

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

Направление подготовки/специальность: 09.03.01 Информатика и вычислительная техника

Наименование образовательной программы: Вычислительные машины, комплексы, системы и сети

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Защита информации**

**Москва
2022**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Рытов А.А.
	Идентификатор	R37263e31-RytovAA-c7235577

(подпись)

А.А. Рытов

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной
программы

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Гольцов А.Г.
	Идентификатор	R64210572-GoltsovAG-cebbd3e8

(подпись)

А.Г. Гольцов

(расшифровка
подписи)

Заведующий
выпускающей кафедры

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Вишняков С.В.
	Идентификатор	R35b26072-VishniakovSV-02810d9

(подпись)

С.В.

Вишняков

(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-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИД-2 Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью

2. ПК-1 Способен обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности

ИД-3 Производит оценку влияния применяемых технических решений на общее функционирование системы

3. ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании

ИД-1 Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии

ИД-2 Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа

ИД-4 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%) (Лабораторная работа)

2. Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа)

3. Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа)

4. Контрольно-зачетное занятие (К331) по курсу ЗИ Модуль 1 (65%) (Тестирование)

5. Контрольно-зачетное занятие (К332) по курсу ЗИ Модуль 2 (65%) (Тестирование)

6. Контрольно-зачетное занятие (К333) по курсу ЗИ Модуль 3 (65%) (Тестирование)

Форма реализации: Смешанная форма

1. Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью)

2. Контроль посещения лекций №1-5 по курсу ЗИ Модуль 1 (15%) (Интервью)

3. Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью)

БРС дисциплины

8 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:	5	5	5	9	9	9	14	14	14
Традиционные симметричные криптосистемы										
Традиционные симметричные криптосистемы	+	+	+							
Проектирование и анализ потоковых шифров										
Проектирование и анализ потоковых шифров					+	+	+			
Современные симметричные криптосистемы										
Современные симметричные криптосистемы					+	+	+			
Асимметричные криптосистемы										
Асимметричные криптосистемы								+	+	+
Управление криптографическими ключами										
Управление криптографическими ключами								+	+	+
Алгоритмы шифрования на основе SP-сети										
Алгоритмы шифрования на основе SP-сети								+	+	+
Вес КМ:	5	7	21	5	7	21	5	7	22	

\$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-3	ИД-2 _{ОПК-3} Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью	Знать: угрозы безопасности при работе в сети Интернет Уметь: устанавливать и применять средства защиты информации при её хранении и передаче по сети	Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью) Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа) Контрольно-зачетное занятие (К333) по курсу ЗИ Модуль 3 (65%) (Тестирование)
ПК-1	ИД-3 _{ПК-1} Производит оценку влияния применяемых технических решений на общее функционирование системы	Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения Уметь: осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности	Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью) Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа) Контрольно-зачетное занятие (К332) по курсу ЗИ Модуль 2 (65%) (Тестирование)
ПК-2	ИД-1 _{ПК-2} Демонстрирует знание нормативной базы, методов описания, анализа	Знать: принципы построения современных	Контроль посещения лекций №1-5 по курсу ЗИ Модуль 1 (15%) (Интервью) Контроль выполнения комплекса лабораторных работ №1-4 по курсу

	и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии	криптографических систем Уметь: использовать современные информационные технологии при решении задач защиты информации	ЗИ Модуль 1 (20%) (Лабораторная работа) Контрольно-зачетное занятие (К331) по курсу ЗИ Модуль 1 (65%) (Тестирование)
ПК-2	ИД-2ПК-2 Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	Знать: основные алгоритмы и стандарты криптографической защиты информации Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью) Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа) Контрольно-зачетное занятие (К333) по курсу ЗИ Модуль 3 (65%) (Тестирование)
ПК-2	ИД-4ПК-2 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации Уметь: использовать современные инструментальные средства и технологии программирования	Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью) Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа) Контрольно-зачетное занятие (К333) по курсу ЗИ Модуль 3 (65%) (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контроль посещения лекций №1-5 по курсу ЗИ Модуль 1 (15%)

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 5

Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись.

Зарегистрироваться в Webex и присутствовать на лекции.

Пример выполнения (не выполнения) задания:

	А-04-17	Лекции 15					5	
		№1	№2	№3	№4	№5		
1	Васильев Игорь Сергеевич (В)			1			1	3
2	Горбонос Игорь Игоревич	1	1	1	1	1	5	15
3	Гулько Антон Артемович	1	1	1	1	1	5	15
4	Дергунов Александр Алексеевич (В)	1		1	1		3	9
5	Ким Дмитрий Александрович	1	1	1	1	1	5	15
6	Липатова Надежда Дмитриевна (В)			1			1	3
7	Михтиев Иван Олегович	1	1	1			3	9
8	Поддубный Федор Сергеевич	1	1	1	1	1	5	15
9	Сурьев Денис Александрович	1	1	1	1	1	5	15

Контрольные вопросы/задания:

Знать: принципы построения современных криптографических систем	<ol style="list-style-type: none"> 1. принципы криптографической защиты информации 2. основные этапы в развитии криптографии 3. основные задачи криптографии 4. определение шифра перестановки 5. определение шифра простой замены 6. определение шифра сложной замены 7. определение шифра гаммирования
Уметь: использовать современные информационные технологии при решении задач защиты информации	<ol style="list-style-type: none"> 1. определить ключевое пространство простейшего шифра 2. рассчитать энтропию открытого и зашифрованного текста

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 5 лекций модуля 1 равно 15. Оценка 5 находится в диапазоне 14 -15 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 5 лекций модуля 1 равно 15. Оценка 4 находится в диапазоне 11 -13 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 5 лекций модуля 1 равно 15. Оценка 3 находится в диапазоне 6 -12 баллов.

КМ-2. Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 7

Процедура проведения контрольного мероприятия: При очной форме обучения лабораторные работы выполняются в компьютерном классе, в котором доступна сетевая версия Wolfram Mathematica 9. Одна лабораторная работа длится 2 академических часа. Отчет формируется в бумажном варианте. При дистанционной форме обучения лабораторные работы выполняются в Wolfram Cloud | Open Access system. Контроль и консультации в течение лабораторной работы в системе Webex. Рабочее задание и необходимые методические материалы размещаются в системе Moodle. Отчет по выполненной лабораторной работе загружается в систему Moodle, где производится контроль выполнения и выставляется суммарное число баллов по правильно выполненным пунктам рабочего задания.

Краткое содержание задания:

Пример рабочего задания лабораторной работы №1

Лабораторная работа №1

Исследование частотных свойств шифра простой замены

В работе используется программа “ALFAVIT”, позволяющая провести частотный анализ открытого и зашифрованного текста в рамках русского алфавита. Текст необходимо набирать в “Блокноте”, либо ввести из заранее подготовленного файла.

Опция «Посчитать» производит анализ текста, определяет количество букв и строит диаграмму распределения числа букв по алфавиту.

Опция «Зашифровать» производит преобразование исходного текста по алгоритму одноалфавитного шифра простой замены (система шифрования Цезаря) с ключом $K = 3,15$ (опция «Сдвиг»).

Опция «Н» предназначена для подсчета информационной энтропии как открытого, так и зашифрованного текста.

Рабочее задание.

1. Набрать текст (или ввести в “ALFAVIT” из файла) в “Блокноте” (порядка 100 букв), исключить пробелы, знаки препинания и заменить заглавные буквы на строчные.
2. Провести анализ текста (опции «Посчитать» и «Н»), выделить и зафиксировать наиболее информативные признаки (3-4 наибольших значения и их положение относительно друг друга) полученного распределения.
3. Для значения $KE = (N+3) \bmod 11 + 2$, где N – номер по списку в группе, зашифровать текст и вновь провести анализ. Сравнить полученные результаты.
4. Построить вариационный ряд (упорядочить буквы по убыванию вероятности), сравнить с распределением частот русского языка :

Частоты букв p_i в русском языке

Пробел	0,175	р	0,040	я	0,018	х	0,009
о	0,090	в	0,038	ы	0,016	ж	0,007
е, ё	0,072	л	0,035	з	0,016	ю	0,006
а	0,062	к	0,028	ь, ъ	0,014	ш	0,006
и	0,062	м	0,026	б	0,014	щ	0,003
т	0,053	д	0,025	г	0,013	щ	0,003
н	0,053	п	0,023	ч	0,012	э	0,003
с	0,045	у	0,021	й	0,010	ф	0,002

5. Расшифровать предлагаемый текст CN (N- номер по списку группы), используя наиболее вероятное распределение частот появления букв в тексте на русском языке (пробел в программе ALFAVIT исключен из анализа).
6. Используя результаты п.5, определить ключ расшифрования KD.
7. Открыть пакет "Математика" и прочитать (ReadList) первые 10 букв из файла п.1.
8. С помощью функции FromCharacterCode перевести коды ASCII в символы.
9. Создать строку, содержащую первые пять символов русского алфавита и с помощью функции ToCharacterCode определить коды представления русского алфавита.
10. Перевести символы вектора п.7 из кодов ASCII в UNICOD и вновь вывести с помощью FromCharacterCode (см. Character Codes в системе документации Wolfram Mathematica).
11. Используя пример (шаблон) для латинского алфавита сформировать программу, реализующую шифр Цезаря для русского алфавита с вводом данных из файла. С помощью функции ToCharacterCode и FromCharacterCode пакета "Математика", преобразующих символы в ASCII коды и обратно (код буквы а-97, код буквы в-98 и т.д.), можно задать шифр Цезаря с помощью следующей функции:

```
CaesarCipher[plaintext_, key_] :=
FromCharacterCode[ Mod[ ToCharacterCode[plaintext] - 97 +key, 26] + 97]
```

Пример использования:

```
CaesarCipher[plaintext_, key_] := FromCharacterCode[ Mod[ ToCharacterCode[plaintext] - 97
+key, 26] + 97]
```

```
plaintext="typehereyourplaintextinsmallletters";
```

```
key=24;
```

```
CaesarCipher[plaintext,key]
```

```
rwncfscrcwmspnjyglrcvrglqkyjjjсгсrq
```

12. Реализовать расшифровку заданного в п.5 файла CN методом силовой атаки (использовать первые 40 символов текста).

Пример для латинского алфавита : ciphertext="yhaklwpmw";

```
Table[CaesarCipher[ciphertext,-key],{key,1,26}].
```

13. Разработать программный модуль шифрования текста системой афинных подстановок.

14. Разработать программный модуль шифрования текста системой Цезаря с ключевым словом.

15. Построить три совмещенные по вертикали диаграммы распределения символов текста из п1:

- исходный открытый текст;
- текст, зашифрованный с помощью основного алгоритма Цезаря на ключе $KE = (N+3) \bmod 11+2$;
- текст, зашифрованный на произвольном ключе с помощью системой афинных подстановок;
- текст, зашифрованный на произвольном ключе с помощью системы Цезаря с ключевым словом..

Веса (баллы за правильное выполнение) пунктов рабочего задания приведены в следующей таблице:

Лабораторная работа №1 Шифры простой замены	
Пункт рабочего задания	Вес
1	2
2	1
3	1
4	1
5	5
6	2
7	2
8	1
9	1
10	1
11	3
12	2
13	3
14	3
15	2
	30

По каждой лабораторной работе выставляется соответствующее рабочему заданию число баллов.

Максимальное число баллов за выполнение цикла лабораторных работ модуля 1 равно 124.

НеделяЛабораторная работа Баллы
 1Lab 1 Шифры простой замены 30
 2Lab 2 Криптосистема Хилла 35
 3Lab 3 Шифры перестановки 30
 4Lab 4 Система шифрования Вижинера 29

Контрольные вопросы/задания:

Знать: принципы построения современных криптографических систем	1.Определение шифра сложной замены 2.Афинная система подстановок 3.Принципы построения криптосистемы Хилла 4.Система шифрования Вижинера 5.Принцип построения системы шифрования Вернама
Уметь: использовать современные информационные технологии при решении задач защиты информации	1.Разработать модуль расшифрования по базовой таблице шифра Вижинера 2.Разработать модуль подготовки данных для шифрования Вернама

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 124. Оценка 5 находится в диапазоне 112 -124 балла.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 124. Оценка 5 находится в диапазоне 87 -112 балла.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 124. Оценка 3 находится в диапазоне 50 - 87 баллов.

КМ-3. Контрольно-зачетное занятие (КЗ31) по курсу ЗИ Модуль 1 (65%)

Формы реализации: Компьютерное задание

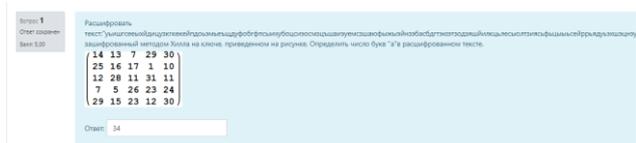
Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 21

Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащённом сетевой версией Mathematica. Длительность контрольной 2 академических часа. К занятию допускаются студенты, выполнившие цикл лабораторных работ модуля 1 и представившие отчеты по лабораторным работам. При дистанционной форме обучения контроль за участниками ведется в Webex, тестирование проводится в системе Moodle. К тестированию допускаются студенты, загрузившие в Moodle электронные отчеты и получившие по ним положительную оценку. Загрузка отчетов должна быть завершена за 24 часа до начала контрольной.

Краткое содержание задания:

Пример теста КЗ31 криптосистема Хилла. :



Контрольные вопросы/задания:

<p>Знать: принципы построения современных криптографических систем</p>	<p>1.КЗ31 ключевое слово. Число баллов за правильно выполненное задание = 5. Число вариантов задания 104. 2.КЗ31 криптосистема Хилла. Число баллов за правильно выполненное задание = 5. Число вариантов задания 50.</p>
<p>Уметь: использовать современные информационные технологии при решении задач защиты информации</p>	<p>1.КЗ31 простая перестановка. Число баллов за правильно выполненное задание = 3. Число вариантов задания 70. 2.КЗ31 система шифрования Вижинера. Число баллов за правильно выполненное задание = 7. Число вариантов задания 50. 3.КЗ31 столбцовая перестановка. Число баллов за</p>

правильно выполненное задание = 7. Число вариантов задания 50.

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 7 заданий равно 37. Оценка 5 находится в диапазоне 34 - 37 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 7 заданий равно 37. Оценка 4 находится в диапазоне 26 - 33 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 7 заданий равно 37. Оценка 3 находится в диапазоне 15 - 26 баллов.

КМ-4. Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%)

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 5

Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись.

Зарегистрироваться в Webex и присутствовать на лекции.

Пример выполнения (не выполнения) задания:

	А-12-17	Лекции 15					4
		№6	№7	№8	№9		
1	Восканьянц Нина Кирилловна	1	1	1	1	4	15
2	Гиль Иван Викторович	1	1	1	1	4	15
3	Ендерюков Роман Андреевич	1	1	1	1	4	15
4	Зиновкин Александр Юрьевич	1	1	1	1	4	15
5	Клочков Алексей Сергеевич (В)					0	0
6	Лазарев Вадим Игоревич	1	1	1	1	4	15
7	Макаров Евгений Сергеевич	1	1	1	1	4	15
8	Муканова Александра Ренатовна	1	1	1	1	4	15
9	Неганова Валентина Сергеевна	1	1	1	1	4	15
10	Палагина Софья Алексеевна	1	1	1	1	4	15
11	Подхолозина Мария Андреевна	1	1			2	7,5
12	Самсонов Михаил Евгеньевич	1	1	1	1	4	15
13	Сидорова Анастасия Вячеславовна	1	1	1	1	4	15
14	Сухоруков Матвей Дмитриевич	1	1	1	1	4	15
15	Торчков Михаил Васильевич	1				1	3,8
16	Успенская Екатерина Олеговна	1	1	1	1	4	15
17	Французов Илья Сергеевич	1	1	1	1	4	15

Контрольные вопросы/задания:

Знать: этапы проведения эксперимента по проверке корректности принимаемого	1.методы программной реализации генераторов псевдослучайных последовательностей 2.методы аппаратной реализации генераторов
--	---

проектного решения	псевдослучайных последовательностей 3. отечественные и зарубежные стандарты алгоритмов блочного шиф-рования; 4. режимы использования блочных шифров;
Уметь: осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности	1. выбрать системные параметры линейного конгруэнтного генератора

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 4 лекций модуля 1 равно 15. Оценка 5 находится в диапазоне 14 -15 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 4 лекций модуля 1 равно 15. Оценка 4 находится в диапазоне 11 -13 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 4 лекций модуля 1 равно 15. Оценка 3 находится в диапазоне 6 -12 баллов.

КМ-5. Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 7

Процедура проведения контрольного мероприятия: При очной форме обучения лабораторные работы выполняются в компьютерном классе, в котором доступна сетевая версия Wolfram Mathematica 9. Одна лабораторная работа длится 2 академических часа. Отчет формируется в бумажном варианте. При дистанционной форме обучения лабораторные работы выполняются в Wolfram Cloud | Open Access system. Контроль и консультации в течение лабораторной работы в системе Webex. Рабочее задание и необходимые методические материалы размещаются в системе Moodle. Отчет по выполненной лабораторной работе загружается в систему Moodle, где производится контроль выполнения и выставляется суммарное число баллов по правильно выполненным пунктам рабочего задания.

Краткое содержание задания:

Пример рабочего задания лабораторной работы №5:

Лабораторная работа № 5

Система шифрования Вернама по курсу «Защита информации»

Рабочее задание.

1. Сформировать таблицу кодирования букв русского алфавита двоичным пятиразрядным кодом. Выравнивание осуществлять с помощью команды PadLeft[].
2. Преобразовать строку открытого текста plainText="прилетаюдвадцатьтретьегомарта" в двоичный список. Определить длину полученного списка.
3. Установить начальное состояние генератора случайных чисел равным номеру по списку в группе и получить ключ в виде двоичного списка, с помощью команды RandomInteger[]. Длина ключевой последовательности должна быть равна длине двоичного списка открытого текста.
4. Зашифровать plainText (путем сложения по mod2 двоичных последовательностей), а затем расшифровать на ключе, сформированном в п. 3.
5. Разработать модуль шифрования по методу Вернама – входные параметры: строка текста и строка ключевой последовательности; выход: строка шифртекста.
6. Разработать модуль дешифрования по методу Вернама – входные параметры: строка шифртекста и строка ключевой последовательности; выход: строка расшифрованного текста.
7. Подготовить программный модуль, реализующий генератор BBS с параметрами, приведенными в work task \ tableBBS_W.xls, N – номер по списку в группе. Получить ключевую последовательность длиной m.
8. Зашифровать, а затем расшифровать Plaintext \Text-N.txt на ключе п. 7.
9. Получить ключевую последовательность от генератора BBS длиной 50m (см. п.7).
10. Провести анализ качества ключевой последовательности с помощью частотного теста в подпоследовательностях (Frequency Test Within a Block): articles\ Методы оценки качества ПСП\стр. 165.

Максимальное число баллов за выполнение цикла лабораторных работ модуля 2 равно 91.

Неделя Лабораторная работа Баллы

6 Lab 5 Система шифрования Вернама 27

7 Lab 6 РСЛОС 32

8 Lab 7 Поточковый шифр 32

Контрольные вопросы/задания:

<p>Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения</p>	<p>1.число допустимых состояний РСЛОС 2.требования к исходному многочлену для построения РСЛОС с максимальным периодом 3.алгоритм формирования S-блока потокового шифра - аналога RC4</p>
<p>Уметь: осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности</p>	<p>1.провести частотный анализ двоичной последовательности на выходе РСЛОС 2.разработать программный модуль генератора Геффе 3.разработать и протестировать модуль шифрования RC4 4.разработать и протестировать модуль расшифрования RC4</p>

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 91. Оценка 5 находится в диапазоне 82 - 91 балл.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 91. Оценка 4 находится в диапазоне 64 - 81 балл.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 91. Оценка 3 находится в диапазоне 37 - 63 балл.

КМ-6. Контрольно-зачетное занятие (К332) по курсу ЗИ Модуль 2 (65%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 21

Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенный сетевой версией Mathematica. Длительность контрольной 2 академических часа. К занятию допускаются студенты, выполнившие цикл лабораторных работ модуля 1 и представившие отчеты по лабораторным работам. При дистанционной форме обучения контроль за участниками ведется в Webex, тестирование проводится в системе Moodle. К тестированию допускаются студенты, загрузившие в Moodle электронные отчеты и получившие по ним положительную оценку. Загрузка отчетов должна быть завершена за 24 часа до начала контрольной.

Краткое содержание задания:

Пример одного из заданий К332:

Вопрос: 1
Ответ сохранен
Балл: 1,00

По заданной двоичной последовательности 0000000010011101100001110 определить коэффициенты обратной связи РСЛОС. Вводить коэффициенты, начиная со старших разрядов.

Ответ: 1111101

Контрольные вопросы/задания:

Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения	1.К332 РСЛОС последовательность. Число баллов за правильно выполненное задание = 3. Число вариантов задания 500.
Уметь: осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности	1.К332 РСЛОС состояние. Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 36. Оценка 5 находится в диапазоне 33- 36 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 36. Оценка 4 находится в диапазоне 25 - 33 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 36. Оценка 3 находится в диапазоне 14 - 24 баллов.

КМ-7. Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%)

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 5

Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись.

Зарегистрироваться в Webex и присутствовать на лекции.

Пример выполнения (не выполнения) задания:

№ п/п	Фамилия И.О.	Лекция 10						Модуль 3 ЗИ						Весенний семестр 2020/2021 уч.г.					
		№10	№11	№12	№13	№14	№15	№10	№11	№12	№13	№14	№15	№16	№17	№18	№19	№20	
1	Андреев Олег Казбекович	1	1	1	2	6	15	16,0	17,0	33,0	36,0								
2	Артем Владислав Владимирович (В)																		
3	Белова Ирина Михайловна	1	1	1	2	6	15	16,0	17,0	33,0	36,0								
4	Борисов Александр Александрович (Б)																		
5	Бурцева Анна Александровна	1	1	1	2	5	12,5	16,0	17,0	33,0	36,0								
6	Иванов Георг Александрович	1	1	1	2	6	15	16,0	17,0	33,0	36,0								
7	Ушаева Анастасия Устиновна	1	1	1	2	6	15	16,0	17,0	33,0	36,0								
8	Колесникова Юлия Юрьевна (К)																		
9	Курбанова Екатерина Сергеевна	1	1	1	2	4	10	16,0	17,0	33,0	36,0								
10	Лавренко Михаил Евгеньевич	1	1	1	2	5	12,5	16,0	17,0	33,0	36,0								
11	Маринова Вера Владимировна	1	1	1	2	6	15	16,0	17,0	33,0	36,0								
12	Новосел Александр Юрьевич	1	1	1	2	6	15	8,0	8,0	16,0	36,0								
13	Пайсова Александра Сергеевна	1	1	1	2	5	12,5	16,0	17,0	33,0	36,0								
14	Садков Игорь Тимурович	1	1	1	2	4	10	16,0	17,0	33,0	36,0								
15	Соловьева Олеся Валентиновна	1	1	1	2	4	10	16,0	17,0	33,0	36,0								
16	Траншова Мария Сергеевна	1	1	1	2	6	15	16,0	17,0	33,0	36,0								
17	Фадеев Василий Сергеевич	1	1	1	2	6	15	16,0	17,0	33,0	36,0								
18	Фетисова Анна Максимовна	1	1	1	2	6	15	16,0	17,0	33,0	36,0								

Контрольные вопросы/задания:

Знать: угрозы безопасности при работе в сети Интернет	1. Принципы построения криптосистемы RSA 2. Хэш функции 3. Электронно-цифровая подпись RSA 4. Комбинированный метод шифрования
Знать: основные алгоритмы и стандарты криптографической защиты информации	1. Протоколы с нулевым разглашением
Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации	1. Обобщенная схема асимметричной криптосистемы
Уметь: устанавливать и применять средства защиты информации при её хранении и	1. применить встроенные хэш - функции системы Mathematica 2. проверить документ с ЭЦП RSA

Описание шкалы оценивания:*Оценка: 5**Нижний порог выполнения задания в процентах: 90**Описание характеристики выполнения знания:* Максимальное число набранных баллов при посещении всех 6 лекций модуля 3 равно 15. Оценка 5 находится в диапазоне 14 -15 баллов.*Оценка: 4**Нижний порог выполнения задания в процентах: 70**Описание характеристики выполнения знания:* Максимальное число набранных баллов при посещении всех 6 лекций модуля 3 равно 15. Оценка 4 находится в диапазоне 11 -13 баллов.*Оценка: 3**Нижний порог выполнения задания в процентах: 40**Описание характеристики выполнения знания:* Максимальное число набранных баллов при посещении всех 6 лекций модуля 3 равно 15. Оценка 3 находится в диапазоне 6 -12 баллов.**КМ-8. Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ
Модуль 3 (20%)****Формы реализации:** Компьютерное задание**Тип контрольного мероприятия:** Лабораторная работа**Вес контрольного мероприятия в БРС:** 7**Процедура проведения контрольного мероприятия:** При очной форме обучения лабораторные работы выполняются в компьютерном классе, в котором доступна сетевая версия Wolfram Mathematica 9. Одна лабораторная работа длится 2 академических часа. Отчет формируется в бумажном варианте. При дистанционной форме обучения лабораторные работы выполняются в Wolfram Cloud | Open Access system. Контроль и консультации в течение лабораторной работы в системе Webex. Рабочее задание и необходимые методические материалы размещаются в системе Moodle. Отчет по выполненной лабораторной работе загружается в систему Moodle, где производится контроль выполнения и выставляется суммарное число баллов по правильно выполненным пунктам рабочего задания.**Краткое содержание задания:**

Пример рабочего задания лабораторной работы №8:

Лабораторная работа № 8

Основы работы с системой «Криптон»

Рабочее задание.

1. Установить пакет программ из папки ArcMail в следующей последовательности: Api , E-Crypton, ArcMailW , Crypto, Key.
2. Открыть "Руководство пользователя"(CrEncrypt\userguid.doc – Руководство пользователя) и ознакомиться с назначением (1.1 Назначение и условия применения, 1.2 Основные термины), принципами шифрования (1.3.1 Архивное шифрование файлов.), управлением ключевой информацией (2.3.1 Генерация Узла Замены, 2.3.2 Генерация Главного Ключа ,2.3.3 Генерация Ключа Пользователя) и обработкой файлов в интерактивном режиме (2.4).

3. Создать текстовый файл размером 2-4 килобайта в своей папке и создать отдельную папку для хранения зашифрованных текстов.
4. Провести операции шифрования на пароле, на "Главном" ключе, на "Главном" ключе+пароль, используя следующие опции: не уничтожать исходные файлы, копировать дату и атрибуты, не использовать сложные имена, размещать зашифрованные файлы в соответствующем каталоге (для отражения данных опций нажать кнопку "Больше").
5. С помощью программы WinHex определить число совпадающих символов в зашифрованных файлах.
6. Используя программу "Мастер ключей шифрования"(KeyMaster.exe) создать "Ключ Пользователя"; с помощью программы WinHex построить гистограмму распределения символов в ключе, а затем зашифровать исходный файл.
7. Провести расшифрование полученных ранее четырех файлов шифртекста.
8. Определить начальную позицию размещения исходного файла – WinHex\Инструменты\Открыть диск. Провести уничтожение исходного файла, используя опцию Криптон-Шифрование-Уничтожить. Проверить наличие информации на позиции (смещении) исходного файла.
9. Создать “ключевую дискету” на имеющемся сменном носителе, содержащую новый узел замены, главный ключ, ключ пользователя.
10. Провести операции шифрования и расшифрования произвольного текстового файла для ключей, расположенных на сменном носителе.
11. Удалить сменный носитель и попробовать расшифровать зашифрованный файл.

Максимальное число баллов за выполнение цикла лабораторных работ модуля 3 равно 82.

НеделяЛабораторная работа Баллы

- | | | |
|----|--|----|
| 10 | Lab 8 Основы работы с системой «Криптон» | 16 |
| 11 | Lab 9 Криптосистема RSA | 17 |
| 12 | Lab 10 ЭЦП RSA | 33 |
| 13 | Lab 11 Схемы разделения секрета | 16 |

Контрольные вопросы/задания:

Знать: угрозы безопасности при работе в сети Интернет	1.Активный перехват 2.Ренегатство 3.Подмена 4.Повтор
Знать: основные алгоритмы и стандарты криптографической защиты информации	1.Системы с несколькими открытыми ключами
Знать: способы и технологии	1.Атака “человек посередине” (Man in the middle)

применения криптографии в решении задач идентификации и аутентификации	
Уметь: использовать современные инструментальные средства и технологии программирования	1.Инсталлировать систему CRYPTON на виртуальной машине 2.Создать ключ пользователя

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 3 равно 82. Оценка 5 находится в диапазоне 74 - 82 балла.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 3 равно 82. Оценка 4 находится в диапазоне 58 - 73 балла.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 3 равно 82. Оценка 3 находится в диапазоне 33 - 57 балла.

КМ-9. Контрольно-зачетное занятие (К333) по курсу ЗИ Модуль 3 (65%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 22

Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенный сетевой версией Mathematica. Длительность контрольной 2 академических часа. К занятию допускаются студенты, выполнившие цикл лабораторных работ модуля 1 и представившие отчеты по лабораторным работам. При дистанционной форме обучения контроль за участниками ведется в Webex, тестирование проводится в системе Moodle. К тестированию допускаются студенты, загрузившие в Moodle электронные отчеты и получившие по ним положительную оценку. Загрузка отчетов должна быть завершена за 24 часа до начала контрольной.

Краткое содержание задания:

Пример одного из заданий К333:

Вопрос 1 Ответ сохранен Балл: 5,00	Сумма контракта подписана двумя участниками сделки: 1052573293. Модуль для ЭЦП равен 1445152223. Значение хэш - функции ("CRC32") общего третьего ключа равно 398476976. Файл со значениями ключей находится в папке: К33 модуль 3/ОpenKey/keys.dat. Определить сумму контракта.
	Ответ: <input type="text" value="658754"/>

Контрольные вопросы/задания:

Знать: угрозы безопасности при	1.К333 ЭЦП RSA.Число баллов за правильно
--------------------------------	--

работе в сети Интернет	выполненное задание = 7. Число вариантов задания 500.
Знать: основные алгоритмы и стандарты криптографической защиты информации	1.К333 OpenKey. Число баллов за правильно выполненное задание = 5. Число вариантов задания 500. 2.К333 Схемы разделения секрета. Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.
Уметь: устанавливать и применять средства защиты информации при её хранении и передаче по сети	1.К333 RSA+Цезарь. Число баллов за правильно выполненное задание = 3. Число вариантов задания 48.
Уметь: устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.К333 КОД 16 -- Криптон. Число баллов за правильно выполненное задание = 5. Число вариантов задания 48.
Уметь: использовать современные инструментальные средства и технологии программирования	1.К333 Умножение байтов AES. Число баллов за правильно выполненное задание = 7. Число вариантов задания 250.

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 34. Оценка 5 находится в диапазоне 31- 34 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 34. Оценка 4 находится в диапазоне 24- 31 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 34. Оценка 3 находится в диапазоне 14- 31 баллов.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

МЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №6 Защита информации ИВТИ	Утверждаю Зав.кафедрой ВМСС																																		
Теоретические вопросы к экзамену по курсу ЗИ																																				
1. Алгоритм открытого распределения ключей Диффи-Хеллмана.																																				
2. Система омофонов.																																				
Задание №2 Задания уровня 3																																				
Текст анщъдщцъзъдмнщзъмнкъд зашифрован с помощью системы Цезаря. Провести расшифрование и ввести ответ в виде трехзначного десятичного числа в поле ввода.																																				
Задание №3 Задания уровня 5																																				
Регистр сдвига с линейными обратными связями имеет характеристический многочлен $1+x^{17}+x^{20}$. Начальное состояние РСЛОС составляет СВСDB h. На 20-ом такте работы состояние РСЛОС в десятичной форме соответствует паролю, на котором в системе 'КРИПТОН' зашифрован ключ пользователя. Ключ пользователя и сообщение находятся в локальной сети : KZI\Test\Crypt-Test-1\Test 1- 6. Расшифруйте и введите текст сообщения в поле ввода.																																				
Задание №4 Задания уровня 7																																				
Расшифровать текст с номером 6 из папки CrypttextPRM, зашифрованный на ключе из таблицы, приведенной на рисунке. В поле ввода ввести строку из 10 символов, которые расположены начиная с 20 позиции в расшифрованном тексте.																																				
<table border="1"><thead><tr><th>Традиционные оценки в РФ</th><th>Оценки в 100-балльной шкале</th><th>Оценки в расширенной 5-балльной шкале</th><th>Оценки ECTS</th></tr></thead><tbody><tr><td>5</td><td>90 – 100</td><td>5</td><td>A</td></tr><tr><td rowspan="2">4</td><td>81 – 89</td><td>4+</td><td>B</td></tr><tr><td>70 – 80</td><td>4</td><td>C</td></tr><tr><td rowspan="2">3</td><td>66 – 69</td><td>3</td><td>D</td></tr><tr><td>60 – 65</td><td>3-</td><td>E</td></tr><tr><td rowspan="2">2</td><td>31 – 59</td><td>2+</td><td>FX</td></tr><tr><td>0 – 30</td><td>2</td><td>F</td></tr><tr><td>Зачет</td><td>60 – 100</td><td>Зачет</td><td>Passed</td></tr></tbody></table>	Традиционные оценки в РФ	Оценки в 100-балльной шкале	Оценки в расширенной 5-балльной шкале	Оценки ECTS	5	90 – 100	5	A	4	81 – 89	4+	B	70 – 80	4	C	3	66 – 69	3	D	60 – 65	3-	E	2	31 – 59	2+	FX	0 – 30	2	F	Зачет	60 – 100	Зачет	Passed			
Традиционные оценки в РФ	Оценки в 100-балльной шкале	Оценки в расширенной 5-балльной шкале	Оценки ECTS																																	
5	90 – 100	5	A																																	
4	81 – 89	4+	B																																	
	70 – 80	4	C																																	
3	66 – 69	3	D																																	
	60 – 65	3-	E																																	
2	31 – 59	2+	FX																																	
	0 – 30	2	F																																	
Зачет	60 – 100	Зачет	Passed																																	
Примечание. ECTS – European Credit Transfer and Accumulation System																																				

Процедура проведения

При очной форме обучения экзамен проводится в комбинированной форме по билетам. Два теоретических вопроса выполняются письменно и оцениваются в диапазоне 0 - 10 баллов преподавателем. Три практических задания выполняются в рамках системы Moodle : максимальная оценка 15 баллов. Результирующая оценка за экзамен определяется как сумма баллов, набранных по теории и практике и пересчитывается к пятибалльной системе (Традиционные оценки РФ) по представленной во вкладке "билет" шкале. В дистанционном режиме экзамен проводится в системе Moodle и Webex (идентификация и контроль, в том числе визуальный) и состоит из двух тестов (вопросы или задания выполняются строго последовательно): Первый тест содержит 20 вопросов по теоретической части курса.

Общая продолжительность теста 15 минут. Максимальное число баллов по теоретической части - 40. Второй тест содержит 6 практических заданий (2 задания уровня 3, 2 задания уровня 5, 2 задания уровня 7), аналогичных заданиям КЗЗ. Среднее время на выполнение задания 10 минут. Общая продолжительность теста 60 минут. Максимальное число баллов второго теста - 60. Результирующая оценка за экзамен определяется как сумма баллов, набранных в первом и втором тестах и пересчитывается к пятибалльной системе (Традиционные оценки РФ) по представленной во вкладке "билет" шкале.

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

1. Компетенция/Индикатор: ИД-2_{ОПК-3} Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью

Вопросы, задания

1. Принципы криптографической защиты информации.
2. Основные типы криптоаналитических атак.
3. Тест-задание: ЭЦП RSA
4. Электронно-цифровая подпись DSA .
5. Электронная цифровая подпись на основе схемы Эль - Гамала

Материалы для проверки остаточных знаний

1. Проверка подписи в асимметричных криптосистемах предполагает использование
Ответы:

открытого ключа получателя личного ключа получателя открытого ключа отправителя личного ключа отправителя

Верный ответ: открытого ключа отправителя

2. Какое равенство применяется при проверке электронно-цифровой подписи по схеме Эль-Гамала

Ответы:

$(y^a \cdot x^b) \bmod p = (g^M) \bmod p$ $(a^y \cdot a^b) \bmod p = (g^M) \bmod p$ $(y^a \cdot a^b) \bmod p = (g^M) \bmod p$
 $p (y^a \cdot a^b) \bmod p = (M^g) \bmod p$

Верный ответ: $(y^a \cdot a^b) \bmod p = (g^M) \bmod p$

3. Какая из атак может быть эффективна против классической реализации алгоритма Диффи-Хеллмана

Ответы:

атака "грубой силы" атака "человек посередине" маскард ренегатство повтор

Верный ответ: атака "человек посередине"

2. Компетенция/Индикатор: ИД-3_{ПК-1} Производит оценку влияния применяемых технических решений на общее функционирование системы

Вопросы, задания

1. Регистры сдвига с линейной обратной связью.
2. Тест-задание: РСЛОС состояние
3. Методы генерации псевдослучайных последовательностей чисел.
4. Методы оценки качества псевдослучайных последовательностей.
5. Оценка результатов тестирования статистических свойств генератора ПСП.
6. Анализ прохождения статистических тестов.
7. Анализ статистической безопасности криптоалгоритмов.

Материалы для проверки остаточных знаний

1.Какая логическая функция применяется в цепи обратной связи РСЛОС

Ответы:

"И" "ИЛИ" "НЕ" "Исключающее ИЛИ" "xtime"

Верный ответ: "Исключающее ИЛИ"

2.Длина двоичной последовательности, достаточная для определения коэффициентов обратной связи n-разрядного РСЛОС.

Ответы:

n $2n$ n^2 $10n$ n^3

Верный ответ: $2n$

3.Каким должен быть многочлен для РСЛОС с выходной последовательностью максимальной длины

Ответы:

составным разреженным примитивным с четной старшей степенью с нечетной старшей степенью

Верный ответ: примитивным

4.Чему равен максимальный период последовательности n - разрядного РСЛОС

Ответы:

n $2n-1$ 2^n $2^n - 1$ $2^{(n-1)}$

Верный ответ: $2^n - 1$

3. Компетенция/Индикатор: ИД-1_{ПК-2} Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии

Вопросы, задания

- 1.Асимметричные криптосистемы.
- 2.Основные параметры алгоритма ГОСТ Р 34.12-2015 «Кузнечик».
- 3.Полнораундовый алгоритм шифрования ГОСТ Р 34.12-2015 «Кузнечик».
4. Обобщенная схема симметричной, асимметричной криптосистемы.
5. Шифрование методом гаммирования.
- 6.Современные симметричные криптосистемы.
- 7.Режим "Электронная кодовая книга".
8. Режим "Сцепление блоков шифра".
9. Режим "Обратная связь по шифру".
- 10.Режим "Обратная связь по выходу".

Материалы для проверки остаточных знаний

1.Алгоритм шифрования ... не имеет слабых ключей

Ответы:

DES AES ГОСТ 28147-89

Верный ответ: AES

2.Криптографическая система считается практически стойкой, если она имеет достаточно длинный ключ и для нее не существует метода вскрытия, существенно более эффективного, чем метод

Ответы:

«встреча посередине» бумеранга грубой силы

Верный ответ: грубой силы

3.Получение раундовых ключей из основного ключа шифрования называется

Ответы:

расписанием использования ключа процедурой расширения ключа ключевым пространством

Верный ответ: процедурой расширения ключа

4. Электромеханические шифровальные машины наподобие «Энигмы» основаны на использовании шифра

Ответы:

колонной замены Виженера гаммирования

Верный ответ: Виженера

5. Шифром замены является:

Ответы:

«скитала» «квадрат Полибия» «решетка Кардано»

Верный ответ: «квадрат Полибия»

4. Компетенция/Индикатор: ИД-2_{ПК-2} Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа

Вопросы, задания

1. Структура шифра AES.

2. Алгоритм ГОСТ Р 34.12-2015 «Кузнечик».

3. Алгоритм шифрования данных IDEA

4. Стандарт шифрования данных ГОСТ 28147-89.

5. Одноразовая система шифрования.

6. Шифрование методом Вернама.

7. Стандарт шифрования данных DES.

Материалы для проверки остаточных знаний

1. Блочными являются классические шифры

Ответы:

простой замены сложной замены перестановки

Верный ответ: перестановки

2. Число раундов алгоритма AES определяется

Ответы:

размером входного блока длиной ключа содержимым входного блока

Верный ответ: размером входного блока длиной ключа содержимым входного блока

3. Стойкость современных симметричных композиционных шифров, таких как DES, базируется:

Ответы:

на реализации принципов рассеивания и перемешивания; на секретности алгоритма шифрования; на бесконечности ключевой последовательности.

Верный ответ: на реализации принципов рассеивания и перемешивания;

4. S-блоком симметричного блочного алгоритма шифрования называется:

Ответы:

циклический сдвиг блока битов; таблица перестановки битов в блоке; таблица замены группы битов.

Верный ответ: таблица замены группы битов.

5. Алгоритмы DES и ГОСТ 28147 89 имеют структуру

Ответы:

«квадрат»; подстановочно-перестановочная сеть; сеть Фейстеля.

Верный ответ: сеть Фейстеля

5. Компетенция/Индикатор: ИД-4ПК-2 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем

Вопросы, задания

1. Распределение ключей с участием центра распределения для симметричных криптосистем.
2. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
3. Криптография с несколькими открытыми ключами.
4. Схема интерполяционных полиномов Лагранжа.
5. Протокол Фиата—Шамира.
6. Система аутентификации Шнорра.
7. Монетная система Чаума (David Chaum).

Материалы для проверки остаточных знаний

1. Если число N является простым, то значение функции Эйлера от N равно
Ответы:
 $N-1$
Верный ответ: $N-1$
2. Криптосистема Диффи — Хеллмана является протоколом
Ответы:
шифрования распределения ключей электронной подписи взаимной аутентификации
Верный ответ: распределения ключей
3. Модификация и подмена сообщений, передаваемых по каналу зашифрованной связи, а также навязывание ложных сообщений называется
Ответы:
помехами атакой на основе сбоя имитацией
Верный ответ: имитацией
4. Безопасность криптосистемы RSA основана на вычислительной сложности задачи ...
больших чисел
Ответы:
дискретного логарифмирования факторизации вычисления степени по модулю
Верный ответ: факторизации

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 5 находится в интервале от 90 до 100 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 4 находится в интервале от 70 до 89 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 3 находится в интервале от 60 до 69 баллов.

III. Правила выставления итоговой оценки по курсу

Итоговая оценка по курсу может быть рассчитана как среднее от текущей успеваемости и итогов промежуточной аттестации по 100 балльной шкале. Текущая успеваемость также рассчитывается как среднее по трем модулям по 100 балльной шкале. Только после этого можно переходить к 5-и балльной шкале. Промежуточное округление оценок в 5-и балльной системе и нелинейная шкала оценок в БАРС приводят к существенному завышению результирующих оценок.