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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по

МДК 02.02 Криптографические средства защиты информации

для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Регистрационный №23ИБ/ ФОС

Санкт-Петербург
2023

Фонд оценочных средств по МДК 02.02 Криптографические 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 02.02 Криптографические 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 02.02 Криптографические средства защиты информации.

КОС включают контрольные материалы для проведения промежуточной аттестации.

КОС разработан на основании рабочей программы МДК 02.02 Криптографические средства защиты информации.

1.2 Система контроля и оценки освоения программы практики .

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**
умения: — 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 уничтожения информации;	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

— 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 02.02.

1 . Алгебраические структуры. Группы. Кольца. Поля. Кольца многочленов

2 . Алгебраические структуры. Поля GF(2n). Полиномы

3 . Современные блочные шифры. Подстановка, транспозиция. Атаки на блочные шифры.

4 . Полноразмерные ключевые шифры. Шифр без ключа

5 . Компоненты современного блочного шифра. P-блоки.

6 . Компоненты современного блочного шифра. S-блоки

7 . Компоненты современного блочного шифра. Понятие операции

"исключающее или".

8 . Компоненты современного блочного шифра. Операция циклического сдвига.

9 . Компоненты современного блочного шифра. Замена. Разбиение и объединение

10 .Составной шифр. Рассеивание и перемешивание. Понятие раунда

11 .Схема Фейстеля и не-Фейстеля

12 .Современные блочные криптосистемы

13 .Симметричные стандарты шифрования - DES

14 .Симметричные стандарты шифрования - AES

15 .Симметричные стандарты шифрования - ГОСТ 28147-89

16 .Современные поточные шифры

17 .Синхронные шифры потока. Одноразовый блокнот

18 .Матрица состояний потоковых шифров. Алгоритм шифрования RC4

19 .Линейные генераторы псевдослучайных последовательностей.

20 .Генераторы псевдослучайных последовательностей. Датчики Фибоначчи

21 .Генераторы псевдослучайных последовательностей. Алгоритм BBS

22 .Принципы использования ГПсЧ при потоковом шифровании

23 .Понятие простого числа. Испытание простоты чисел

24 .Функция Эйлера. Понятие хеш-функции

25 .Шифры с открытыми ключами. Асимметричные системы шифрования ГОСТ 94

26 .Шифры с открытыми ключами. Асимметричные системы шифрования RSA

27 .Криптосистемы на основе эллиптических уравнений

2 8. Экономика информационной безопасности на примере оценки криптосистем

29 .Оценка эффективности криптографической защиты

30 .Квантовые алгоритмы шифрования

Типовые практические задания:

1. ОКольца многочленов. Задача на построение кольца многочленов
2. Конечные поля. Задача на построение конечных полей заданного порядка
3. Задача на построение модели блочного шифра подстановки как шифра перестановки
4. Задача на составление отношений между входами/выходами для S-блока
5. Задача на реализацию компонентов современного блочного шифра. P-блоки.
6. Задача на реализацию компонентов современного блочного шифра. Понятие операции "исключающее или".
7. Задача на реализацию компонентов современного блочного шифра.

Операция циклического сдвига.

8. Задача на реализацию компонентов современного блочного шифра. Замена. Разбиение и объединение
9. Задача на реализацию шифрования по схеме Фейстеля
10. Задача на реализацию алгоритма шифрования - DES
11 .Задача на реализацию алгоритма шифрования - AES
12. Задача на реализацию алгоритма шифрования - ГОСТ 28147-89
13. Задача на реализацию алгоритма шифрования RC4
14. Задача на реализацию алгоритма шифрования с помощью линейного конгруэнтного ГПсЧ
15. Задача на реализацию алгоритма шифрования с помощью ГПсЧ с задержкой по методу Фибоначчи
16. Задача на реализацию алгоритма шифрования с помощью алгоритма BBS
17. Задача на реализацию алгоритма шифрования Эль Гамаля
18. Задача на реализацию алгоритма шифрования RSA
19. Задача на применение протокола обмена ключами Диффи-Хелмана
20. Задача на применение ЭЦП на основе алгоритма шифрования с открытым ключом
21. **Критерии оценивания**

«5» «отлично» или «зачтено» - студент показывает глубокое и полное овладение содержанием программного материала по практике 1111 02, 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 по практике ПП 02, 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 по практике ПП 02 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 по практике 1111 02, 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. — 312с.

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 3 0 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. Росстандарт, 2014.

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

37. 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.

3. 8. 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.

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

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

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

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

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

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

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

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

47. 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. — 312с. 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»

11. http://www.law.edu.ru/

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