

**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: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

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

**Москва
2024**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

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

Б.В. Евтеев

СОГЛАСОВАНО:

Руководитель
образовательной
программы

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

О.Р.
Баронов

Заведующий
выпускающей кафедрой

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

А.Ю.
Невский

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-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем

ИД-2 Применяет программные средства обеспечения безопасности данных

2. 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-4.3	ИД-2 _{ОПК-4.3} Применяет программные средства обеспечения безопасности данных	Знать: принципы работы программно-аппаратных криптографических средств защиты информации требования, предъявляемые к функционированию этих средств Уметь: выполнять работы по обеспечению штатного функционирования криптографических средств защиты информации	Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание) Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа) Защита реферата (Реферат)
ОПК-9	ИД-1 _{ОПК-9} Настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации	Знать: методы обеспечения конфиденциальности, целостности информации, подлинности сторон информационного взаимодействия, невозможности отказа от	Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание) Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа) Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи» (Контрольная работа) Защита реферата (Реферат)

		авторства, неотслеживаемости принципы построения современных криптосистем и криптопротоколов Уметь: применять методы обеспечения конфиденциальности, целостности, подтверждения подлинности, невозможности отказа от авторства, неотслеживаемости использовать принципы 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 : требования, предъявляемые к функционированию этих средств	1.Методы криптоанализа классических шифров
Уметь: выполнять работы по обеспечению штатного функционирования криптографических средств	1.Дешифровать шифр Виженера: ОПХБОЫХСЯСЫМГАТСОЫ_ТТЕЭЪС_ШЯ_О_ЮМЦШ_ЩНКЫЛВХЬЛЯП_Э НЮФМТХЭЗНЮСЫРШЩМДВЮМЛАРЛЯПЩЦАЫСЪ_ЦЧЧЕЧЯЪМПЪЛБ_ ЩЗЮФЪМПФСРЖЛИАГЪРШИССЪЪА_ЯЧЬЮЦМХПЯМЗТТЩНКЖЛТРЪ ЛПЮСЮЕЪСЩОТМШ_ЬТЮЕ_ЪМЛРЮЛИЧСЦОБ_ЬЫДСЮОУЦМ_ФЧЧАЫЪ ЛИЭВЮРВЮСНЪМЛИП_ЬУЦЪС_БДЮ_ТВС_Я_ЩЯБЯЪ_Э_ЛВЮГЛЯПИФТР ПЛП_ЬОЖЧЭТТТЛУЖЧЩЫДСЪ_Б_Ш_ЖГЪ_АБЪРЮСПОАДРА_ВЮВРСН УФДЮ_С_ЬОБНЭАПЩМ_Ъ_ЩТ_ЧЬПЯМДПЪЩФЮБШАЕЪСЙПТЛНХСЩ АФСЫРШБЪДЭМШИПБССВБЭАЪЛЗТДВИБСОЕАНШАПЪЩТ_ЬПУНКС_Э _ЛЧБ_ЛПЮЦЪАЧДШЕТТСТАРЛПЮЦЛИЭЕЪРЪТБИХЫЛУБФСРЦЦСНШЧЛ ОПЪМПИЮОПУЯДВКСЕПЩМ_ШЯ_О_ЮМЦШЧХ_ЭТЫОБЯФЛЮСШНХС УНРЮСНШГЯЮПВБЕЭДЛИЧС_ИЫНШАПФЖПВВЦНШЬЛВКЙСДЗЧПОПЯ М_МЬАЭМЛВПГЖСОИМ_ФЧОЯБНЭОБСГЕАГЗДХВКТПВСДЛЮЪМПХЪД ВСЩЕЪЪХ_СЪУНХВШЕЭСЮРЮХМЕБСУАПАЯГЮФФЦВСНЕЭЦТАЬЧЩА ПФЖПВВЦНШЪМ_Ъ_ЧЛХЦТАПЧПОПЪПРРЭЛДРВЮИЭСАОГЮМНПЪЛП_ _ФЗЭ_ЭИБСОСХХЪ_ЮЩЦОПВЧОТ_ЛПЫТЭТЪТЭСКСЮАЪСЪНПЯМПВГЭ ТТДСТПЮЪЛЮЦЪГЮСВЕЫ_ОЕЪТЛВПЯМЧРЭС_ХХЪ_ЬТЬХБЖ_ШЯЮЕ_ ЧЭНЮСССЫЪЛБКСИТВСЭЦХЯЯ_ЭТЫИАТЧИПЯССЪ_ЧЪЪ_ЛДХВКТШЭСТ ШЫЛСЯДЭТОСЩЕПВЦАЧТЧ_СМЛТЮГЛЫШЩЦЕАЮСНПЪЩАЖЧЛИЭЕЪ РЪТБИОСЫРХЦЭТРФЧЯНСЦАЪЪС_РУЭУ_ЦЩЫХСЪАЧХЪВЮБЖ_Ь_ПЛШС НЬПФССБЪЭЫПФЛДХЭЪВЮЮЛМШБС_АЪЛЛЬЪ_ВСОААСФНГ_БМРЗФИ

защиты информации	ПЙОЕЦЗМРШРЛВХЭФКРРЛСББМНРСЯ_ЭЪА_АГЪЛЛЬЪ_ШЯ_О_ЮМЦШЪ ЛЯПВЧЫЗТЧ_ШЯРЕЪВЛСБ_ФМЮВЮИПЪЩФЮБШАЕЪФ_Я_ГЕЫСОВХБА РУЭУ_ЦЩЫП_ЩИПАЪТЮЮЯ_ЖГЪ_ШЯ_О_ЮМЦШРЛХЮГК_ШСФГ_ТС ТПФЭЕПУЪЛХЧЛЗЭТВИЪДЙ_ЧЪПФЛНРЙСЙПШФЗЭЪЛНХСКВЫРСТАРЛ ЧХЮЮОП_ЭЯЧТСМКЮЛИПЯС_Я_РДРЧЮСОСЮОЖЯЪМВСФЗЪЧЪЕЭЪЙ_ ЪТЦ_ЪТЮЕ_ЪМЛКСЧИЕТЛП_ЧТНШЖЛЭЯ_А_ШЯ_О_ЮМЦШ_ЩНРРЛРХФ ЪЛНЗФЯПГЪЛЛЬЪ_ЭТВИЭТСТАРЛС_ЧРСБФМ_АФКЗШСЩЕШЩНЕЦЯЪ_Я РЕЗЧОЕНГЛТРЪЛЖХСЪЕЧЪЪ_ЪТЦ_ТСЭВЮЧЛВ_ЧШЯПФЖЧШВЧИБЧЪЭ ТК_БЧАНШЪМ_Ъ_ПДРСФХПВЮОШЮЪСБНЛДЮВЮАБ_ВНЮСЭНШЩФТ АРЛИПВЪЕЧ_ЩИ_ДСТПВЛД_ДПИЪЪЛДЮВЮИЦЧЩИОЮФ_БЧАНЮЭЫГШ ЪЛРХГФВКЧЛАФЮФНШВЮРРГЪРКСФ_ЭЧЪВЭМС_Я_ЧИБЪЦИПАСРХВЮ АЭДЮ_ВАЪМШЯМТЛСОЫ_ТТЕЭЪС_ШЯ_О_ЮМЦШ_ЩНРРЛМРХФСБМ ЛЛСЫРЮВЮОПАЪТЮЮЯ_ЖГЪ_ЮЯЪ_Ъ_РНЮСФ_ЯБССБЪТНЮСШАУЪЭ Т_ТЧЫПВЮАЭЧЮ_ЧМЛЛЯЪСБНЙ_ШСЦАЪСИЛХЪЮРШИССБЪЪ_ТМУОТ ЧЮ_ФТЧЕЪ_ЛИФДДИХСЫОАЭСДАГОИОСВТЮУЖ_Я_ЩЯБНЛПЮИСМВС ФНГ_ЪМРЗФЯПВЮАЭ_ОИБВК_ШСБЕЭГЪ_ТВСГЮСФ_ТВК_ТТНЮСЫОЭР ЮБЪМКПГСХЭ_ЧОУЪК_ШЩЩЕЭРСТПВЫОА_НЫПЧС_ЮУЪАС_ЮКШС ЪБПОЮОЪСПЛРФЩЫЪСЪЪ_ТУОЪСФ_Я_ХДХГЛРХИЗ_ТСРАЭЯЪЙПХЧАТЧ ЛСЫТНОПАЪДУ_ЮОТЭСНЭМС_ЖЪЮАБЧЧИПЯС_ЧЯМЮИЪС_ЯБФНЕЪЫ ОТСЪАС_ЮБПФЖЧШВЧИБЧЪЭ_Х_БЧАНШЪФ_ШСФСБ_ЫИШССЕПБМЗТ ЪЮИОСЫОБДВАБСЩЕЮУАОФЪШЫЩСШИЭЪШУЪСЭВХЦСНШЫЛЧБ_Н ЫПАЪОФ_ЧЖШГЗ_ЖГСНШЧЛКЭЪПИПТЛЕАЭФ_ТМЛЗЭТСТХСЦАЪСЪАС_ ЮАНГЛЩШЕЪОТМС_Ъ_ШПЛПНОЕ_МЛМЮШСТХСЭПЮЪЙЭ_ЛП_ЧИАГ МТЛСЦЕАЪЛЛЬЪ_АГЪАЭЪБ_ШСЫЕ_ЧХТШСЭРРЦЯ_ЪСЮРХГЗЕЩСПЛР ФС
Уметь: формулировать и решать задачи построения защитных профессионально-ориентированных автоматизированных	1.Дешифровать шифр простой замены: 58 62 32 39 99 31 29 58 72 62 99 58 13 54 15 56 31 63 39 72 84 15 13 56 77 15 82 56 56 56 58 54 29 77 56 – 39 99 56 31 56 77 32 12 15 54 31 48 76 63 15 52 13 39 72 39 54 16 72 39 32 72 62 58 58 15, 37 62 77 52 39 13 39 72 39 32 39 31 62 54 39 77 84 39 21 31 39 16 72 62 99 58 13 15 54 56 13 46 16 39 58 13 95 16 15 13 62 12 46 31 39 62 72 15 77 54 56 13 56 62 84 31 39 32 56 76 58 63 62 72 33 62 12 39 54 62 33 62 58 52 39 91 99 62 29 13 62 12 46 31 39 58 13 56. 56 31 63 39 72 84 15 82 56 39 31 31 48 62 13 62 76 31 39 12 39 32 56 56 16 72 39 33 31 39 54 39 53 12 56 54 37 56 77 31 62 58, 39 37 72 15 77 39 54 15 31 56 62, 16 72 39 56 77 54 39 99 58 13 54 39, 39 13 52 72 48 54 33 62 12 39 54 62 52 95 31 62 37 48 54 15 12 48 62 54 39 77 84 39 21 31 39 58 13 56 16 39 58 52 39 72 39 58 13 56 16 39 12 95 33 62 31 56 29 56 39 37 72 15 37 39 13 52 62 56 31 63 39 72 84 15 82 56 56, 15 13 15 52 21 62 16 39 15 54 13 39 84 15 13 56 77 15 82 56 56 16 72 39 56 77 54 39 99 58 13 54 62 31 31 48 76, 95 16 72 15 54 12 62 31 33 62 58 52 56 76 56 56 31 48 76 16 72 39 82 62 58 58 39 54

сис те м с испол ьзова нием крипт ограф ическ их мето дов	
---	--

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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не 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: принципы работы программно-аппаратных криптографических средств защиты информации	1.Примеры симметричных и асимметричных криптосистем. 2. После скольких раундов работы AES каждый байт текущего состояния зависит от всех байт исходного состояния? 3.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 y_m , где $m = (i+j) \bmod 3$. Ключи для зашифрования выбираются равновероятно. Является ли данный шифр совершенным? Ответ обосновать.
Уметь: применять методы обеспечения конфиденциальности, целостности, подтверждения подлинности, невозможности отказа от авторства, неотслеживаемости	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 $X = 27$. 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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не 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:

Знать: методы обеспечения конфиденциальности, целостности информации,	1. Криптографические хэш-функции
---	----------------------------------

подлинности информационного взаимодействия, невозможности отказа от авторства, неотслеживаемости	
Знать: принципы построения современных криптосистем и криптопротоколов	1.Протоколы распределения ключей.
Уметь: использовать принципы построения современных криптосистем и криптопротоколов	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 $\alpha = 17$.

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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не 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: принципы работы программно-аппаратных криптографических средств защиты информации	1.Исторический аспект криптографических методов защиты информации
Знать: требования, предъявляемые к функционированию этих средств	1.Криптография и информационная безопасность
Знать: принципы построения	1.Блочные шифры. Стандарт шифрования данных

современных криптосистем и криптопротоколов	AES 2.Электронная подпись. Отечественный стандарт электронной подписи
Уметь: использовать принципы построения современных криптосистем и криптопротоколов	1.Алгоритмы «облегченной» (lightweight) криптографии и их предназначение 2.Математические модели источников открытых сообщений и шифров 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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не 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: <i>Криптографические методы защиты информации</i> направление подготовки: <i>10.03.01</i> форма обучения: <i>очная</i>	(подпись)
2021 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

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

1. Компетенция/Индикатор: ИД-2_{ОПК-4.3} Применяет программные средства обеспечения безопасности данных

Вопросы, задания

1. Симметричные, асимметричные и комбинированные криптосистемы
2. Методы генерации и анализа псевдослучайных последовательностей на базе ЛРС
3. Алгоритм Берлекемпа – Мессии, пример
4. Варианты усложнения линейных рекуррентных последовательностей
5. Системы шифрования с открытыми ключами. Криптосистема RSA
6. Системы шифрования с открытыми ключами. Криптосистема Эль Гамала
7. Системы шифрования с открытыми ключами и атаки на них
8. Управление ключами. Открытое распределение ключей Диффи-Хеллмана
9. Электронная подпись. Алгоритмы RSA и Эль Гамала
10. Российский стандарт электронной подписи
11. Американский стандарт электронной подписи
12. Хэш-функции, требования к ним и их типы
13. Отечественный стандарт хэш-функций
14. Российский стандарт шифрования данных КУЗНЕЧИК
15. Классификация средств криптографической защиты информации
16. Основные принципы построения СКЗИ
17. Аппаратные, программные и аппаратно-программные СКЗИ
18. Криптографические средства создания защищенных виртуальных сетей
19. СКЗИ для передачи данных в локальных сетях

Материалы для проверки остаточных знаний

1. 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.Какой размер сеансового ключа в DES?

Ответы:

-

Верный ответ: 56 бит

3.Какой размер раундовых ключей в DES?

Ответы:

-

Верный ответ: 48 бит.

4.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.

5.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.

2. Компетенция/Индикатор: ИД-1ОПК-9 Настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации

Вопросы, задания

- 1.Модели и критерии распознавания открытых текстов
- 2.Понятие шифра, требования к шифрам, формальные модели шифров
- 3.Классификация шифров
- 4.Теоретическая и практическая стойкость шифров
- 5.Шифры замены. Примеры
- 6.Элементы криптоанализа шифров замены
- 7.Шифры перестановки. Примеры
- 8.Элементы криптоанализа шифров перестановки
- 9.Шифрование методом гаммирования и его криптоанализ
- 10.Криптоаналитические атаки и их классификация
- 11.Блочные системы шифрования, структура их построения
- 12.Режимы работы блочных шифров и их сравнение
- 13.Режим сцепления блоков шифра (CBC) на примере DES
- 14.Режим обратной связи по выходу (OFB) на примере DES
- 15.Режим сцепления блоков шифра (CBC) на примере DES
- 16.Элементы криптоанализа алгоритмов блочного шифрования
- 17.Стандарт шифрования данных DES
- 18.Современный американский стандарт шифрования данных AES
- 19.Российский стандарт шифрования данных МАГМА
- 20.Поточные системы шифрования. Принципы их построения
- 21.Линейные рекуррентные последовательности и их характеристики
- 22.Сетевые протоколы криптографической защиты
- 23.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. 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.

3. Что такое криптографический протокол?

Ответы:

-

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

4. Что такое хэш-функция 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.

5. 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

Оценка: 2

Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

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.