**Министерство науки и высшего образования РФ**
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Национальный исследовательский университет «МЭИ»**

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: ЭТАЛОН: информационная безопасность**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

# Оценочные материалы
# по дисциплине
# Методы и средства криптографической защиты информации

**Москва**
**2022**

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:**

| | | |
|---|---|---|
| Преподаватель | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Евтеев Б.В.<br>Идентификатор: Rbb7ca24a-YevteevBV-e22a6fbb | Б.В. Евтеев |
| (должность) | (подпись) | (расшифровка подписи) |

**СОГЛАСОВАНО:**

| | | |
|---|---|---|
| Руководитель образовательной программы | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Баронов О.Р.<br>Идентификатор: R90d76356-BaronovOR-7bf8fd7e | О.Р. Баронов |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |
| Заведующий выпускающей кафедры | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |

## ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-9 способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

ИД-1 Настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Защита задания

1. Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание)
2. Защита реферата (Реферат)

Форма реализации: Письменная работа

1. Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа)
2. Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи» (Контрольная работа)

**БРС дисциплины**

5 семестр

| Раздел дисциплины | Веса контрольных мероприятий, % | | | | |
|---|---|---|---|---|---|
| | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
| | Срок КМ: | 4 | 8 | 12 | 15 |
| Основы криптографической защиты информации | | | | | |
| Место криптографической защиты информации в обеспечении информационной безопасности | | + | | | + |
| Тема 1. Основные понятия криптографической защиты информации | | + | | | + |
| Тема 2. Основы криптографических методов защиты информации | | + | | | + |
| Симметричные и асимметричные криптосистемы, средства их реализации | | | | | |
| Тема 3. Симметричные блочные шифры | | | + | | + |
| Тема 4. Поточные шифры | | | + | | + |

| | | | | |
|---|---|---|---|---|
| Тема 5. Концепция криптосистем с открытыми ключами и ее реализация на базе модулярной арифметики и эллиптических кривых | | + | | + |
| Тема 6. Нормативно-правовые акты криптографической защиты информации | | + | | + |
| Криптографические протоколы, хэш-функции, электронные подписи средства их реализации | | | | |
| Тема 7. Криптографические протоколы | | | + | + |
| Тема 8. Хэш-функции и электронные подписи | | | + | + |
| Вес КМ: | 25 | 25 | 25 | 25 |

$Общая часть/Для промежуточной аттестации$

**СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ**

***I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций***

| Индекс компетенции | Индикатор | Запланированные результаты обучения по дисциплине | Контрольная точка |
|---|---|---|---|
| ОПК-9 | ИД-1$_{ОПК-9}$ Настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации | Знать:<br>методы обеспечения конфиденциальности, целостности информации, подлинности сторон информационного взаимодействия, невозможности отказа от авторства, неотслеживаемости принципы построения современных криптосистем и криптопротоколов<br>Уметь:<br>применять методы обеспечения конфиденциальности, целостности, подтверждения подлинности, невозможности отказа от авторства, неотслеживаемости использовать принципы | Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание)<br>Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа)<br>Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи» (Контрольная работа)<br>Защита реферата (Реферат) |

| | | | |
|---|---|---|---|
| | | построения современных криптосистем и криптопротоколов формулировать и решать задачи построения защищенных профессионально-ориентированных автоматизированных систем с использованием криптографических методов | |

*II. Содержание оценочных средств. Шкала и критерии оценивания*

**КМ-1. Защита домашнего задания «Дешифрование классических шифров»**

**Формы реализации**: Защита задания
**Тип контрольного мероприятия:** Домашнее задание
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Защита домашнего задания «Дешифрование классических шифров». Необходимо найти ключ и расшифровать текст

**Краткое содержание задания:**
Найти ключ и расшифровать текст

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: принципы построения современных криптосистем и криптопротоколов | 1.Классические шифры, примеры. |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-2. Контрольная работа №1 «Симметричные и асимметричные криптосистемы»**

**Формы реализации**: Письменная работа
**Тип контрольного мероприятия:** Контрольная работа
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Контрольная работа по теме: «Симметричные и асимметричные криптосистемы». Необходимо решить задания и верно ответить на вопросы контрольной работы. Время выполнения 2 академических часа.

**Краткое содержание задания:**
Выполнить задания

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы обеспечения конфиденциальности, целостности информации, | 1.Примеры симметричных и асимметричных криптосистем.<br>2. После скольких раундов работы AES каждый байт |

| | |
|---|---|
| подлинности сторон информационного взаимодействия, невозможности отказа от авторства, неотслеживаемости | текущего состояния зависит от всех байт исходного состояния?<br>3.Ниже приведено описание шифра. Множества открытых текстов X, шифрованных текстов Y и ключей K заданы следующим образом: X = {x0, x1}, Y = {y0, y1, y2}, K = {k0, k1, k2}. Зашифрование открытого текста xi на ключе kj дает зашифрованный текст ym, где m=(i+j) mod 3. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать. |
| Уметь: формулировать и решать задачи построения защищенных профессионально-ориентированных автоматизированных систем с использованием криптографических методов | 1.При использовании шифра Эль-Гамаля с параметрами модуль P = 311, образующий множества ненулевых вычетов по модулю P α = 17, секретный ключ a = 19, случайно выбираемое число (рандомизатор) r = 41, найти зашифрованное сообщение Y, шифруемого сообщения X = 27.<br>2.Для двоичной последовательности 111110111 найти её линейную сложность и регистр сдвига слева направо, на котором она реализуется, с указанием начального заполнения этого регистра сдвига. |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-3. Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи»**

**Формы реализации**: Письменная работа
**Тип контрольного мероприятия:** Контрольная работа
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Контрольная работа по теме: «Криптографические протоколы, хэш-функции и электронные подписи». Необходимо решить задания и верно ответить на вопросы контрольной работы. Время выполнения 2 академических часа.

**Краткое содержание задания:**
Выполнить задания

**Контрольные вопросы/задания:**

| | |
|---|---|
| Уметь: использовать принципы | 1.Согласно протоколу Диффи - Хеллмана выработать |

| | |
|---|---|
| построения современных криптосистем и криптопротоколов | секретный ключ для связи абонентов A и B. Параметры: модуль P = 311, образующий множества ненулевых вычетов по модулю P α = 17.<br>2. Проверить электронную подпись сообщения, хэш-свертка которого равна 4, используя группу точек эллиптической кривой $Y^2=X^3+2X+6$ (mod 7). Генерирующая точка G= ( 3 , 5 ) порядка 11. Открытый ключ подписи(5,6), а сама подпись ( 1 , 2 ). |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-4. Защита реферата**

**Формы реализации**: Защита задания
**Тип контрольного мероприятия:** Реферат
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Выполнить реферат из перечня тем рефератов по курсу «Криптографические методы защиты информации» и защитить готовую работу

**Краткое содержание задания:**
Защита реферата

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы обеспечения конфиденциальности, целостности информации, подлинности сторон информационного взаимодействия, невозможности отказа от авторства, неотслеживаемости | 1.Электронная подпись. Отечественный стандарт электронной подписи |
| Знать: принципы построения современных криптосистем и криптопротоколов | 1.Блочные шифры. Стандарт шифрования данных AES |
| Уметь: использовать принципы построения современных криптосистем и криптопротоколов | 1.Стандарты шифрования данных AES и Гост 28147-89, их сравнительный анализ |
| Уметь: применять методы обеспечения конфиденциальности, | 1.Алгоритмы «облегченной» (lightweight) криптографии и их предназначение<br>2.Математические модели источников открытых |

| | |
|---|---|
| целостности, подтверждения подлинности, невозможности отказа от авторства, неотслеживаемости | сообщений и шифров<br>3.Гомоморфное шифрование информации и области его применения |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

## СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

**5 семестр**

**Форма промежуточной аттестации:** Экзамен

**Пример билета**

| НИУ «МЭИ» ИнЭИ | ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1 | Утверждаю: *Зав. кафедрой БИТ* |
|---|---|---|
| Кафедра *БИТ* | по дисциплине: *Криптографические методы защиты информации* | |
| 2021 год | направление подготовки: *10.03.01* форма обучения: *очная* | (подпись) |
| 1. Шифры и их формальные модели.<br>2. Классификация средств криптографической защиты информации<br>3. .Проверить электронную подпись сообщения, хэш-свертка которого равна 2, используя группу точек эллиптической кривой $Y^2=X^3+2X+6$ (mod 7). Генерирующая точка G= ( 3 , 5 ) порядка 11. Открытый ключ подписи ( 4 , 1 ), а сама подпись ( 2 , 2 ). | | |

**Процедура проведения**

Экзамен проводится в письменной форме по билетам согласно программе экзамена

***I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины***

**1. Компетенция/Индикатор:** ИД-1$_{ОПК-9}$ Настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации

**Вопросы, задания**

1.Симметричные, асимметричные и комбинированные криптосистемы
2.Модели и критерии распознавания открытых текстов
3.Понятие шифра, требования к шифрам, формальные модели шифров
4.Классификация шифров
5.Теоретическая и практическая стойкость шифров
6.Шифры замены. Примеры
7.Элементы криптоанализа шифров замены
8.Шифры перестановки. Примеры
9.Элементы криптоанализа шифров перестановки
10.Шифрование методом гаммирования и его криптоанализ
11.Криптоаналитические атаки и их классификация
12.Блочные системы шифрования, структура их построения
13.Режимы работы блочных шифров и их сравнение
14.Режим сцепления блоков шифра (CBC) на примере DES
15.Режим обратной связи по выходу (OFB) на примере DES
16.Режим сцепления блоков шифра (CBC) на примере DES
17.Элементы криптоанализа алгоритмов блочного шифрования
18.Стандарт шифрования данных DES
19.Современный американский стандарт шифрования данных AES
20.Российский стандарт шифрования данных МАГМА
21.Поточные системы шифрования. Принципы их построения
22.Синхронизация поточных систем шифрования, примеры
23.Шифр системы Гиффорда, A5 и RC4
24.Линейные рекуррентные последовательности и их характеристики
25.Методы генерации и анализа псевдослучайных последовательностей на базе ЛРС
26.Алгоритм Берлекемпа – Месси, пример

27.Варианты усложнения линейных рекуррентных последовательностей
28.Элементы криптоанализа поточных шифров
29.Системы шифрования с открытыми ключами. Криптосистема RSA
30.Системы шифрования с открытыми ключами. Криптосистема Эль Гамаля
31.Системы шифрования с открытыми ключами и атаки на них
32.Управление ключами. Открытое распределение ключей Диффи-Хеллмана
33.Электронная подпись. Алгоритмы RSA и Эль Гамаля
34.Российский стандарт электронной подписи
35.Американский стандарт электронной подписи
36.Хэш-функции, требования к ним и их типы
37.Отечественный стандарт хэш-функций
38.Американский стандарт хэш-функций
39.Криптографические протоколы и их классификация. Примеры
40.Российский стандарт шифрования данных КУЗНЕЧИК
41.Описание криптографических средств защиты информации в ОС Windows
42.Описание криптографических средств защиты информации в MSDN
43.Стандарты криптографической защиты информации
44.Классификация средств криптографической защиты информации
45.Основные принципы построения СКЗИ
46.Аппаратные, программные и аппаратно-программные СКЗИ
47.Криптографические средства создания защищенных виртуальных сетей
48.СКЗИ для передачи данных в локальных сетях
49.Сетевые протоколы криптографической защиты
50.Персональные криптографические средства аутентификации

**Материалы для проверки остаточных знаний**

1.Что такое шифр?

Ответы:

-

Верный ответ: Семейство обратимых отображений множества открытых текстов в множество шифрованных текстов, задаваемых функцией шифрования.

2.Какой шифр называется совершенным?

Ответы:

-

Верный ответ: Шифр при использовании которого шифрованный текст не дает противнику, не знающего секретного ключа, никакой информации об открытом тексте, т.е. условное распределение на множестве открытых текстов при заданном шифрованном тексте совпадает с безусловным распределением на множестве открытых текстов.

3.Какой размер сеансового ключа в DES?

Ответы:

-

Верный ответ: 56 бит

4.Какой размер раундовых ключей в DES?

Ответы:

-

Верный ответ: 48 бит.

5.Электронные подписи

Верный ответ: Электронная подпись – это закодированная информация о лице, как физическом, так и юридическом, которая необходима для его идентификации при подаче документов в электронном виде. Она позволяет защитить документ от

редактирования сторонними лицами, а также обеспечивает невозможность отказа от факта подписи.

6.В чем разница между криптографическими и стеганографическими методами защиты информации?

Ответы:

-

Верный ответ: Стеганографические методы направлены на сокрытие факта наличия определенной информации в передаваемом сообщении , а криптографические методы преобразуют (шифруют) информацию к виду не понятному третьим лицам.

7.Что такое криптографический протокол?

Ответы:

-

Верный ответ: Протокол, предназначенный для выполнения функций криптографической системы, в процессе выполнения которого участники используют криптографические алгоритмы.

8.В чем разница между блочными и поточными системами шифрования?

Ответы:

-

Верный ответ: В блочной системе шифрования открытый текст перед шифрованием разбивается на блоки, состоящие из нескольких знаков, т.е. исходное сообщение обрабатывается блоками, а в поточной каждый знак сообщения шифруется отдельно.

9.Что такое хэш-функция и и хэш-значение?

Ответы:

-

Верный ответ: Хэш-функция отображает входное слово конечной длины в конечном алфавите в слово, заданной, обычно фиксированной длины. Хэш-значение - значение хэш-функции для данного аргумента.

10.Что такое криптографические средства?

Ответы:

-

Верный ответ: В широком смысле это средства обеспечения информационной безопасности, использующие криптографические функции. В узком смысле это средства, реализованные в виде документов, механических, электромеханических, электронных технических устройств или программ, предназначенные для выполнения функций криптографической системы.

***II. Описание шкалы оценивания***

*Оценка:* 5

*Нижний порог выполнения задания в процентах:* 70

*Описание характеристики выполнения знания:* Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

*Оценка:* 4

*Нижний порог выполнения задания в процентах:* 60

*Описание характеристики выполнения знания:* Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 50

*Описание характеристики выполнения знания:* Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

### *III. Правила выставления итоговой оценки по курсу*

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетной / экзаменационной составляющих.