СОГЛАСОВАНО

Председатель Учебно-методической комиссии по специальности 2301

_____ Сюзев В.В.
"____" _____ 2007 года

УТВЕРЖДАЮ

И.О. Ректора Московского государственного технического университета гражданской авиации

_____ Елисеев Б.П.
"____" _____ 2007 года

Ф О Н Д
контрольных заданий
по дисциплине
"Методы и средства защиты информации"
специальность 230103
4 курс

Заведующий кафедрой ВМКСС _____ (В.В. Соломенцев)

Ответственный преподаватель _____ (А.И. Терентьев)

Москва, 2007 г.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 1

1. Определение и свойства информации.

2. Определение, свойства и примеры практического применения функции хэширования (хэш-функции).

3. Методы и средства защиты информации от вредоносных программ.

4. Вычислить открытый (*E*) и закрытый (*D*) криптографические ключи (алгоритм RSA) при значениях $P = 3$ и $G = 17$.

5. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{zi-1}(m_i \quad z_{i-1}) \quad m_i$

КОНТРОЛЬНОЕ ЗАДАНИЕ № 2

1. Абстрактные графические модели систем защиты информации.

2. На какой математической проблеме основана криптостойкость шифрования по алгоритму RSA?

3. Средства администрирования ОС Windows NT/2000/XP для защиты информации в автономных ПЭВМ и локальных компьютерных сетях.

4. Определить размерность хэш-значения, если функция хэширования построена на базе блочного шифратора по алгоритму ГОСТ 28147-89.

5. При какой длине криптографического ключа имеет максимальную криптостойкость аддитивный шифр по методу "одноразовый шифр-блокнот", если длина шифруемого блока (открытого текста) составляет 200 бит.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 3

1. Основные виды и классификация вредоносных программ. Типы программных закладок. Методы и средства защиты от вредоносных программ.

2. Принципы построения и требования к современным криптографическим системам.

3. Сколько классов защищенности средств вычислительной техники от НСД к информации установлено руководящим документом Гостехкомиссии России "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"?

4. Приведите пример двух составных чисел, являющихся взаимно простыми.

5. Приведите пример построения матрицы доступа (размерность не менее 5 5) к файлам компьютерной системы.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 4

1. Информационные процессы и жизненный цикл информации.

2. Криптографические методы защиты компьютерной информации от несанкционированного доступа и модификации: основные понятия и определения. Исторический обзор примитивных методов шифрования.

3. Основное назначение датчика (извещателя) охранно-пожарной сигнализации.

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{mi}(z_{i-1})$ z_{i-1}

5. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 3$ и $G = 19$.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 5

1. Государственные стандарты Российской Федерации в области защиты информации.

2. Алгоритмы шифрования с открытым ключом. Алгоритм шифрования RSA.

3. Какое количество циклов (раундов) шифрования установлено в стандарте криптографического преобразования DES?

4. Вычислить – $a \bmod b$, где a - последние две цифры номера зачетной книжки, b - сумма последних двух цифр номера зачетной книжки.

5. Какую размерность может иметь хэш-значение, если функция хэширования построена на базе блочного шифратора по алгоритму Rijndael (AES).

КОНТРОЛЬНОЕ ЗАДАНИЕ № 6

1. Характерные угрозы и атаки на информационные ресурсы автоматизированных систем. Назначение и функции подсистемы информационной безопасности автоматизированной системы.

2. Определение и примеры простого числа.

3. Алгоритм электронной цифровой подписи Эль-Гамаля.

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{zi-1}(m_i)$ z_{i-1} m_i

5. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 3$ и $G = 23$.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 7

1. Модель потенциального нарушителя.

2. Общие технические требования и классы защищенности средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, установленные руководящими документами Государственной технической комиссии при Президенте Российской Федерации.

3. Сколько ключей используется в асимметричных криптографических системах?

6. Определить размерность хэш-значения, если функция хэширования построена на базе блочного шифратора по алгоритму DES.

4. Приведите пример построения матрицы доступа (размерность не менее 5 5) к файлам компьютерной системы.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 8

1. Иерархический принцип организации информационной системы предприятия.

2. Сравнительный анализ параметров современных алгоритмов шифрования с секретным ключом ГОСТ 28147-89 и Rijndael.

3. Сколько классов защищенности автоматизированных систем от НСД к информации установлено руководящим документом Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации"?

4. Вычислить – $a \bmod b$, где a - последние две цифры номера зачетной книжки, b - сумма последних двух цифр номера зачетной книжки.

5. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{zi\text{-}1}(m_i)$ $z_{i\text{-}1}$ m_i

КОНТРОЛЬНОЕ ЗАДАНИЕ № 9

1. Компьютерные вирусы, их классификация и признаки наличия вирусной инфекции. Методы и средства защиты от вредоносных программ.

2. Защита информации от НСД по каналам побочных электромагнитных излучений и наводок (ПЭМИН). Методы и средства защиты информации от утечки по каналам ПЭМИН.

3. Базовое требование (правило Кирхгофа), предъявляемое к современным системам шифрования.

4. Приведите примеры простых и взаимно простых чисел.

5. Сколько паролей (длина 8 символов) можно составить из строчных и прописных букв русского алфавита?

КОНТРОЛЬНОЕ ЗАДАНИЕ № 10

1. Определение канала утечки информации.

2. Алгоритм шифрования ГОСТ 28147-89.

3. Определение простого числа и взаимно простых чисел.

4. Приведите пример построения матрицы доступа (размерность не менее 5 5) к файлам компьютерной системы.

5. Найти мощность множества двоичных криптографических ключей длиной 64 бита.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 11

1. Объекты защиты информации и их классификация.

2. Идентификация и аутентификация пользователей в ОС Windows NT/2000/XP.

3. Какое количество циклов (раундов) шифрования установлено в стандарте криптографического преобразования DES?

4. Приведите пример двух составных чисел, являющихся взаимно простыми.

5. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{mi}(z_{i-1})$ m_i z_{i-1}

КОНТРОЛЬНОЕ ЗАДАНИЕ № 12

1. Классификация автоматизированных систем (согласно руководящему документу Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации").

2. Защита информации в распределенных компьютерных сетях. Защита информации в сети Internet.

3. Какую длину имеет ключ криптографического преобразования в отечественном стандарте (ГОСТ 28147-89)?

4. Приведите пример построения матрицы доступа (размерность не менее 5 5) к файлам компьютерной системы.

6. Найти мощность множества двоичных криптографических ключей длиной 256 бит.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 13

1. Информатизация и объекты информатизации. Объекты защиты компьютерной информации.

2. Защита юридической значимости электронных документов. Электронная цифровая подпись.

3. Основное назначение корректирующих (помехоустойчивых) кодов.

4. Вычислить $a \bmod b$, где a - последние две цифры номера зачетной книжки, b - сумма последних двух цифр номера зачетной книжки.

5. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 3$ и $G = 23$.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 14

1. Классификация методов защиты программного обеспечения от несанкционированного копирования (НСК). Структура системы защиты программного обеспечения от несанкционированного копирования (НСК).

2. Алгоритмы шифрования с открытым ключом. Алгоритм шифрования Эль-Гамаля.

3. Принципы мандатного (полномочного) разграничения доступа.

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{mi}(m_i \quad z_{i-1}) \quad z_{i-1}$

5. Приведите пример двух взаимно простых чисел, одно из которых является простым.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 15

1. Значение и задачи организационно-правового обеспечения в области защиты информации. Информация как объект гражданско-правовых отношений.

2. Защита информации от помех и умышленной модификации с помощью корректирующих (помехоустойчивых) кодов.

3. Какое количество циклов (раундов) шифрования определено в стандарте США на криптографическое преобразование данных Rijndael (AES)?

4. Приведите пример построения матрицы доступа (размерность не менее 5 5) к файлам компьютерной системы.

5. Какую корректирующую способность имеет помехоустойчивый код с минимальным расстоянием Хэмминга (кодовым расстоянием) $d = 5$?

КОНТРОЛЬНОЕ ЗАДАНИЕ № 16

1. Классификация угроз информации как объекту защиты и их источников.

2. Защита информации от несанкционированного доступа: назначение, структура и элементы систем контроля и управления доступом (СКУД).

3. Какую длину имеет ключ криптографического преобразования в стандарте шифрования DES?

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{mi \quad zi\text{-}1}(m_i) \qquad m_i$

5. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях P = 3 и 29.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 17

1. Политика безопасности. Модели разграничения доступа к информации.

2. Алгоритмы шифрования с секретным ключом. Алгоритм шифрования Rijndael.

3. Принципы избирательного (дискреционного) разграничения доступа.

4. Вычислить $a \bmod b$, где a - последние две цифры номера зачетной книжки, b - сумма последних двух цифр номера зачетной книжки.

5. Найти мощность множества двоичных криптографических ключей длиной 512 бит.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 18

1. Физические принципы работы датчиков (извещателей) охранно-пожарной сигнализации.

2. Принципы построения и требования к современным криптографическим системам. Симметричные, асимметричные и гибридные криптографические системы.

3. Современные средства физического разграничения доступа.

4. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 5$ и $G = 11$.

5. Приведите пример двух составных чисел, являющихся взаимно простыми.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 19

1. Методы защиты информации от несанкционированного доступа (НСД): управление доступом к объектам защиты информации, идентификация и аутентификация объекта (субъекта).

2. Алгоритмы шифрования с секретным ключом. Алгоритм шифрования DES.

3. Организационно-административные меры защиты от внедрения вредоносных программ.

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{mi \quad zi\text{-}1}(z_{i\text{-}1}) \qquad z_{i\text{-}1}$

5. Приведите пример построения матрицы доступа (размерность не менее 5 5) к файлам компьютерной системы.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 20

1. Классификация и характеристика технических средств разведки. Методы и средства противодействия техническим разведкам.

2. Какая длина блока данных для шифрования установлена в стандарте криптографического преобразования DES?

3. В чем заключается управление криптографическими ключами?

4. Какую корректирующую способность имеет помехоустойчивый код с минимальным расстоянием Хэмминга (кодовым расстоянием) $d = 3$?

5. Сколько паролей (длина 6 символов) можно составить из строчных и прописных букв русского алфавита?

КОНТРОЛЬНОЕ ЗАДАНИЕ № 21

1. Физическое ограничение доступа к защищаемым объектам. Инженерно-технические средства охраны.

2. Какую длину может иметь блок данных для шифрования в стандарте США на криптографическое преобразование данных Rijndael (AES)?

3. Назначение и цель использования средств архивирования и хранения информации.

4. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 5$ и $G = 17$.

5. Приведите пример двух составных чисел, являющихся взаимно простыми.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 22

1. Основные этапы и принципы проектирования систем защиты информации.

2. Симметричные блочные шифры. Принцип итерации. Конструкция Фейстеля.

3. Современные средства защиты персональных ЭВМ от внедрения компьютерных вирусов.

4. Вычислить – $a \bmod b$, где a - последние две цифры номера зачетной книжки, b - сумма последних двух цифр номера зачетной книжки.

5. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 7$ и $G = 17$.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 23

1. Принципы построения систем защиты программного обеспечения от несанкционированного копирования и распространения.

2. Реализация хэш-функций на базе блоковых шифраторов.

3. Организационно-административные меры защиты информации от несанкционированного копирования.

4. Приведите пример построения матрицы доступа (размерность не менее 5 5) в охраняемые (контролируемые) помещения воображаемого предприятия (организации).

5. Какую корректирующую способность имеет помехоустойчивый код с минимальным расстоянием Хэмминга (кодовым расстоянием) $d = 7$?

КОНТРОЛЬНОЕ ЗАДАНИЕ № 24

1. Идентификация и аутентификация личности, технических средств и документов.

2. Определение и свойства функций хэширования.

3. В каких алгоритмах шифрования используется конструкция (структура) Фейстеля?

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{mi \quad zi\text{-}1}(m_i) \qquad z_{i\text{-}1}$

5. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 7$ и $G = 19$.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 25

1. Элементы криптоанализа: частотное распределение букв в алфавите.

2. Методы и средства защиты информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

3. На какой математической задаче основана криптостойкость электронной цифровой подписи по алгоритму Эль-Гамаля?

4. Найти мощность множества криптографических ключей длиной 512 бит.

5. Сколько паролей (длина 6 символов) можно составить в случае использования в качестве символов прописных букв русского алфавита и цифр?

КОНТРОЛЬНОЕ ЗАДАНИЕ № 26

1. Принципы оценки эффективности систем защиты информации.

2. Достоинства и недостатки современных стандартов шифрования с секретным и открытым ключом.

3. Инженерно-технические средства охраны (примеры использования).

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{mi \quad zi\text{-}1}(z_{i\text{-}1}) \quad m_i$

5. Приведите пример построения матрицы доступа (размерность не менее 5 5) к файлам компьютерной системы.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 27

1. Взаимосвязь модели потенциального нарушителя и основных принципов проектирования систем защиты информации.

2. Простейшие методы шифрования информации: перестановки, замены, аддитивные (гаммирование).

3. Какой специальной структурой данных описываются атрибуты защиты объекта в операционных системах семейства Windows NT/2000/XP.

4. Вычислить – $a \bmod - b$, где a - последние две цифры номера зачетной книжки, b - сумма последних двух цифр номера зачетной книжки.

5. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{zi-1}(m_i \quad z_{i-1}) \quad m_i \quad z_{i-1}$

КОНТРОЛЬНОЕ ЗАДАНИЕ № 28

1. Криптографические методы защиты информации от несанкционированного доступа. Основные понятия и определения.

2. Физическое ограничение доступа к охраняемым объектам. Современные методы и средства.

3. Какую длину может иметь криптографический ключ в стандарте США на криптографическое преобразование данных Rijndael (AES)?

4. Сколько паролей (длина 8 символов) можно составить в случае использования в качестве символов строчных, прописных букв русского алфавита и цифр?

5. Построить простейший комбинированный (производный) шифр, используя методы перестановки и замены.

КОНТРОЛЬНОЕ ЗАДАНИЕ № 29

1. Основные нормативные правовые акты Российской Федерации в области информационной безопасности.

2. Общая классификация современных криптографических систем.

3. Назначение и применение охранно-пожарной сигнализации.

4. При какой длине криптографического ключа имеет максимальную криптостойкость аддитивный шифр по методу "одноразовый шифр-блокнот", если длина шифруемого блока (открытого текста) составляет 100 бит.

5. Какую корректирующую способность имеет помехоустойчивый код с минимальным расстоянием Хэмминга (кодовым расстоянием) $d = 9$?

КОНТРОЛЬНОЕ ЗАДАНИЕ № 30

1. Методы защиты информации от НСД: контроль и предотвращение доступа к аппаратуре.

2. Виды и классификация ошибок оператора, методы защиты от них.

3. Гибридные (комбинированные) криптографические системы.

4. Построить на основе блочного шифратора с секретным ключом схему функции хэширования $z_i = E_{zi-1}(m_i)$ m_i

5. Вычислить открытый (E) и закрытый (D) криптографические ключи (алгоритм RSA) при значениях $P = 13$ и $G = 17$.