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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по

МДК 02.01 Программные и программно-аппаратные средства защиты информации

для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Регистрационный №23ИБ/ ФОС

Санкт-Петербург
2023

Фонд оценочных средств по МДК 02.01 Программные и программно-аппаратные средства защиты информации 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 02.01 Программные и программно-аппаратные средства защиты информации 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. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу МДК 02.01 Программные и программно - аппаратные средства защиты информации.

КОС включают контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы МДК 02.01 Программные и программно - аппаратные средства защиты информации.

1.2 Система контроля и оценки освоения программы

Контроль и оценка результатов освоения МДК 02.01 Программные и программно - аппаратные средства защиты информации осуществляется преподавателем в процессе проведения экзамена.

Результаты обучения (освоенные умения, усвоенные знания), с учетом личностных результатов, профессионального стандарта	**Формы и методы контроля и оценки результатов обучения**
<u>умения:</u> — устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; — устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; — диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; — применять программные и программно-аппаратные средства для защиты информации в базах данных; — проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; — применять математический аппарат для выполнения криптографических преобразований; — использовать типовые программные криптографические средства, в том числе электронную подпись; — применять средства гарантированного	Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, экзамен Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, экзамен

уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; ~ осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. **знания:** – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	

2. Комплект оценочных средств

2.1 Типовые тестовые задания для оценки освоения МДК 02.01. Программные и программно - аппаратные средства защиты информации

Тестовое задание	Вариант ответа
1. Защита информации это-	А) потенциальная возможность неправомерного преднамеренного или случайного воздействия , приводящее к потере или разглашению информации.

	Б) реализация права на государственную тайну и конфиденциальную информацию В) устранение или нейтрализация негативных источников, причин и условий воздействия на информацию **Г) правовые, организационные и технические меры, направленные на обеспечение защиты информации**
2. Каналы утечки информации - это	А) это комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки информации **Б) методы и пути утечки информации из информационной системы** В) потенциальная возможность неправомерного преднамеренного или случайного воздействия Г) соблюдение конфиденциальности информации ограниченного доступа
3. Существуют следующие виды ПО (добавьте недостающее).	**А)** Прикладное ПО Б) Системное ПО **В) Инструментальное ПО**
4. К функциям ОС относится :	А) поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой **Б) управление процессором путем чередования выполнения программ;**

	В)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы; **Г)управление памятью путем выделения программам на время их выполнения требуемой памяти;**
5. Операционная система Windows является :	**А) многозадачной** Б) однозадачной **В) многопользовательской** Г) однопользовательской
6. Атаки на ОС бывают:	**А) Локальными** Б) Глобальными **В) Удаленными** Г) Близкими
7. Профессиональный взлом имеет следующую структуру (восстановите последовательность)	А) попытка внедрения вредоносных программ Б) поиск уязвимостей в ПО ЗИ В) тщательный анализ ПО Г) анализ выбранной политики безопасности **Ответ Г,В,Б,А**
8. Когда пользователь знает что-то, что подтверждает его подлинность, то существуют следующие способы аутентификации:	**А) парольная аутентификация** Б) аутентификация по магнитному носителю В) модель рукопожатия Г) аутентификация по характеристикам работы пользователя
9. Когда пользователь что-то имеет, что подтверждает его подлинность, то существуют следующие способы аутентификации:	А) парольная аутентификация **Б) аутентификация по магнитному носителю** В) модель рукопожатия Г) аутентификация по характеристикам работы пользователя
10. К защите от удаленного НСД можно отнести:	**А) модель рукопожатия Б) Протокол Kerberos**

	В) Аутентификация по биометрическим характеристикам Г) Аутентификация по росписи мышью
11. Целью защиты информации является:	А) предотвращение хищения, утечки, искажения, утраты и подделки информации; **Б) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;** В) реализация права на государственную тайну и конфиденциальную информацию Г) выявление правил и норм поведения человека, направленные на обеспечение безопасности информации
12. К основным видам средств защиты информации относится:	**А) нормативно-правовые** **Б) Технические** В) Экологические Г) Этнические
13. Технические средства защиты - это	А) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации **Б) это комплексы специального технического и программного обеспечения** В) правила и нормы поведения, направленные на обеспечение безопасности информации

	Г) законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе
14. К каналам утечки информации относится:	**А) Магнитный канал** **Б) Виброакустический канал** **В) Лазерный канал** Г) Специальный канал
15. К назначению ОС относится:	А)управление процессором путем чередования выполнения программ; Б)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы; В)у правление памятью путем выделения программам на время их выполнения требуемой памяти; **Г)поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой;**
16. Многопроцессорная обработка в ОС бывает:	**А) Симметричной** Б) Квадратичной В) Полной **Г) Ассиметричной**
17. К локальной защите от НСД относится:	**А) Аутентификация на основе биометрических характеристик** Б) Протокол CHAP **В) Парольная аутентификация** Г) Проток PAP
18. Когда пользователь и есть то лицо, за которое себя выдает то существуют следующие способы аутентификации:	А) парольная аутентификация Б) аутентификация по магнитному носителю

	В) модель рукопожатия **Г) аутентификация по характеристикам работы пользователя**
19. Какой протокол направленный для защиты от удаленного НСД основан на использовании одноразовых паролей.	А) PAP Б) CHAP **В) S/KEY** Г) Kerberos
20. К недостаткам дискреционного управления доступом относится:	А) **нельзя контролировать утечку конфиденциальной информации** Б) неудобство для пользователя В) нет опасности утечки конфиденциальной информации Г) слабая защита от вредоносных программ

Критерии оценки:

Количество правильных ответов	**Процент выполнения**	**Оценка**
19-20	**более 90%**	**Отлично**
17-18	**80-90%**	**Хорошо**
14-16	**60-79%**	**Удовлетворительно**
До 13	**менее 60%**	**Неудовлетворительно**

Типовые практические задания:

1. Ограничение доступа на вход в систему.
2. Идентификация и аутентификация пользователей.
3. Разграничение доступа.
4. Регистрация событий (аудит).
5. Контроль целостности данных
6. Уничтожение остаточной информации.
7. Распределение каналов в соответствии с источниками воздействия на информацию.
8. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО.
9. Защита информации от несанкционированного копирования с использованием специализированных программных средств.
10. Применение средства восстановления остаточной информации на примере Foremost или аналога.
11. .Применение специализированного программно средства для восстановления удаленных файлов.
12. Применение программ для безвозвратного удаления данных.

Критерии оценивания

«5» «отлично» или «зачтено» - студент показывает глубокое и полное овладение содержанием программного материала, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» или «зачтено» - студент в полном объеме освоил программный материал, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» или «зачтено» - студент обнаруживает знание и понимание основных положений программного материала, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» или «не зачтено» - студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

3. Информационное обеспечение

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им,

используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с

2. 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.

3. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н.Криптографическая защита информации в объектах информационной инфраструктуры, 1-е изд., ИЦ АКАДЕМИЯ ,2020 -288 с.

4. 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.

Дополнительные источники:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. - М.: МЦНМО, 2006 г

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. 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».

10. Положение о сертификации средств защиты информации.

Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

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

от 30 августа 2002 г. № 282.

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

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

от 31 августа 2010 г. № 416/489.

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

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. 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.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.

№ 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации

шифровальных (криптографических) средств защиты информации».

23. 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

24. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

25. 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

26. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

27. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

28. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

29. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

30. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

31. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

32. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

33. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

34. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

35. 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.

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

37. ГОСТ Г ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт,

2012.

38. ГОСТ Г 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). Госстандарт, 2013.

39. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК Госсии 14 февраля 2008 г.

40. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией Госсии, 2002.

41. ГОСТ Г 50922-2006 Защита информации. Основные термины и определения. Гостехрегулирование, 2006.

42. ГОСТ Г 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Гостехрегулирование, 2006.

43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией Госсии, 2002.

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

45. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК Госсии И февраля 2014 г.

46. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК Госсии 25 декабря 2006 г.

47. программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

48. базы данных, информационно-справочные и поисковые системы: www.fstec.ru;www.gost.ru/wps/portal/tk362.

Электронные издания (электронные ресурсы):

1.1. 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» htpp\\:www.ict.edu.ru

12. Сайт Научной электронной библиотеки www.elibrary.ru.Цифровая **образовательная среда СПО РИОГобразование:**

- Пащинская, Л. И. Социально-экономические аспекты современного общества : учебное пособие / Л. И. Пащинская. — Воронеж : Воронежский государственный университет инженерных технологий, 2018. — 208 с. — ISBN 978-5-00032-3 79-3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/88435 (дата обращения: 12.07.2020). — Режим доступа: для авторизир. пользователей