Утверждаю
Зам. директора по УР
«31» 08 2023г.

Иванешко И.В.

Согласовано
Ведущий специалист-эксперт отдела по защите информации ГУ-ОПФ по Смоленской области
«31» 08 2023г.

Ефремов А.А.,

Контрольно-оценочные средства для промежуточной аттестации
по МДК 02.02 Криптографическая защита информации
для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Экзамен является промежуточной формой контроля, подводит итог освоения МДК 02.02 Криптографическая защита информации.

Профессиональные компетенции:

ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

Общие компетенции:
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 09. Использовать информационные технологии в профессиональной деятельности.

Экзамен по МДК 02.02 Криптографическая защита информации проводится в форме тестирования.

Тест содержит 20 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 50 вопросов, второй блок 75 вопросов) заданий по 10 вопросов. Время тестирования – 80 минут для каждой подгруппы (по 3 минуты на каждый вопрос из первого блока, по 5 минуты на каждый вопрос закрытого типа). Для прохождения тестирования, студенты разбиваются на три подгруппы (по количеству персональных компьютеров в сдаваемой аудитории). Время на подготовку и проверку тестирования – 30 мин.

Критерии оценивания
«5 баллов» - получают студенты, справившиеся с работой 100-90%;
«4 балла» - ставится в том случае, если верные ответы составляют 89-76% от общего количества;
«3 балла» - соответствует работа, содержащая 60-75% правильных ответов;
«2 балла» - соответствует работа, содержащая менее 60% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
5 «отлично»	Студент набрал 5 баллов
4 «хорошо»	Студент набрал 4 балла
3 «удовлетворительно»	Студент набрал 3 балла
2 «неудовлетворительно»	Студент набрал 0-2 балла

Первый блок

Формируемые компетенции ОК 01, ОК2, ОК3, ОК9, ПК 2.3

1. Что такое шифрование?
а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
в) удобная среда для вычисления конечного пользователя
2. Что такое кодирование?
а) преобразование обычного, понятного текста в код
б) преобразование
в) написание программы

3. Что требуется для восстановления защитного текста?
а) ключ
б) матрица
в) вектор

4. Что за секретная информация, которая хранится в Windows? (Выберите три правильных ответа)
а) пароли для доступа к сетевым ресурсам
б) пароли для доступа в Интернет
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере+

5. Какие примеры алфавитов правильные? (Выберите два правильных ответа)
а) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8
б) восьмеричный и шестнадцатеричный алфавиты
в) AEE

6. Что такое шифрование?
а) преобразовательный процесс исходного текста в зашифрованный
б) упорядоченный набор из элементов алфавита
в) нет правильного ответа

7. Что такое дешифрование?
а) на основе ключа шифрованный текст преобразуется в исходный
б) пароли для доступа к сетевым ресурсам
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

8. Что представляет собой криптографическая система?
а) семейство T преобразований открытого текста, члены его семейства индексируются символом k
б) программу
в) систему

9. Что такое пространство ключей k?
а) набор возможных значений ключа
б) длина ключа
в) нет правильного ответа

10. На какие виды подразделяют криптосистемы? (Выберите три правильных ответа)
а) симметричные
б) ассиметричные
в) с открытым ключом

11. Какого количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования?
а) 1
б) 2
в) 3

12. Какого количество используемых ключей в системах с открытым ключом?
а) 2
б) 3
в) 1

13. Какие есть ключи, используемые в системах с открытым ключом? (Выберите два правильных ответа)
а) открытый
б) закрытый
в) нет правильного ответа

14. Как связаны ключи друг с другом в системе с открытым ключом?
а) математически
б) логически
в) алгоритмически

15. Что принято называть электронной подписью?
а) присоединяемое к тексту его криптографическое преобразование
б) текст
в) зашифрованный текст

16. Что такое криптостойкость?
а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
б) свойство гаммы
в) все ответы верны

17. Что относится к показателям криптостойкости? (Выберите два правильных ответа)
а) количество всех возможных ключей
б) среднее время, необходимое для криптоанализа +
в) количество символов в ключ

18. Каковы требования, предъявляемые к современным криптографическим системам защиты информации? (Выберите три правильных ответа)
а) знание алгоритма шифрования не должно влиять на надежность защиты
б) структурные элементы алгоритма шифрования должны быть неизменными
в) не должно быть простых и легко устанавливаемых зависимостью между ключами

19. Какие следующие обширные требования сформулированы для современных криптографических систем защиты? (Выберите два правильных ответа)
а) длина шифрованного текста должна быть равной лине исходного текста

б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа
в) нет правильного ответа

20. Какие основные современные методы шифрования? (Выберите три правильных ответа)
а) алгоритм гаммирования
б) алгоритмы сложных математических преобразований +
в) алгоритм перестановки

21. Какого преимущество RSA над DSA?
а) Он может обеспечить функциональность цифровой подписи и шифрования
б) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
в) Это блочный шифр и он лучше поточного
г) Он использует одноразовые шифровальные блокноты

22. Какова эффективная длина ключа в DES?
а) 56
б) 64
в) 32
г) 16

23. Что за процесс, выполняемый после создания сеансового ключа DES?
а) Подписание ключа
б) Передача ключа на хранение третьей стороне (key escrow)
в) Кластеризация ключа
г) Обмен ключом

24. Какое правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты?
а) Оно обеспечивает проверку целостности и правильности данных
б) Оно требует внимательного отношения к процессу управления ключами
в) Оно не требует большого количества системных ресурсов
г) Оно требует передачи ключа на хранение третьей стороне (escrowed)

25. Какова основная цель использования одностороннего хэширования пароля пользователя?
а) Это снижает требуемый объем дискового пространства для хранения пароля пользователя
б) Это предотвращает ознакомление кого-либо с открытым текстом пароля
в) Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
г) Это предотвращает атаки повтора (replay attack)

Формируемые компетенции ОК 01, ОК2, ОК3, ОК9, ПК 2.1, ПК 2.2

26. Что такое ядро безопасности?
1) совокупность аппаратных, программных и специальных компонент вычислительных сетей, реализующих функции защиты и обеспечения безопасности
2) состояние защищенности информации, хранимой и обрабатываемой в автоматизированной системе, от негативного воздействия на нее
3) совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности
4) совокупность норм и правил, регламентирующих безопасность компьютерных сетей

27. Что такое защита информации?
1) ненадежный контакт при подключении компьютера
2) события или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации

3) возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации

4) процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности

28. Совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности. Что это?

1) политика безопасности (Security Policy)
2) качество информации
3) уязвимость информации
4) конфиденциальность информации

29. Какого понятие дискреционного или произвольного управления доступом? (Discretionary Access Control).

1) возможность удаленного доступа к ресурсам
2) управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов
3) использование биометрических свойств пользователей
4) доступ без использования пароля

30. Каковы принципы построения защиты в автоматизированных системах?

1) системность, комплексность, непрерывность защиты, разумная достаточность, гибкость управления и применения, открытость алгоритмов и механизмов защиты, простота применения защитных мер и средств
2) отсутствие технического персонала
3) малые габариты устройств
4) низкая стоимость

31. На каком принципе основана защита компьютерных систем, предполагающая необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов?

1) на принципе непрерывности защиты
2) на принципе системности защиты
3) на принципе гибкости защиты
4) на принципе разумной достаточности

32. Какие есть методы защиты от копирования информации?

1) отключение принтера
2) удаление из компьютера накопителей для гибких CD-дисков
3) нестандартное форматирование носителя информации, перепрограммирование контроллеров внешнего запоминающего устройства, аппаратные регулировки и настройки, изменение алгоритма подсчета контрольной суммы
4) архивирование файлов

33. Шифрование, архивация, использование самогенерирующих кодов, «обман» дизассемблера. Что это?

1) методы защиты от копирования
2) методы защиты от вирусов
3) организация мандатного доступа
4) методы защиты от дизассемблирования

34. С помощью каких программ осуществляют отладку и дизассемблирование?

1) отладчики
2) редакторы графических изображений
3) программы-симуляторы
4) электронные таблицы

35. Уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы. Что это?

1) программа архиватор
2) идентификатор
3) криптографический ключ
4) программа-отладчик

36. Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных. Что это?
1) процесс дисассемблирования
2) процесс блочного криптографического преобразователя
3) процесс идентификации
4) процесс расшифрования закрытого текста

37. Что такое аутентификации?
1) присвоение пользователю идентификатора
2) уникальное количество информации о пользователе
3) метод расшифрования
4) присвоение принадлежности пользователю предъявленного им идентификатора (подтверждение или проверка подлинности)

38.Что такое учетная запись пользователя?
1) совокупность идентификатора и пароля
2) программа для идентификации пользователя
3) метод зашифрования
4) криптографический ключ

39. Что такое парольная система
1) секретное сообщение
2) программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей автоматизированной системы на основе одноразовых или многоразовых паролей
3) техническая система (турникет) для доступа граждан
4) система защиты от механического повреждения компьютера

40. Что такое криптографическая защита информации?
1) процесс подтверждения аутентичности документов с помощью электронной цифровой подписи
2) процесс вычисления ХЭШ-функций
3) преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий, при этом факт передачи информации не скрывается
4) процесс передачи информации в телекоммуникационных системах

41. Что такое зашифрование?
1) преобразование закрытого текста в открытый
2) процесс генерирования ключей
3) процесс аутентификации электронной цифровой подписи
4) процесс криптографического преобразования множества открытых сообщений во множество закрытых

42. Что такое расшифрование?
1) процесс криптографического преобразования множества закрытых сообщений во множество открытых
2) процесс, обратный гаммированию
3) получение ключей криптографического преобразователя
4) незаконный процесс формирования открытого текста в закрытый

43. Что такое дешифрование
1) процесс получения открытого текста с помощью гаммы
2) процесс преобразования открытого текста в закрытый
3) процесс нахождения открытого сообщения, соответствующему заданному закрытому при неизвестном криптографическом преобразовании
4) процесс создания электронной цифровой подписи

44. Что такое ключ зашифрования?
1) специальная карточка для организации доступа

2) определенное число
3) размер управляющей программы в битах
4) управляющая информация, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма криптографического преобразования

45. Какие есть типы ключей криптографического преобразования?
1) симметричные, асимметричные
2) символы алфавита, цифры
3) механические, электронные
4) короткие и длинные

46. Какой основные способы криптографического преобразования?
1) вычисления
2) замена и перестановка
3) формирование блоков
4) ручной и автоматизированный

47. Какова основная характеристика криптографических методов защиты?
1) стоимость
2) размер программы
3) криптостойкость
4) удобство использования

48. Что такое блочное криптографическое преобразование?
1) последовательное преобразование каждого символа открытого текста в закрытый
2) передача открытого текста по блокам
3) этап формирования гаммы
4) многократное математическое преобразование блока открытого текста в закрытый

49. Что такое алгоритм поточного криптографического преобразования?
1) последовательное преобразование каждого символа открытого текста в закрытый с помощью гаммы +
2) этап генерирования ключей
3) процесс аутентификации
4) разбивка открытого текста на блоки

50. Что такое электронная цифровая подпись (ЭЦП)?
1) программа, обеспечивающая мандатный доступ
2) виртуальное подтверждение аутентичности документов
3) разновидность антивирусной программы
4) способ преобразования открытого текста в закрытый

Второй блок

Формируемые компетенции ОК1, ОК2, ОК3, ОК9, ПК2.1. ПК 2.2

1. Что понимается под DoS-атакой?
2. Как может создаваться код аутентификации сообщения (MAC)?
3. Атака «man in the middle» является чем?
4. Для чего используются в криптографии сдвиговые регистры с обратной связью?
5. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?
6. Какие сбои оборудования бывают?
7. Какие потери информации, связанные с несанкционированным доступом, бывают?
8. Как называются средства защиты данных, функционирующие в составе программного обеспечения?
9. Какие Вы знаете программные средства защиты информации?
10. Что такое программное средство защиты информации?
11. Что такое тональный сигнал?

12. Что представляет наибольшую угрозу для безопасности сети?
12. На что можно разделить программные средства защиты?
13. Когда срабатывает сигнал самоуничтожения программы?

13. Занимается обеспечением скрытности информации в информационных массивах. Что это?
14. Какие методы защиты от копирования информации Вы знаете?
15. Что является объектами защиты?
16. Какие системы включает криптография?
17. Какие классы Вы знаете криптографических СЗИ?
18. Криптографические средства класса КС1, что делают?
19. Какие из сервисов реализуются при использовании криптографических преобразований?
20. Что позволяет предотвратить использование криптографических преобразований?
22. Какие есть механизмы защиты информационных систем от несанкционированного доступа?
23. Что делает функция технологии RAID ?
24. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст?
25. Генерация ключей, для которой используются случайные значения, называется Функцией генерации ключей (KDF). Какие значения обычно не используются при этом в процессе генерации ключей?

Составил преподаватель _____Скряго О.С.

Рассмотрено на заседании МК компьютерных сетей и администрирование
Протокол №1 от 31.08.2023г
Председатель МК_____О.С. Скряго