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
6 семестр
для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Промежуточная аттестация по МДК 02.02 Криптографическая защита информации, которая проходит в 6 семестре является другая форма аттестации в виде тестирования.

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.

Тест содержит 10 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 30 вопросов, второй блок 20 вопросов) заданий по 5 вопросов. Время тестирования – 45 минут для каждой подгруппы (по 3 минуты на каждый вопрос из первого блока, по 6 минут на каждый вопрос закрытого типа).

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, ПК21., ПК 2.2, 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 операционной системе? (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. Какое 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)

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

Второй блок

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

1. Какие методы защиты от копирования информации Вы знаете?
2. Что такое пространство ключей k?
3. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
4. Какие основные методы шифрования вы знаете?
5. Что такое криптоанализ?
6. Что такое шифр перестановки?
7. Что такое кодирование?
8. Что такое OpenSSL?
9. Что поддерждивает OpenSSL?
10. В каком виде OpenSSL доступна для большинства UNIX-подобных операционных систем?
11. Что такое протокол Диффи-Хелмана?
12. На какое количество пользователей применяется алгоритм Диффи-Хелмана?
13. Что такое асимметричное шифрование?
14. Что такое электронная подпись?
15. Что такое сертификат ключа проверки электронной подписи ?
16. Какие функции выполняет ЭЦП?
17. Какой ключ должен обязательно присутствовать в документе с ЭЦП?
18 . Какие действия можно выполнять с документом, подписанным ЦП?
19. Какая информация хранится в ЭЦП?
20. Какие существуют системы сертификатов ЭЦП?

Составил преподаватель Скряго О.С.