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
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бровко Т.А. Идентификатор: R2d31a545-BrovkoTA-c057cc38	Т.А. Бровко

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Комаров А.А. Идентификатор: R8495daf1-KomarovAlA-eada3f0e	А.А. Комаров
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Комаров А.А. Идентификатор: R8495daf1-KomarovAlA-eada3f0e	А.А. Комаров

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: Смешанная форма

1. Асимметричные системы шифрования (Проверочная работа)
2. Линейные пространства над конечным кольцом (Проверочная работа)
3. Основные понятия защиты информации (Проверочная работа)
4. Симметричные системы шифрования (Проверочная работа)

БРС дисциплины

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Основные понятия защиты информации (Проверочная работа)
КМ-2 Линейные пространства над конечным кольцом (Проверочная работа)
КМ-3 Симметричные системы шифрования (Проверочная работа)
КМ-4 Асимметричные системы шифрования (Проверочная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
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:	25	25	25	25

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-З$_{ПК-1}$ 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 основные угрозы безопасности РЭС и пути их предотвращения современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации общие понятия и принципы защиты информации в информационных радиоэлектронных системах (РЭС) Уметь:	КМ-1 Основные понятия защиты информации (Проверочная работа) КМ-2 Линейные пространства над конечным кольцом (Проверочная работа) КМ-3 Симметричные системы шифрования (Проверочная работа) КМ-4 Асимметричные системы шифрования (Проверочная работа)

		проводить сопоставительный анализ и рациональный выбор по совокупности показателей качества из существующих и перспективных методов и систем шифрования и расшифрования данных	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Основные понятия защиты информации

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
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:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: общие понятия и принципы защиты информации в информационных радиоэлектронных системах (РЭС)	1.Понятие: “безопасность РЭС” 2.Понятие “угроза безопасности”.
Знать: современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации	1.Понятие: уязвимость РЭС. 2.Понятие: атака на РЭС.

Описание шкалы оценивания:

Оценка: 5 («отлично»)
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 («хорошо»)
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 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. Линейные пространства над конечным кольцом

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Проверочная работа

Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Каждый студент получает письменный вариант индивидуального задания.

Краткое содержание задания:
1.Определения, свойства и примеры линейных пространств над конечным кольцом
2. Кольца Галуа

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: математический аппарат, используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации	1.Определение линейных пространств над конечным кольцом 2.Примеры линейных пространств над конечным кольцом

Описание шкалы оценивания:

Оценка: 5 («отлично»)
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 («хорошо»)
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 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. Симметричные системы шифрования

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
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. Зашифруйте сообщение на русском языке, использующем алфавит из 33 прописных букв и символ пробела, методом Хилла, применяя линейное преобразование с заданной матрицей T?

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

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: проводить сопоставительный анализ и рациональный выбор по совокупности показателей качества из существующих и перспективных методов и систем шифрования и расшифрования данных	1.Зашифруйте слово КРИПТОЗАЩИТА, используя в качестве ключа таблицу 4x3, а перестановка строк выполняется по ключевому слову ВОДА и перестановка столбцов выполняется по ключевому слову СОН 2.Зашифруйте слово 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 («отлично»)
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 («хорошо»)
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 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Асимметричные системы шифрования

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Каждый студент получает письменный вариант индивидуального задания.

Краткое содержание задания:

1.Зашифруйте методом RSA с открытым ключом (*n*, *k*o) = (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:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: основные угрозы безопасности РЭС и пути их предотвращения	1.Что значит Открытый ключ? 2.Поясните понятие имитовставка 3.Поясните понятие электронная цифровая подпись

Описание шкалы оценивания:

Оценка: 5 («отлично»)
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 («хорошо»)
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 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

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

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

1. Компетенция/Индикатор: ИД-З$_{ПК-1}$ Разрабатывает алгоритмы и проводит исследования в целях совершенствования функциональных узлов радиоэлектронных систем

Вопросы, задания

1.Определите понятие “сильная идентификация”
2.Поясните сущность (протокол шифрования и расшифрования) метода RSA
3.Какими средствами обеспечивается проверка подлинности (аутентификация) в системах шифрования ГОСТ 28147-89?
4.Охарактеризуйте возможные действия злоумышленника (противника) для реализации угроз безопасности РЭС путём воздействия на аппаратные средства
5.Зашифруйте слово КРИПТОЗАЩИТА, используя в качестве ключа таблицу 3х4, перестановку строк по ключевому слову СОН и перестановку столбцов по ключевому слову ВОДА

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

7.7. Для аутентификации пользователя в системе используется

Ответы:

а) login (имя пользователя в системе)
б) пароль

Верный ответ: б)

8.8. "Система рукопожатия" используется при

Ответы:

а) при идентификации пользователя системой

б) при идентификации системы пользователем
в) при взаимной идентификации (включая аутентификацию) системы и пользователя
Верный ответ: в)
9.9. Является ли DoS типовой угрозой в сети Internet?
Ответы:
а) Нет
б) Да
Верный ответ: б)
10.10. VPN (Virtual Private Network) используется для
Ответы:
а) логической структуризации IP-сети
б) локализации трафика ЭВМ сети по защищённым каналам
Верный ответ: б)

II. Описание шкалы оценивания

Оценка: 5 («отлично»)
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 («хорошо»)
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 («удовлетворительно»)
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

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

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».