

**Приложение 4 Фонд оценочных средств учебных дисциплин
к ОПОП по специальности
10.02.05 Обеспечение информационной
безопасности автоматизированных систем.**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по

**МДК 03.02 Инженерно-технические средства физической защиты объектов
информатизации**

для специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Регистрационный №22ИБ/ ФОС

Санкт-Петербург
2023

Фонд оценочных средств по МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации составлен на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного Приказом Министерства образования и науки от 09.12.2016 № 1553.

Организация-разработчик:

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

Разработчик: Еропкин И.В.

преподаватель высшей категории СПб ГБПОУ «АПТ»

Фонд оценочных средств по МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации рассмотрен на заседании учебной цикловой комиссии

Информационных технологий

ФОС соответствует требованиям к содержанию, структуре, оформлению.

Протокол № 10 от 06.06. 2023

Председатель УЦК Еропкин И.В.

Фонд оценочных средств соответствует требованиям к содержанию, структуре, оформлению.

Фонд оценочных средств одобрен на заседании Педагогического совета и рекомендован к использованию в учебном процессе.

Протокол №1 от 28.08.2023

1. Общие положения.....	4
2. Результаты освоения междисциплинарного курса, подлежащие проверке на экзамене.....	4
3. Оценка освоения междисциплинарного курса	7
4. Информационное и материально-техническое обеспечение.....	10

1. Общие положения

Результатом освоения междисциплинарного курса является готовность обучающегося к выполнению вида профессиональной деятельности Защита информации техническими средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ОПОП в целом.

Формой аттестации по междисциплинарному курсу является экзамен. Для осуществления текущего контроля применяются: индивидуальный и фронтальный опрос в ходе аудиторных занятий, практических работ, интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.

2. Результаты освоения междисциплинарного курса, подлежащие проверке на экзамене

2.1. В результате аттестации по междисциплинарному курсу осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Профессиональные и общие компетенции, которые возможно сгруппировать для проверки	Показатели оценки результата
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
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
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
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации

информации.	
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
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- грамотность устной и письменной речи, - ясность формулирования и изложения мыслей
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;

<p>ОК 9. Использовать информационные технологии в профессиональной деятельности.</p>	<p>эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;</p>
<p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.</p>	<p>эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.</p>

3. Оценка освоения междисциплинарного курса

3.1. Типовые задания для оценки освоения МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации

Список экзаменационных вопросов:

1. Понятие информации. Проблема обеспечения безопасности в информационных системах, политика информационной безопасности.
2. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
3. Физические средства
4. Аппаратные средства
5. Программные средства
6. Криптографические средства
7. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
8. Генераторы шума.
9. Особенности работы и основные характеристики сканирующих радиоприемников.
10. Блок-схема типового сканирующего радиоприемника.
11. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения локализации в пространстве закладных устройств.
12. Виды модуляции и кодирования передаваемой информации.
13. Амплитудная модуляция. Амплитудная модуляция с подавлением верхней или нижней боковой частоты. Частотная модуляция. Фазовая модуляция.
14. Кодово-импульсная модуляция. Специальные виды модуляции. Основные требования к специальным системам связи.
15. Использование ШПС и ППРЧ сигналов. Основные характеристики.
16. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
17. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений.
18. Концепции инженерно-технической защиты информации.
19. Системный подход к защите информации.
20. Основные проблемы инженерно-технической защиты информации.
21. Основные концептуальные положения инженерно-технической защиты информации.

22. Направления инженерно-технической защиты информации.
23. Показатели эффективности инженерно-технической защиты информации.
24. Теоретические основы инженерно-технической защиты информации.
25. Источники опасных сигналов.
26. Виды побочных опасных электромагнитных излучений.
27. Характеристика технической разведки.
28. Технические каналы утечки информации.
29. Методы инженерно-технической защиты информации.
30. Методы инженерной защиты и технической охраны объекта.
31. Методы скрытия информации и ее носителей.
32. Физические основы защиты информации.
33. Физические основы побочных электромагнитных излучений и наводок.
34. Распространение сигналов в технических каналах утечки информации.
35. Физические процессы подавления опасных сигналов.
36. Технические средства добывания и инженерно-технической защиты.
37. Средства технической разведки.
38. Средства инженерной защиты и технической охраны.
39. Средства предотвращения утечки информации по техническим каналам.
40. Организационные основы инженерно-технической защиты информации.
41. Государственная система защиты информации.
42. Контроль эффективности инженерно-технической защиты информации.
43. Методическое обеспечение инженерно-технической защиты автоматизированных систем от вредоносных программных воздействий.
44. Моделирование инженерно-технической защиты информации.
45. Методические рекомендации по оценке эффективности защиты информации.

Типовое практическое задание для оценки освоения МДК 03.02 инженерно-технические средства физической защиты объектов информатизации

Инструкция для выполнения задания

Внимательно прочитайте задание.

Время выполнения задания - 45 минут.

Текст задания

Промышленное предприятие (условно ОАО «Маяк»), специализирующееся на производстве пластмассовых труб, которые по своим качествам пользуются большим спросом. Охрана и защита коммерческих секретов, связанных с технологией производства труб, находятся в центре внимания руководства и службы безопасности предприятия. Предприятие имеет административную зону, где расположены управленческие структуры, производственную и складскую зоны. Все эти зоны разделены заборами. Предприятие имеет широкий круг партнеров, клиентов (в том числе и за рубежом). В сфере деятельности предприятия часто возникают конфликтные ситуации с конкурентами и спорные вопросы с органами местной власти по земельным и финансовым вопросам.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Критерии оценки

Выполнение задания

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

Подготовленный продукт

- разработанная система видеонаблюдения административной зоны.

Устное обоснование

- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.

4.Требования к минимальному материально-техническому обеспечению Лаборатория технических средств защиты информации

Оборудование учебного кабинета: доска, 15 автоматизированных рабочих мест для студентов: столы-15 шт., стулья -15 шт., ПК-15 шт., автоматизированное рабочее место для преподавателя - 1 шт., сканер-1 шт., принтер-1 шт., проектор - 1шт., экран - 1 шт.; программное обеспечение общего и профессионального назначения, лабораторные учебные макеты.

Основное оборудование: учебно-методическая документация; аппаратные средства аутентификации пользователя.

4.1. Информационное обеспечение

4.1.1. Основные печатные 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.

4.1.2. Дополнительные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2020.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2021
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб, пособие. - М.: МИЭТ, 2019-172 с.
4. Организационно-правовое обеспечение Информационной безопасности: учеб, пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. - М.: Издательский центр «Академия», 2019-336с
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации Академия, - 336 с. - 2020
7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

- И. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
 13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
 14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
 15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
 16. 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».
 17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
 18. 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.
 19. 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.
 20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
 21. 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.
 22. 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.
 23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

24. от 30 августа 2002 г. № 282.
25. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
26. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
27. от 31 августа 2010 г. № 416/489.
28. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
29. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
30. 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.
31. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
32. 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
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
36. 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. Госстандарт, 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 11 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.

3,2.3 Электронные ресурсы

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.

<https://urait.ru/bcode/456793>

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.

<https://urait.ru/bcode/449548>

3. 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.

<https://urait.ru/bcode/451933>

4. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
5. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
6. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
7. Справочно-правовая система «Консультант Плюс» www.consultant.ru
8. Справочно-правовая система «Гарант» » www.garant.ru
9. Федеральный портал «Российское образование www.edu.ru
10. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
11. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>