

**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: Организация и технология защиты информации**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Криптографические методы защиты информации**

**Москва  
2022**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Евтеев Б.В.
	Идентификатор	Rbb7ca24a-YevteevBV-e22a6fbb

(подпись)

Б.В. Евтеев

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(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. ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
2. ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
3. ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
4. ПСК-2 Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасного функционирования объектов энергетики с элементами АСУ ТП

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

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15

РАЗДЕЛ 1. Основы криптографической защиты информации.				
Введение	+			+
Тема 1. Основные понятия криптографической защиты информации	+			+
Тема 2. Основы криптографических методов защиты информации	+			+
РАЗДЕЛ 2. Симметричные и асимметричные шифрсистемы.				
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.		+	+	+
РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи				
Тема 6. Криптографические протоколы.			+	+
Тема 7. 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
ПК-1	ПК-1(Компетенция)	Знать: действующую классификацию средств криптографической защиты информации Уметь: пользоваться стандартными математическими методами при анализе криптографических алгоритмов	Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание) Защита реферата (Реферат)
ПК-4	ПК-4(Компетенция)	Знать: состояние нормативно-законодательной базы и стандарты в области криптографической защиты информации сущность системного подхода к защите информации Уметь: формулировать и решать задачи проектирования защищенных	Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание) Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа)

		<p>профессионально-ориентированных автоматизированных систем с использованием криптографических методов</p>	
ОК-5	ОК-5(Компетенция)	<p>Знать: классификацию, требования к шифрам и основные характеристики шифров Уметь: применять на практике положения законов РФ и ведомственных нормативных актов в области защиты информации</p>	<p>Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание) Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа)</p>
ПСК-2	ПСК-2(Компетенция)	<p>Знать: принципы построения современных криптосистем и криптопротоколов Уметь: применять криптографические методы защиты информации в различных предметных областях</p>	<p>Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа) Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи» (Контрольная работа) Защита реферата (Реферат)</p>

## 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: действующую классификацию средств криптографической защиты информации	1.Что собой представляют математические модели шифров перестановки и замены?
Знать: состояние нормативно-законодательной базы и стандарты в области криптографической защиты информации	1.Модели открытого текста
Знать: сущность системного подхода к защите информации	1.Классические шифры, примеры. 2.Методы криптоанализа классических шифров
Знать: классификацию, требования к шифрам и основные характеристики шифров	1.Критерии распознавания открытого текста

#### 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:**

Решить задания

**Контрольные вопросы/задания:**

Знать: принципы построения современных криптосистем и криптопротоколов	1.Ниже приведено описание шифра. Множества открытых текстов $X$ , шифрованных текстов $Y$ и ключей $K$ заданы следующим образом: $X = \{x_0, x_1\}$ , $Y = \{y_0, y_1, y_2\}$ , $K = \{k_0, k_1, k_2\}$ . Зашифрование открытого текста $x_i$ на ключе $k_j$ дает зашифрованный текст $u_m$ , где $m=(i+j) \bmod 3$ . Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.
Уметь: формулировать и решать задачи проектирования защищенных профессионально-ориентированных автоматизированных систем с использованием криптографических методов	1.При использовании шифра Эль-Гамала с параметрами модуль $P = 311$ , образующий множества ненулевых вычетов по модулю $P$ $\alpha = 17$ , секретный ключ $a = 19$ , случайно выбираемое число (рандомизатор) $r = 41$ , найти зашифрованное сообщение $Y$ , шифруемого сообщения $X = 27$ .
Уметь: применять на практике положения законов РФ и ведомственных нормативных актов в области защиты информации	1.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:**

Решить задания

**Контрольные вопросы/задания:**

Уметь: применять криптографические методы защиты информации в различных предметных областях	1. Согласно протоколу Диффи - Хеллмана выработать секретный ключ для связи абонентов А и В. Параметры: модуль $P = 311$ , образующий множества ненулевых вычетов по модулю $P$ $a = 17$ .
---	---

**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: действующую классификацию средств криптографической защиты информации	1. Шифры и их классификация
Знать: принципы построения современных криптосистем и криптопротоколов	1. Стандарты шифрования данных AES и Гост 28147-89, их сравнительный анализ 2. Блочные шифры. Стандарт шифрования данных AES
Уметь: пользоваться стандартными математическими	1. Атаки на секретные ключи асимметричных систем.

методами при анализе криптографических алгоритмов	
Уметь: применять криптографические методы защиты информации в различных предметных областях	1. 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

6 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ «МЭИ» ИнЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1	Утверждаю: Зав. кафедрой БИТ
Кафедра БИТ	по дисциплине: <i>Криптографические методы защиты информации</i> направление подготовки 10.03.01	(подпись)
20 год		
1. Шифры и их формальные модели. 2. Классификация средств криптографической защиты информации 3. Проверить электронную подпись сообщения, хэш-свертка которого равна 2, используя группу точек эллиптической кривой $Y^2=X^3+2X+6 \pmod{7}$ . 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

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

#### 1. Компетенция/Индикатор: ПК-1(Компетенция)

##### Вопросы, задания

- 1.Российский стандарт электронной подписи
- 2.Американский стандарт электронной подписи

##### 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.

#### 2. Компетенция/Индикатор: ПК-4(Компетенция)

##### Вопросы, задания

- 1.Стандарты криптографической защиты информации

##### Материалы для проверки остаточных знаний

- 1.Какой размер раундовых ключей в DES?

Ответы:

-

Верный ответ: 48 бит.

### **3. Компетенция/Индикатор: ОК-5(Компетенция)**

#### **Вопросы, задания**

- 1.Криптоаналитические атаки и их классификация

#### **Материалы для проверки остаточных знаний**

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

Ответы:

-

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

### **4. Компетенция/Индикатор: ПСК-2(Компетенция)**

#### **Вопросы, задания**

- 1.Современный американский стандарт шифрования данных AES
- 2.Алгоритмы «облегченной» (lightweight) криптографии и их предназначение

#### **Материалы для проверки остаточных знаний**

- 1.Что такое криптографический протокол?

Ответы:

-

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

- 2.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.

- 3.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.