

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

**Направление подготовки/специальность: 11.04.01 Радиотехника**

**Наименование образовательной программы: Радиотехнические системы**

**Уровень образования: высшее образование - магистратура**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Защита информации в радиоэлектронных системах**

**Москва  
2021**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Губонин Н.С.
	Идентификатор	Rd0607fd3-GuboninNS-9d6214d0

(подпись)

Н.С. Губонин

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Комаров А.А.
	Идентификатор	R8495daf1-KomarovAIA-eada3f0e

(подпись)

А.А.

Комаров

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Комаров А.А.
	Идентификатор	R8495daf1-KomarovAIA-eada3f0e

(подпись)

А.А.

Комаров

(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 Способен проводить исследования в целях совершенствования радиоэлектронных систем

ИД-3 Разрабатывает алгоритмы и проводит исследования в целях совершенствования функциональных узлов радиоэлектронных систем

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Письменная работа

1. Коллоквиум № 6 Российский стандарт шифрования, стандарты DES и AES (Коллоквиум)

2. Коллоквиум № 7 Система шифрования с открытым ключом RSA. Идентификация и аутентификация электронных данных (Коллоквиум)

3. Коллоквиум № 8 Сильная и слабая идентификация. Удалённые атаки в сети Internet. (Коллоквиум)

4. Коллоквиум №1. Основные понятия защиты информации (Коллоквиум)

5. Коллоквиум №2. Модулярные операции. Угрозы безопасности РЭС (Коллоквиум)

6. Коллоквиум №3. Криптографические функции со специальными свойствами. Опасные воздействия на РЭС (Коллоквиум)

7. Коллоквиум №4 Шифрование с использованием шифровальной таблицы. Реализация угроз безопасности РЭС (Коллоквиум)

8. Коллоквиум №5 Шифрование методом Хилла. Меры обеспечения безопасности компьютерных систем (Коллоквиум)

Форма реализации: Проверка задания

1. Комплексное расчётное задание (КРЗ) (Решение задач)

## БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %									
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8	КМ-9
	Срок КМ:	4	5	6	8	10	12	14	16	16
Принципы защиты информации в автоматизированных системах обработки информации										
Принципы защиты информации в автоматизированных системах обработки информации	+									+

Элементы дискретной математики (алгебра и теория чисел)									
Элементы дискретной математики (алгебра и теория чисел)		+							+
Симметричные системы шифрования									
Симметричные системы шифрования			+	+	+	+			+
Системы шифрования с открытым ключом (асимметричные системы шифрования). Защита данных в информационных сетях									
Системы шифрования с открытым ключом (асимметричные системы шифрования). Защита данных в информационных сетях							+	+	+
Вес КМ:	8	8	8	8	8	8	8	8	36

\$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	ИД-3ПК-1 Разрабатывает алгоритмы и проводит исследования в целях совершенствования функциональных узлов радиоэлектронных систем	Знать: математический аппарат, используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации основные угрозы безопасности РЭС и пути их предотвращения общие понятия и принципы защиты информации в информационных радиоэлектронных системах (РЭС)	Коллоквиум №1. Основные понятия защиты информации (Коллоквиум) Коллоквиум №2. Модулярные операции. Угрозы безопасности РЭС (Коллоквиум) Коллоквиум №3. Криптографические функции со специальными свойствами. Опасные воздействия на РЭС (Коллоквиум) Коллоквиум №4 Шифрование с использованием шифровальной таблицы. Реализация угроз безопасности РЭС (Коллоквиум) Коллоквиум №5 Шифрование методом Хилла. Меры обеспечения безопасности компьютерных систем (Коллоквиум) Коллоквиум № 6 Российский стандарт шифрования, стандарты DES и AES (Коллоквиум) Коллоквиум № 7 Система шифрования с открытым ключом RSA. Идентификация и аутентификация электронных данных (Коллоквиум) Коллоквиум № 8 Сильная и слабая идентификация. Удалённые атаки в сети Internet. (Коллоквиум) Комплексное расчётное задание (КРЗ) (Решение задач)

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

### КМ-1. Коллоквиум №1. Основные понятия защиты информации

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС:** 8

**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания

#### Краткое содержание задания:

1. Понятия: безопасность РЭС, угроза безопасности. Приведите пример угрозы безопасности РЭС
2. Понятия: уязвимость РЭС, атака на РЭС. Приведите примеры

#### Контрольные вопросы/задания:

Знать: общие понятия и принципы защиты информации в информационных радиоэлектронных системах (РЭС)	<ol style="list-style-type: none"><li>1. Понятие: “безопасность РЭС”</li><li>2. Понятие “угроза безопасности”. Приведите пример угрозы безопасности РЭС</li><li>3. Понятие: уязвимость РЭС. Приведите примеры</li><li>4. Понятие: атака на РЭС. Приведите примеры</li></ol>
--	---

#### Описание шкалы оценивания:

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий: (5, 5), (5, 4)

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий: (5, 3), (4, 4), (4,3)

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий: (3, 3)

### КМ-2. Коллоквиум №2. Модулярные операции. Угрозы безопасности РЭС

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС:** 8

**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания

#### Краткое содержание задания:

1. Найти  $7^{(-1)} \bmod 15$  и НОД (945, 378), используя алгоритм Евклида
2. Содержание угроз: «нарушение конфиденциальности информации», «нарушение конфиденциальности данных», «нарушение целостности данных». Приведите примеры

**Контрольные вопросы/задания:**

Знать: математический аппарат, используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации	1.Содержание угроз: «нарушение конфиденциальности информации». Приведите примеры 2.Содержание угрозы: «нарушение конфиденциальности данных». Приведите примеры 3.Содержание угрозы: «нарушение целостности данных». Приведите примеры 4.Поясните алгоритм расчета значения $7^{(-1)} \bmod 15$ , используя алгоритм Евклида 5.Поясните алгоритм расчета значения НОД (945, 378), используя алгоритм Евклида
--	---

**Описание шкалы оценивания:***Оценка: 5**Нижний порог выполнения задания в процентах: 90**Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 5), (5, 4)**Оценка: 4**Нижний порог выполнения задания в процентах: 70**Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 3), (4, 4), (4,3)**Оценка: 3**Нижний порог выполнения задания в процентах: 60**Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (3, 3)***КМ-3. Коллоквиум №3. Криптографические функции со специальными свойствами. Опасные воздействия на РЭС****Формы реализации:** Письменная работа**Тип контрольного мероприятия:** Коллоквиум**Вес контрольного мероприятия в БРС:** 8**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания**Краткое содержание задания:**

- 1.Понятие "хэш-функция". Какими дополнительными свойствами наделяют хэш-функцию при использовании в криптографии?
2. Перечислите основные опасные воздействия на РЭС

**Контрольные вопросы/задания:**

Знать: основные угрозы безопасности РЭС и пути их предотвращения	1.Перечислите основные опасные воздействия на РЭС 2.Понятие "хэш-функция" 3.Какими дополнительными свойствами наделяют хэш-функцию при использовании в криптографии?
--	--

**Описание шкалы оценивания:***Оценка: 5**Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий:  
(5, 5), (5, 4)

*Оценка:* 4

*Нижний порог выполнения задания в процентах:* 70

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий:  
(5, 3), (4, 4), (4,3)

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 60

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий:  
(3, 3)

#### **КМ-4. Коллоквиум №4 Шифрование с использованием шифровальной таблицы. Реализация угроз безопасности РЭС**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС:** 8

**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания

#### **Краткое содержание задания:**

1. Зашифруйте слово КРИПТОЗАЩИТА, используя в качестве ключа таблицу 3x4, перестановку строк по ключевому слову СОН и перестановку столбцов по ключевому слову ВОДА
2. Охарактеризуйте возможные действия злоумышленника (противника) для реализации угроз безопасности РЭС путём воздействия на аппаратные средства

#### **Контрольные вопросы/задания:**

Знать: основные угрозы безопасности РЭС и пути их предотвращения	1. Охарактеризуйте возможные действия злоумышленника (противника) для реализации угроз безопасности РЭС путём воздействия на аппаратные средства 2. Поясните алгоритм шифрования слова КРИПТОЗАЩИТА, если в качестве ключа используется таблица 3x4, а перестановка строк выполняется по ключевому слову СОН и перестановка столбцов выполняется по ключевому слову ВОДА
--	---

#### **Описание шкалы оценивания:**

*Оценка:* 5

*Нижний порог выполнения задания в процентах:* 90

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий:  
(5, 5), (5, 4)

*Оценка:* 4

*Нижний порог выполнения задания в процентах:* 70

*Описание характеристики выполнения знания:* Значения оценок рецензентом обоих заданий:  
(5, 3), (4, 4), (4,3)

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 60



Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий:  
(3, 3)

### **КМ-5. Коллоквиум №5 Шифрование методом Хилла. Меры обеспечения безопасности компьютерных систем**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС:** 8

**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания

#### **Краткое содержание задания:**

1. Можно ли зашифровать сообщение на русском языке, использующем алфавит из 33 прописных букв и символ пробела, методом Хилла, применяя линейное преобразование с заданной матрицей T?

$$T = \begin{pmatrix} 4 & 1 & 0 \\ 2 & 8 & 0 \\ 6 & 0 & 2 \end{pmatrix}$$

2. Перечислите основные административные и программно-аппаратные меры обеспечения безопасности компьютерных систем

#### **Контрольные вопросы/задания:**

Знать: основные угрозы безопасности РЭС и пути их предотвращения	1. Перечислите основные программно-аппаратные меры обеспечения безопасности компьютерных систем 2. Можно ли зашифровать сообщение на русском языке, использующем алфавит из 33 прописных букв и символ пробела, методом Хилла, применяя линейное преобразование с заданной матрицей T?
--	---

	$\mathbf{T} = \begin{pmatrix} 4 & 1 & 0 \\ 2 & 8 & 0 \\ 6 & 0 & 2 \end{pmatrix}$
--	--

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 5), (5, 4)*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 3), (4, 4), (4,3)*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (3, 3)*

**КМ-6. Коллоквиум № 6 Российский стандарт шифрования, стандарты DES и AES**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС:** 8

**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания

**Краткое содержание задания:**

1. Какими средствами обеспечивается проверка подлинности (аутентификация) в системах шифрования DES и ГОСТ 28147-89?
2. Дайте общую характеристику следующим принципам, используемым при проектировании систем защиты информации: экономическая эффективность, простота, неотключаемость защиты, открытость проектирования и функционирования «механизмов защиты»

**Контрольные вопросы/задания:**

Знать: основные угрозы безопасности РЭС и пути их предотвращения	<ol style="list-style-type: none"> <li>1. Дайте общую характеристику следующему принципу, используемому при проектировании систем защиты информации: “экономическая эффективность”</li> <li>2. Дайте общую характеристику следующему</li> </ol>
--	---

	принципу, используемому при проектировании систем защиты информации: “простота”
--	---

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 5), (5, 4)*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 3), (4, 4), (4,3)*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (3, 3)*

**КМ-7. Коллоквиум № 7 Система шифрования с открытым ключом RSA.**

**Идентификация и аутентификация электронных данных**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС: 8**

**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания

**Краткое содержание задания:**

1. Зашифруйте методом RSA с открытым ключом  $(n, ko) = (33, 7)$  слово НАДЕЖДА
2. Дайте общую характеристику системам идентификации и аутентификация электронных данных, использующим код аутентификации сообщений, имитовставку, электронную цифровую подпись

**Контрольные вопросы/задания:**

Знать: современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации	<ol style="list-style-type: none"> <li>1. Поясните, что лежит в основе метода шифрования RSA</li> <li>2. Что значит Открытый ключ?</li> <li>3. Поясните понятие имитовставка</li> <li>4. Поясните понятие электронная цифровая подпись</li> </ol>
---	---

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 5), (5, 4)*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 3), (4, 4), (4,3)*

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий:  
(3, 3)

### **КМ-8. Коллоквиум № 8 Сильная и слабая идентификация. Удалённые атаки в сети Internet.**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Коллоквиум

**Вес контрольного мероприятия в БРС: 8**

**Процедура проведения контрольного мероприятия:** Каждый студент получает письменный вариант индивидуального задания

#### **Краткое содержание задания:**

1. Сопоставьте методы сильной и слабой идентификации
2. Понятия «типовая удалённая атака» и «типовая угроза безопасности» в сети Internet.

#### **Контрольные вопросы/задания:**

Знать: современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации	1. Определите понятие “сильная идентификация” 2. Определите понятие “слабая идентификация” 3. Что означает понятие «типовая удалённая атака» в сети Internet? 4. Что означает понятие «типовая угроза безопасности» в сети Internet?
---	---

#### **Описание шкалы оценивания:**

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий:  
(5, 5), (5, 4)

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий:  
(5, 3), (4, 4), (4, 3)

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий:  
(3, 3)

### **КМ-9. Комплексное расчётное задание (КРЗ)**

**Формы реализации:** Проверка задания

**Тип контрольного мероприятия:** Решение задач

**Вес контрольного мероприятия в БРС: 36**

**Процедура проведения контрольного мероприятия:** Домашняя работа

#### **Краткое содержание задания:**

КРЗ предполагает выполнение двух заданий. (по вариантам)

Задание 1. Дайте письменный обоснованный ответ (объёмом 3-10 страниц машинописного текста) на вопрос "Какие основные методы организации защиты данных используются в современных радиоэлектронных системах передачи информации (по вариантам) и вызовы, которые приходится при этом преодолевать в связи с бурным развитием информационных технологий?"

Задание 2 Приведите обоснованное решение шести задач по изученным методам шифрования (по вариантам).

### Вариант 1

#### Задание 1

Дайте письменный обоснованный ответ (объёмом 3-10 страниц машинописного текста) на вопрос "Какие основные методы организации защиты данных используются в современных корпоративных радиосетях."

#### Задание 2

##### Задача 1.1

Зашифруйте слово КРИПТОЗАЩИТА, используя в качестве ключа таблицу 2'6, перестановку строк по ключевому слову ДА и перестановку столбцов по ключевому слову АЗИМУТ.

##### Задача 1.2

Зашифруйте слово ИНФОРМАЦИЯ методом аффинной подстановки с параметрами  $a=4$ ,  $k=2$  используя алфавит русских прописных букв (А, Б, ..., Я).

##### Задача 1.3

Зашифруйте слово ИНФОРМАЦИЯ методом подстановки по ключевому слову СОН в алфавите, состоящем из русских прописных букв

##### Задача 1.4

Можно ли при шифровании методом Хилла сообщения на русском языке в алфавите из 33 прописных букв и символа пробела применить линейное преобразование с матрицей

$$\mathbf{T} = \begin{pmatrix} 4 & 1 & 0 \\ 3 & 8 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Ответ поясните.

##### Задача 1.5

Зашифруйте методом RSA с открытым ключом в алфавите прописных русских букв слово НАДЕЖДА

##### Задача 1.6

Сколько в среднем придётся провести последовательных испытаний для определения ключа сообщения на русском языке (объём алфавита  $n=34$ ), зашифрованного в системе шифрования Цезаря?

### Контрольные вопросы/задания:

Знать: математический аппарат,

1.Какими свойствами должна обладать матрица

используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации	линейного преобразования при шифровании методом Хилла?
Знать: общие понятия и принципы защиты информации в информационных радиоэлектронных системах (РЭС)	1.Что такое “политика безопасности”, и какую роль она играет при организации <i>защиты данных</i> <i>используются в современных корпоративных радиосетях?</i> .
Знать: основные угрозы безопасности РЭС и пути их предотвращения	1.Сколько в среднем потребуется попыток при случайном отгадывании ключа шифрования, если известно общее возможное число ключей?
Знать: современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации	1.В чём состоит метод простой замены (подстановки) при шифровании данных? 2.Как используется метод простой подстановки при шифровании методом аффинной подстановки?

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 5), (5, 4)*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (5, 3), (4, 4), (4,3)*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Значения оценок рецензентом обоих заданий: (3, 3)*

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

## 1 семестр

**Форма промежуточной аттестации:** Зачет с оценкой

### Пример билета

Оценка за освоение дисциплины определяется как семестровая оценка в соответствии с «Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

### Процедура проведения

По результатам запланированных контрольных мероприятий выставляется набор оценок, из которых в соответствии с «Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» рассчитывается зачетная оценка

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

**1. Компетенция/Индикатор:** ИД-3ПК-1 Разрабатывает алгоритмы и проводит исследования в целях совершенствования функциональных узлов радиоэлектронных систем

### Вопросы, задания

1. Определите понятие “сильная идентификация”
2. Что означают принципы изоляция и разделение, используемые при проектировании систем защиты РЭС?
3. Поясните сущность (протокол шифрования и расшифрования) метода RSA
4. Поясните понятие имитовставка
5. Какими средствами обеспечивается проверка подлинности (аутентификация) в системах шифрования DES ?
6. Какими средствами обеспечивается проверка подлинности (аутентификация) в системах шифрования ГОСТ 28147-89?
7. Перечислите основные административные и программно-аппаратные меры обеспечения безопасности компьютерных систем
8. Охарактеризуйте возможные действия злоумышленника (противника) для реализации угроз безопасности РЭС путём воздействия на аппаратные средства
9. Зашифруйте слово КРИПТОЗАЩИТА, используя в качестве ключа таблицу 3x4, перестановку строк по ключевому слову СОН и перестановку столбцов по ключевому слову ВОДА
10. Понятие: уязвимость РЭС. Приведите примеры
11. Понятие: атака на РЭС. Приведите примеры
12. Какие алгоритмы, изученные в курсе, могут быть использованы в целях совершенствования функциональных узлов радиоэлектронных систем? Приведите пример и обоснование
13. Покажите, что Вы научились проведению исследования в целях совершенствования функциональных узлов радиоэлектронных систем

### Материалы для проверки остаточных знаний

1. 1. Основные понятия криптографической защиты информации - это:

Ответы:

- а) Шифрование

- б) Расшифрование
- в) Дешифрование
- г) Криптоанализ
- д) Политика безопасности

Верный ответ: а) б) д)

## 2.2. Угрозы информационной безопасности РЭС

Ответы:

- а) нарушение конфиденциальности информации
- б) нарушение конфиденциальности данных
- в) нарушение целостности данных
- г) нарушение синхронности данных

Верный ответ: а) б) в)

## 3.3. Опасные воздействия на РЭС

Ответы:

- а) климатические
- б) радиационные
- в) механические
- г) тепловые
- д) динамические
- е) космические

Верный ответ: а) б) в) г) д)

## 4.4. Для каких специальных целей используются хэш-функции в криптографии?

Ответы:

- а) построения систем контроля целостности данных при их передаче и хранении
- б) аутентификация источника данных
- в) локализация ошибок в полученных данных

Верный ответ: а) б)

## 5.5. Перечислите основные административные меры обеспечения безопасности компьютерных систем

Ответы:

*с открытым ответом - поле ввода*

Верный ответ: Административные (или организационные) меры обеспечения безопасности компьютерных систем – это меры организационного характера, регламентируют процессы взаимодействия, систем обработки данные, использование ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой, чтобы предотвратить возможность реализации угроз безопасности. Основные меры: грамотная проектировка при строительстве и при расстановке оборудования вычислительных центров и других объектов систем обработки данных; мероприятия по разработке правил доступа пользователей к ресурсам системы; мероприятия, осуществляемые при подборе и подготовке персонала системы; организация охраны и надежного пропускного режима; организация учета, хранения, использования и уничтожения документов и носителей с информацией; распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.); организация явного и скрытого контроля за работой пользователей; мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения

## 6.6. Перечислите основные программно-аппаратные меры обеспечения безопасности компьютерных систем

Ответы:

*с открытым ответом - поле ввода*

Верный ответ: Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ,



входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.). следующие способы защиты: •идентификацию и аутентификацию субъектов АСОИ; •разграничение доступа к ресурсам АСОИ; •контроль целостности данных; •обеспечение конфиденциальности данных; •аудит событий, происходящих в АСОИ; •резервирование ресурсов и компонентов АСОИ

## ***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 за освоение дисциплины определяется как семестровая оценка в соответствии с «Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»