциальной информации от утечки по техническим каналам. Сделать вывод о защищенности объекта защиты.*	12	ОК 01-11, ПК 3.4
Тема 3. Применение и эксплуатация инженерно-технических средств физической защиты	**Вид работ: Участие в обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.** **Задание 10.** Проанализировать методы и средства инженерно-технической защиты информации, применяемые на предприятии. *В отчете перечислить основные методы и средства инженерно-технической защиты объекта(предприятия) (с кратким их описанием).* **Задание 11.** Принять участие в проверке технического состояния инженерно-технических средств физической защиты объекта. Разработать предложения по усовершенствованию и повышению эффективности применяемых инженерно-технических средств физической защиты предприятия. *В отчете перечислить основные рекомендации, предложения.* **Вид работ: Организация отдельных работ по физической защите объектов информатизации.** **Задание 12.** Принять участие в разработке проекта по модернизации системы ИТЗИ на предприятии с учетом специфики зон защиты, степени важности информации, допустимого риска (допустимых потерь) и возможностей современных инженерно-технических средств защиты информации. *В отчете представить предложения по модернизации в виде таблицы 5.*	6 12 12	ОК 01-11, ПК 3.5

	Задание 13. Проанализировать экономическую эффективность проекта модернизации системы ИТЗИ на предприятии, исходя из соотношений между гипотетическими доходами, измеряемыми возможными потерями из-за отсутствия надежной системы безопасности на объектах защиты, и произведенными затратами на внедрение предложенной системы. *В отчете представить таблицу, указав компоненты инженерно-технической системы информационной безопасности, их стоимость, стоимость монтажа (исходя из цен по г. Саратову), в комментариях указать эффективность использования данного компонента.* **Вид работ: Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.** **Задание 14.** Разработать проект внутренних организационно-распорядительных и нормативных документов по безопасности информации: положение о пропускном режиме на предприятии на основе типового, положение о видеонаблюдении на предприятии на основе типового (*в отчете положения оформить в виде приложений).*	6 12	
Обобщение материалов и оформление отчета по практике	Обобщение материала, полученного при прохождении практики	6	ОК 01-11, ПК 3.1-3.5
Итого		**144**	

1.3.1 Критерии оценки отчета обучающегося о выполненной работе, содержащегося в документе «Отчет по практике»

	Критерии оценки	Оценка
1	Задания практики выполнены студентом в полном объеме. Отчет о выполнении заданий практики содержит верное описание самостоятельно *(либо под руководством руководителя практики)* выполненных обучающимся действий в соответствии с заданиями практики. Содержит верно выполненный анализ действий (работ), данных, верные и обоснованные выводы, верно оформленные документы.	5 "отлично"
2	Задания практики выполнены студентом в полном объеме. Отчет о выполнении заданий практики содержит верное описание самостоятельно*(либо под руководством руководителя практики)* выполненных обучающимся действий в соответствии с заданиями практики, но допущены несущественные ошибки. Анализ действий (работ), данных выполнен в полном объеме, выводы верные, при оформлении документов допущены несущественные ошибки.	4 "хорошо"
3	Задания практики выполнены студентом в полном объеме. Отчет о выполнении заданий практики содержит верное описание самостоятельно*(либо под руководством руководителя практики)*выполненных обучающимся действий в соответствии с заданиями практики, но допущены неточности и грубые ошибки, не влекущие за собой неверный результат выполненной работы в целом. Отчет содержит результаты поверхностного анализа действий (работ), данных. Отдельные выводы нельзя считать верными, целесообразными и обоснованными. При оформлении документов допущены несущественные ошибки.	3 "удовлетворительно"
4	Задания практики выполнены студентом не в полном объеме. Отчет о выполнении заданий практики содержит множественные грубые ошибки в описании самостоятельно выполненных обучающимся действий. Анализ действий (работ), данных выполнен с грубыми нарушениями, либо не выполнен. Выводы, в большей части, нельзя считать верными. Документы оформлены неверно.	2 "неудовлетворительно"

В случае, если результат выполнения заданий практики по одной из тем, содержащейся в документе «Задание на практику» будет оценен на 2 балла "неудовлетворительно", практика не может быть оценена положительно, т.к. обучающийся не освоил в полном

объеме планируемые программой практики и Заданием на практику результаты освоения практики.

1.3.2. Критерии оценки защиты практики

	Критерии оценки	Оценка
1	При защите практики: студент верно комментирует работы, выполненные им на практике, оперирует в полном объеме фактами и владеет информацией, содержащимися в «Отчете по практике»; приводит соответствующие аргументы для доказательства правоты собственных действий (работ), выводов. Во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал. Студент правильно, полно и уверенно отвечает на поставленные вопросы.	5 "отлично"
2	При защите практики:студент верно комментирует работы, выполненные им на практике, оперирует в достаточном объеме фактами и владеет информацией, содержащимися в «Отчете по практике"; приводит соответствующие аргументы для доказательства правоты собственных действий и выводов. Во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал. Студент правильно,с небольшими затруднениями отвечает на поставленные вопросы. Рекомендуемая оценка, содержащаяся в характеристике организации на обучающегося - "отлично", либо "хорошо".	4 "хорошо"
3	При защите практики: студент отчасти верно комментирует работы, выполненные им на практике, демонстрирует затруднение оперируя фактами и информацией, содержащейся в «Отчете по практике"; приводит не всегда верные аргументы для доказательства правоты собственных действий. Во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал. Студент не дает полных, аргументированных ответов на заданные вопросы, но большинство ответов можно считать верными. Рекомендуемая оценка, содержащаяся в характеристике организации на обучающегося - "удовлетворительно".	3 "удовлетворительно"
4	При защите практики: студент затрудняется пояснить действия, которые он выполнял на практике в соответствии с заданиями, привести аргументы, доказывающие правоту собственных действий, объяснить выводы. На защите отсутствуют наглядные пособия или раздаточный материал. Рекомендуемая оценка, содержащаяся в характеристике организации на обучающегося - "удовлетворительно", либо "неудовлетворительно".	2 "неудовлетворительно"

Перевод десятичной дроби, полученной в результате определения среднего балла по итогам аттестации, в пяти бальную оценочную шкалу:

Оценка	**Количество баллов, набранных за выполнение задания учебной практики, средний балл по итогам аттестации**
Оценка 5 «отлично»	**4,6-5**
Оценка 4 «хорошо»	**3,6-4,5**
Оценка 3 «удовлетворительно»	**3-3,5**
Оценка 2 «неудовлетворительно»	**≤ 2,9**

1.4. Материально-техническое обеспечение для проведения промежуточной аттестации

Аттестация проводится в лаборатории технических средств защиты информации

1.5. Учебно-методическое и информационное обеспечение для проведения промежуточной аттестации

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/
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». - Режим доступа: http://www.consultant.ru/
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

- Режим доступа: http://www.consultant.ru/

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

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21. - Режим доступа: http://www.consultant.ru/

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

13. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/

14. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

15. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

16. 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. – Режим доступа: http://docs.cntd.ru/

17. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

18. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/

19. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/

20. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/

21. 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. – Режим доступа: http://docs.cntd.ru/

22. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/

23. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/

24. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/

25. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/

26. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

27. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/

28. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

29. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/

30. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

31. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

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

Режим доступа: http://docs.cntd.ru/

34. 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. – Режим доступа: http://docs.cntd.ru/

35. 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. – Режим доступа: http://docs.cntd.ru/

36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

38. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

39. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

40. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0.

42. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД "ФОРУМ" : ИНФРА-М, 2021. - 416 с. - (Среднее профессиональное образование). ISBN 978-5-8199-0754-2

Дополнительные учебные издания

43. Специальные требования и рекомендации по технической защите

конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

44. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

45. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

46. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

47. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

48. 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. – Режим доступа: http://docs.cntd.ru/

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

51. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/

52. 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. - Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

53. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) - Режим доступа: https://fstec.ru/

54. Информационно-справочная система по документам в области технической защиты информации - Режим доступа: https://fstec.ru/

55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/

56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/

57. Федеральный портал. Российское образование. - Режим доступа: http://www.edu.ru

58. Сайт Научной электронной библиотеки - Режим доступа: https://www.elibrary.ru/

Методические указания по выполнению заданий практики

5.9. Методические указания по выполнению заданий практики.