

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ
ПП.03 Производственная практика

Регистрационный № 23 ИБ/37-1

Санкт-Петербург
2023

Рабочая программа практики разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем и с учетом профессиональных стандартов

- «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)
- «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)
- «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)
- «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)
- «Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н

Организация-разработчик:

Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Академия промышленных технологий» (СПб ГБОУ «АПТ»)

Разработчики:

Еропкин И.В. – преподаватель высшей квалификационной категории СПб ГБПОУ «АПТ»

Рабочая программа рассмотрена на заседании учебной цикловой комиссии **Информационных технологий**.

Рабочая программа соответствует требованиям к содержанию, структуре, оформлению.

Протокол № 10 от 07.06.2023

Председатель УЦК Еропкин И.В.

Программа одобрена на заседании Педагогического совета и рекомендована к использованию в учебном процессе.

Протокол № 1 от 28 августа 2023

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ
4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения рабочей программы

Рабочая программа 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 деятельности: Защита информации техническими средствами и соответствующих профессиональных компетенций (ПК):

- 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.

1.2. Место практики в структуре образовательной программы: Профессиональный цикл. Производственная практика проводится образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессионального модуля ПМ.03 Защита информации техническими средствами.

1.3. Цели и задачи практики - требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности Защита информации техническими средствами и соответствующими профессиональными

компетенциями обучающийся в ходе освоения программы учебной практики должен

иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
- установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

уметь:

- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации;
- применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять инженерно-технические средства физической защиты объектов информатизации.

знать:

- порядок технического обслуживания технических средств защиты информации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки

информации;

- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

- основные принципы действия и характеристики технических средств физической защиты;

- основные способы физической защиты объектов информатизации;

- номенклатуру применяемых средств физической защиты объектов информатизации.

1.3. Количество часов на освоение рабочей программы практики:
всего - 216 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Результатом освоения рабочей программы практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ.03 Защита информации техническими средствами по основному виду деятельности - Защита информации техническими средствами, в том числе профессиональными компетенциями (ПК):

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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование разделов и тем / виды работ	Содержание учебного материала / содержание работ	Объем часов, в том числе в форме практической подготовки
Раздел 1. Применение и эксплуатация технических средств защиты информации	4 курс, 7 семестр	70
	1. Исследование угроз и методологии оценки уязвимости информации.	
	2. Оценка информационных рисков.	
	3. Исследование методов и моделей оценки уязвимости информации.	
	4. Исследование аналитических моделей для определения базовых показателей уязвимости информации.	
	5. Участие в проектировании политики безопасности информационного объекта.	
	6. Проектирование политики безопасности информационного объекта на конкретном примере.	
	7. Мероприятия по выявлению каналов утечки информации (специальные обследования).	
	8. Участие в монтаже технических средств защиты информации в телефонных линиях	
	9. Участие в обслуживании и эксплуатации технических средств защиты информации в телефонных линиях	
	10. Оценка эффективности защиты речевой информации	
	И. Инструментально-расчётная оценка защищённости защищаемого помещения от утечки речевой информации	
	12. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности: датчики движения для охраны помещений	
		Дифференцированный зачет
	Всего (за 4 курс, 7 семестр)	72
Раздел 2. Применение и эксплуатация инженерно технических средств физической защиты	4 курс, 8 семестр	142
	1. Участие в монтаже, обслуживании и эксплуатации средств инженерной защиты и технической охраны	
	2. объектов: системы защиты от утечки информации по оптическому каналу	
	3. Проектирование системы видеонаблюдения за протяженным периметром. Проектирование системы	

4.	идентификации людей на входе в здание. Проектирование системы видеонаблюдения в транспорте.	
5.	Проектирование системы видеонаблюдения в школе	
6.	Участие в монтаже систем видеонаблюдения. Участие в обслуживании систем видеонаблюдения.	
7.	Эксплуатации систем видеонаблюдения. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: защита информации от утечки по акустическому каналу пассивными методами	
8.	Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: системы защиты от утечки информации по электросетевому каналу	
	Дифференцированный зачет	2
	Всего (за 4 курс, 8 семестр)	144
		Всего 216

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

4.1. Требования к минимальному материально-техническому обеспечению реализации рабочей программы практики:

Практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся на основе договоров, заключаемых между СПб ГБПОУ «АПТ» и организациями.

Материально-техническая база должна соответствовать действующим санитарным и противопожарным нормам.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

4.2. Информационное обеспечение реализации рабочей программы учебной практики:

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, вебсистем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Гребенюк Е. И., Гребенюк Н. А. Технические средства информатизации. Учебник для СПО М.: ИЦ Академия, 2019 - 352 с.
2. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А., М.: ИЦ Академия, 2019 - 272 с.

Дополнительные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О

мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

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

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

16. от 30 августа 2002 г. № 282.

17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

19. от 31 августа 2010 г. № 416/489.

20. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

21. Руководящий документ. Геоинформационные системы. Защита

- информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
22. 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 недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
23. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
3. 2. ГОСТ Р ИСО/МЭК 1333 5-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
33. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
34. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
35. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
3. 6. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
37. 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
38. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
39. 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
40. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
41. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая

защита информации. Функция хэширования"

42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
44. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
45. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
48. Номенклатура показателей качества. Ростехрегулирование, 2005.
49. 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.
50. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
51. 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.
52. 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.
53. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
54. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

55. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
56. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
58. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
59. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 1 февраля 2013 г. № 17.
60. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
61. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

1. Устройства ввода информации - <https://intuit.ru/studies/courses/3460/702/lecture/14158>
2. Устройства вывода информации - <https://intuit.ru/studies/courses/3460/702/lecture/14157>
3. Цифровая образовательная среда СПО РКОРобразование:
 - Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 с. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО РКОРобразование : [сайт]. — URL: <https://profspo.ru/books/87882> (дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

Веб-система для организации дистанционного обучения и управления им:

[Система дистанционного обучения СПб ГБПОУ «Академия промышленных технологий» \(3072.ru\)](https://3072.ru)

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

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

В результате освоения практики в рамках профессионального модуля обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта	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	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике дифференцированный зачет
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике дифференцированный зачет
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике дифференцированный зачет
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике дифференцированный зачет
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике дифференцированный зачет