Министерство науки и высшего образования Российской федерации
Калужский филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»

РАССМОТРЕНО и **ОДОБРЕНО**

на методическом семинаре кафедры *ИУК4 «Программное обеспечение ЭВМ, информационные технологии»*

Протокол № 51.4/02 от « 18 » ноября 2020 г.
Зав.кафедрой_____/Гагарин Ю.Е./

ВОПРОСЫ К ЭКЗАМЕНУ

по дисциплине «Защита информации»
для студентов групп ИУК4-71Б, ИУК4-72Б

Модуль 1 «Основные понятия и определения предмета защиты информации.

Элементы криптоанализа.»

Оценка знаний.

1. Раскройте специфику угроз безопасности информации. Опишите состояния проблемы обеспечения безопасности на объектах информационной безопасности
2. Раскройте сущность безопасной деятельности предприятия, организации. Охарактеризуйте принципы построения и функционирования системы защиты.
3. Опишите сущность вопросов, касающихся элементов теории чисел.
4. Дайте определение простых и составных чисел. Перечислите и раскройте свойства простых чисел
5. Перечислите основные группы методов защиты секретных посланий и приведите область их применения.
6. Изложите требования к криптографическим системам защиты информации.
7. Раскройте сущностью процесса управления криптографическими ключами.
8. Опишите задачу факторизации чисел. Дайте определение наибольшего общего делителя.
9. Опишите роль числовых функций, имеющих большое значение в теории чисел и в криптографии.
10. Изложите концепцию хеширования. Перечислите основные свойства хеш-функции.

Оценка умений.

Сравните криптоалгоритмы с точки зрения количества ключей.

1. Опишите особенности традиционных симметричных криптосистем.
2. Объясните принцип работы современных симметричных криптосистем.
3. Классифицируйте современные асимметричные криптосистемы.
4. Охарактеризуйте системы шифрования с открытым ключом.
5. Сравните системы хеширования.
6. Раскройте сущностью процесса управления криптографическими ключами.
7. Выделите наиболее важные принципы действия электронной цифровой подписи

8. Сравните алгоритмы шифрования биграммами и шифра Гронсфельда, выявите их эффективность и надежность.
9. Сравните Аффинную криптосистему и квадрат Полибия, выявите их эффективность и надежность.
10. Опишите особенности традиционных симметричных криптосистем.

Оценка владения навыками

1. Предложите процедуру установки ЭЦП (подписывание документа) и обоснуйте ее
2. Выполните анализ современного состояния проблемы безопасности и обоснуйте его.
3. Предложите процедуру проверки ЭЦП (аутентификация документа) и обоснуйте ее.
4. Предложите схему установки ЭЦП(подписывание документа) и обоснуйте ее.
5. Предложите два наиболее эффективных метода шифрования информации и аргументируйте свое решение на примерах.
6. Дайте прогноз применения быстрой ЭЦП и поясните свое мнение.
7. Предложите методы разрешения коллизий.
8. Предложите последовательность действий при ассимитричном шифровании .
9. Выполните анализ криптоаналитических атак.
10. Зашифруйте и расшифруйте сообщение "экзамен" по алгоритму RSA.

Модуль 2 «Контроль целостности информации»

Оценка знаний.

1. Раскройте значение функций хеширования в технологии электронно-цифровой подписи.
2. Опишите назначение электронно-цифровой подписи (ЭЦП).
3. Опишите назначение криптографических хеширущих алгоритмов.
4. Раскройте сущность безопасной деятельности предприятий, организаций. Охарактеризуйте принципы построения и функционирования системы защиты.
5. Перечислите основные группы методов защиты секретных посланий и поясните область их применения.
6. Раскройте специфику угроз безопасности информации. Опишите состояния проблемы обеспечения безопасности на объектах информационной безопасности.
7. Изложите концепцию хеширования. Перечислите основные свойства хеш-функции.
8. Охарактеризуйте основные виды угроз безопасности сети.
9. Перечислите и раскройте источники угроз по отношению к ЛВС.
10. Изложите концепцию защиты от несанкционированного доступа.

Оценка умений.

1. Раскройте сущностью процесса управление криптографическими ключами.
2. Охарактеризуйте наиболее важные принципы действия электронной цифровой подписи.
3. Сравните системы хеширования.
4. Опишите особенности основных методов выявления устройств перехвата информации.
5. Классифицируйте современные асимметричные криптосистемы.
6. Охарактеризуйте системы шифрования с открытым ключом.
7. Перечислите основные методы построения ЭЦП.

8. Перечислите и раскройте методы и средства защиты информации в информационных системах.
9. Раскройте основные принципы формирования «безопасных» паролей.
10. Раскройте концепции Dos атак и приведите методы защиты от них.

Оценка владения навыками

1. Выполните анализ современного состояния проблемы безопасности и обоснуйте его.
2. Дайте прогноз применения быстрой ЭЦП и поясните свое решение.
3. Выполните анализ криптоаналитических атак.
4. Сформулируйте принцип работы гибридной схемы распределения ключей.
5. Раскройте принципы проверки на наличие уязвимостей и действия в случае их обнаружения.
6. Сформулируйте принцип работы алгоритма RSA для шифрования и дешифрования.
7. Приведите классификацию подходов к распределению ключей.
8. Проиллюстрируйте на примере распределение ключей по методу Диффи-Хеллмана
9. Сформулируйте принцип работы гибридной схемы распределения ключей
10. Опишите алгоритм электронной подписи RSA.

Модуль 3 «Практические аспекты сетевой безопасности. Защита информации в информационных системах различного вида»

Оценка знаний.

1.Опишите основные методы обеспечения безопасности информации.

2.Опишите основные методы выявления устройств перехвата информации

3. Раскройте физическую сущность «микрофонного эффекта».

4.Перечислите и раскройте воздушные и вибрационные технические каналы утечки информации.

5. Изложите концепцию защиты электронной почты.

6. Приведите классификацию систем сигнализации в сетях связи.

7. Раскройте область применения и перечислите основные свойства цифровых подписей.

8. Приведите основные типы атак методом SQL-инъекций, методы обнаружения и защиты от этих атак.

9. Опишите концепцию использования хеш-функций различной длины.

10. Дайте определение термину стеганография и раскройте область ее применения.

Оценка умений

1.Изложите концепции идентификации пользователей и установления подлинности.

2. Изложите концепции защиты электронной документации.

3. Изложите концепции электронного документооборота.

4. Изложите концепции прямого подключения к телефонным и телеграфным линиям.

5. Опишите особенности реагирования системы на несанкционированный доступ.

6. Опишите механизм регистрации обращений к защищенным ресурсам.

7. Сравните достоинства и недостатки использования контейнера-изображения и звукового контейнера в компьютерной стеганографии.

8. Опишите действия для предотвращения несанкционированных операций над содержимым баз данных SQL –серверов.

9. Перечислите основные методы построения ЭЦП.

10. Изложите концепции идентификации пользователей и установления подлинности.

Оценка владения навыками

1.Раскройте принцип работы однонаправленных хеш-функций. Приведите метод удлинения хеш-значений.

2. Сформулируйте принцип работы алгоритма Эль-Гамаля.

3. Приведите основные принципы компьютерной стенографии.

4. Сформулируйте основные цели высокочастотного навязывания.

5. Проиллюстрируйте на примере понятие «SQL Injection».

6. Обоснуйте важность встраивания механизмов защиты от некорректных входных данных на этапе разработки программного обеспечения.

7. Раскройте принципы проверки на наличие уязвимостей и действия в случае их обнаружения.

8. Классифицируйте каналы проникновения в систему.

9. Сформулируйте принцип работы алгоритма Дифи-Хелманна.

10. Обоснуйте важность применения ЭЦП