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
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Пайков А.С. Идентификатор: R02d5e50d-PaikovAS-2468ee70	А.С. Пайков

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Гольцов А.Г. Идентификатор: R64210572-GoltsovAG-cebbd3e8	А.Г. Гольцов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков

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 (КЗЗ1) по курсу ЗИ Модуль 1 (65%) (Тестирование)
5. Контрольно-зачетное занятие (КЗЗ2) по курсу ЗИ Модуль 2 (65%) (Тестирование)
6. Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%) (Тестирование)

Форма реализации: Смешанная форма

1. Контроль посещения лекций по курсу ЗИ Модуль 1 (25%) (Интервью)
2. Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью)
3. Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью)

БРС дисциплины

8 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 Контроль посещения лекций по курсу ЗИ Модуль 1 (25%) (Интервью)
КМ-2 Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%) (Лабораторная работа)
КМ-3 Контрольно-зачетное занятие (КЗЗ1) по курсу ЗИ Модуль 1 (65%) (Тестирование)
КМ-4 Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью)
КМ-5 Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа)
КМ-6 Контрольно-зачетное занятие (КЗЗ2) по курсу ЗИ Модуль 2 (65%) (Тестирование)
КМ-7 Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью)
КМ-8 Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа)
КМ-9 Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%) (Тестирование)

Вид промежуточной аттестации – Экзамен.

Раздел дисциплины	Веса контрольных мероприятий, %								
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8	КМ-9
	Срок КМ:	4	4	4	8	8	8	12	12	12
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:	7,58	6,06	19,69	7,58	6,06	19,69	7,58	6,06	19,7

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	КМ-1 Контроль посещения лекций по курсу ЗИ Модуль 1 (25%) (Интервью) КМ-7 Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью) КМ-8 Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа) КМ-9 Контрольно-зачетное занятие (КЗЗ3) 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	КМ-4 Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью) КМ-5 Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа) КМ-6 Контрольно-зачетное занятие (КЗЗ2) по курсу ЗИ Модуль 2 (65%) (Тестирование) КМ-7 Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью) КМ-8 Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа) КМ-9 Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%) (Тестирование)
ПК-2	ИД-1$_{ПК-2}$ Демонстрирует знание нормативной базы, методов описания, анализа	Знать: основные алгоритмы и стандарты	КМ-3 Контрольно-зачетное занятие (КЗЗ1) по курсу ЗИ Модуль 1 (65%) (Тестирование) КМ-4 Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%)

	и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии	криптографической защиты информации Уметь: использовать современные информационные технологии при решении задач защиты информации	(Интервью) КМ-6 Контрольно-зачетное занятие (КЗ32) по курсу ЗИ Модуль 2 (65%) (Тестирование) КМ-8 Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа)
ПК-2	ИД-2$_{ПК-2}$ Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации Уметь: использовать современные инструментальные средства и технологии программирования	КМ-5 Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа) КМ-7 Контроль посещения лекций №10-15 по курсу ЗИ Модуль 3 (15%) (Интервью) КМ-8 Контроль выполнения комплекса лабораторных работ №8-11 по курсу ЗИ Модуль 3 (20%) (Лабораторная работа)
ПК-2	ИД-4$_{ПК-2}$ Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	Знать: принципы построения современных криптографических систем Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	КМ-2 Контроль выполнения комплекса лабораторных работ №1-4 по курсу ЗИ Модуль 1 (20%) (Лабораторная работа) КМ-3 Контрольно-зачетное занятие (КЗ31) по курсу ЗИ Модуль 1 (65%) (Тестирование) КМ-4 Контроль посещения лекций № 6-9 по курсу ЗИ Модуль 2 (15%) (Интервью) КМ-5 Контроль выполнения комплекса лабораторных работ №5, 6, 7 по курсу ЗИ Модуль 2 (20%) (Лабораторная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контроль посещения лекций по курсу ЗИ Модуль 1 (25%)

Формы реализации: Смешанная форма
Тип контрольного мероприятия: Интервью
Вес контрольного мероприятия в БРС: 7,58
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	Горбоносов 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	Михтинев 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:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы безопасности при работе в сети Интернет	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: устанавливать и применять средства защиты информации при её хранении и передаче по сети	1.обосновать сильные и слабые стороны исторических шифров 2.провести частотную атаку на шифр Цезаря 3.определить ключевое пространство простейшего шифра 4.рассчитать энтропию открытого и шифрованного текста

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 5 лекций модуля 1 равно 15. Оценка 5 находится в диапазоне 14 -15 баллов.

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 5 лекций модуля 1 равно 15. Оценка 4 находится в диапазоне 11 -13 баллов.

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 5 лекций модуля 1 равно 15. Оценка 3 находится в диапазоне 6 -12 баллов.

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 5 баллов. При отсутствии на всех лекциях по неуважительным причинам проставляется 0.

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: 6,06
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 К = 3¸15 (опция «Сдвиг»).

Опция «H» 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 «H»), выделить и зафиксировать наиболее информативные признаки (3-4 наибольших значения и их положение относительно друг друга) полученного распределения.
3. Для значения KE = (N+3)mod11+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	ц	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 a-97, код буквы b-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]
rwncfcpcwmspnjyglrcvrglqkyjjjcrrcpq
```

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

Пример для латинского алфавита :

```
ciphertext="yhaklwpnw";
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)mod11+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:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: принципы построения современных криптографических систем	1.Определение шифра простой замены 2.Определение шифра сложной замены 3.Система шифрования Цезаря 4.Афинная система подстановок 5.Принципы построения криптосистемы Хилла 6.Система шифрования Вижинера 7.Принцип построения системы шифрования Вернама
Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.Комплексные вопросы на знания и умения задаются на контрольно-зачетном занятии по модулю 1 - КЗЗ1 2.Провести частотную атаку на шифр Цезаря 3.Разработать модули шифрования и дешифрования для криптосистемы Хилла 4.Разработать модуль расшифрования для алгоритма простой перестановки 5.Разработать модуль расшифрования для алгоритма столбцовой перестановки 6.Разработать модуль расшифрования по базовой таблице шифра Вижинера 7.Разработать модуль подготовки данных для шифрования Вернама

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 124. Оценка 5 находится в диапазоне 112 -124 балла.

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 124. Оценка 5 находится в диапазоне 87 -112 балла.

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 124. Оценка 3 находится в диапазоне 50 - 87 баллов.

Оценка: 2 («неудовлетворительно»)

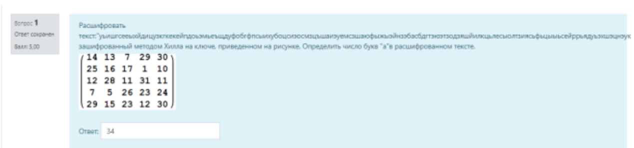
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 49 баллов. При отсутствии отчета по лабораторной работе по неуважительным причинам проставляется 0 баллов, и в соответствии с настройками системы Moodle студент не допускается к КЗЗ, пока не погасит задолженность.

КМ-3. Контрольно-зачетное занятие (КЗ1) по курсу ЗИ Модуль 1 (65%)

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 19,69
Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенном 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:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: основные алгоритмы и стандарты криптографической защиты информации	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.**
Знать: принципы построения современных криптографических систем	1.КЗ31 афинная система подстановок. Число баллов за правильно выполненное задание = 5. Число вариантов задания 450.
Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.**КЗ31 номер Цезарь. Число баллов за правильно выполненное задание = 3. Число вариантов задания 200.** 2.**КЗ31 простая перестановка. Число баллов за правильно выполненное задание = 3. Число вариантов задания 70.**

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	3.**КЗЗ1 система шифрования Вижинера. Число баллов за правильно выполненное задание = 7. Число вариантов задания 50.** 4.**КЗЗ1 столбцовая перестановка. Число баллов за правильно выполненное задание = 7. Число вариантов задания 50.**

Описание шкалы оценивания:

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

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 14 баллов. Оценка 2 проставляется при участии в контрольной, при отсутствии по неуважительным причинам проставляется 0.

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: 7,58
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	Подхолюзина 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:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения	1. режимы использования блочных шифров;
Знать: основные алгоритмы и стандарты криптографической защиты информации	1.методы программной реализации генераторов псевдослучайных последовательностей 2.методы аппаратной реализации генераторов псевдослучайных последовательностей 3.визуальные и оценочные тесты ПСП 4.процедура проведения оценочного теста 5. отечественные и зарубежные стандарты алгоритмов блочного шиф-рования;
Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.Контрольные вопросы на умения при регистрации присутствия не предусматриваются. 2.выбрать системные параметры линейного конгруэнтного генератора 3.анализировать структуру блочного шифра; 4.построить структурные элементы заданного блочного шифра 5.провести сравнительную оценку современных блочных шифров

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90

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

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 4 лекций модуля 1 равно 15. Оценка 4 находится в диапазоне 11 -13 баллов.

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 4 лекций модуля 1 равно 15. Оценка 3 находится в диапазоне 6 -12 баллов.

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 5 баллов. При отсутствии на всех лекциях по неуважительным причинам проставляется 0.

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: 6,06
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 Потоковый шифр 32

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения	1.Правила построения регистров сдвига с линейными обратными связями 2.алгоритмы программной реализации РСЛОС 3.число допустимых состояний РСЛОС 4.требования к исходному многочлену для построения РСЛОС с максимальным периодом 5.алгоритм формирования S-блока потокового шифра - аналога RC4 6.алгоритм шифрования RC4
Уметь: использовать современные инструментальные средства и технологии программирования	1.разработать и протестировать модуль шифрования RC4 2.разработать и протестировать модуль расшифрования RC4
Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.Комплексные вопросы на знания и умения задаются на контрольно-зачетном занятии по модулю 2 - КЗ32 2.разработать программную реализацию РСЛОС по заданному характеристическому многочлену

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	3.провести частотный анализ двоичной последовательности на выходе РСЛОС 4.разработать программный модуль генератора Геффе

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 91. Оценка 5 находится в диапазоне 82 - 91 балл.

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 91. Оценка 4 находится в диапазоне 64 -81 балл.

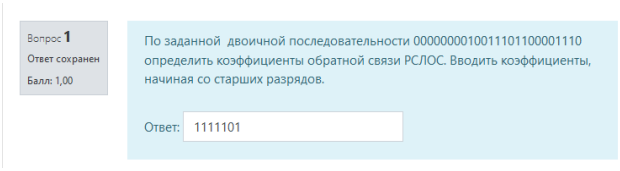
Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 91. Оценка 3 находится в диапазоне 37 - 63 балл.

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 36 баллов. При отсутствии отчета по лабораторной работе по неуважительным причинам проставляется 0 баллов, и в соответствии с настройками системы Moodle студент не допускается к КЗЗ, пока не погасит задолженность.

КМ-6. Контрольно-зачетное занятие (КЗЗ2) по курсу ЗИ Модуль 2 (65%)

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 19,69
Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенном 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 КЗЗ2:



Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения	1.**КЗЗ2 расшифрование RC4. Число баллов за правильно выполненное задание = 5. Число вариантов задания 48.** 2.**КЗЗ2 РСЛОС последовательность. Число баллов за правильно выполненное задание = 3. Число вариантов задания 500.** 3.**КЗЗ2 система Вернама зашифровать. Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.**
Уметь: использовать современные информационные технологии при решении задач защиты информации	1.**КЗЗ2 РСЛОС состояние. Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.** 2.**КЗЗ2 система Вернама расшифровать. Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.** 3.**КЗЗ2 шифрование RC4. Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.**

Описание шкалы оценивания:

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

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 13 баллов. Оценка 2 проставляется при участии в контрольной, при отсутствии по неуважительным причинам проставляется 0.

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: 7,58

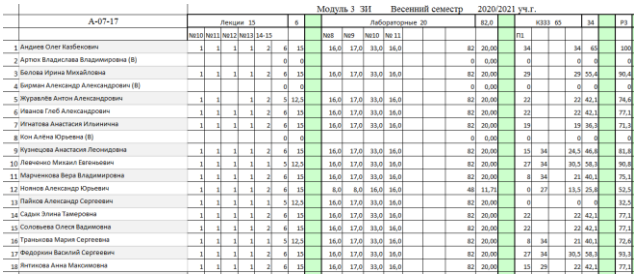
Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись.

Зарегистрироваться в Webex и присутствовать на лекции.

Пример выполнения (не выполнения) задания:



Модуль 3 ЗИ Весенний семестр 2020/2021 уч.г.

А-07-17	Лекции 15					6		Лабораторные 20				82,0		КЗЗЗ 65			34	Р3	
	№10	№11	№12	№13	14-15			№8	№9	№10	№ 11			П1					
1 Андиев Олег Казбекович	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	34			34	63	100
2 Артюх Владислава Владимировна (В)						0	0					0	0,00	0			0	0	0
3 Белова Ирина Михайловна	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	29			29	55,4	90,4
4 Бирман Александр Александрович (В)						0	0					0	0,00	0			0	0	0
5 Журавлёв Антон Александрович	1	1		1	2	5	12,5	16,0	17,0	33,0	16,0	82	20,00	22			22	42,1	74,6
6 Иванов Глеб Александрович	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	22			22	42,1	77,1
7 Игнатова Анастасия Ильинична	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	19			19	36,3	71,3
8 Кон Алёна Юрьевна (В)						0	0					0	0,00	0			0	0	0
9 Кузнецова Анастасия Леонидовна	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	15	34		24,5	46,8	81,8
10 Левченко Михаил Евгеньевич	1	1	1	1	1	5	12,5	16,0	17,0	33,0	16,0	82	20,00	27	34		30,5	58,3	90,8
11 Марченкова Вера Владимировна	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	8	34		21	40,1	75,1
12 Новиков Александр Юрьевич	1	1	1	1	2	6	15	8,0	8,0	16,0	16,0	48	11,71	0	27		13,5	25,8	52,5
13 Пайков Александр Сергеевич	1	1	1	1	1	5	12,5	16,0	17,0	33,0	16,0	82	20,00	0			0	0	32,5
14 Садик Элина Таировна	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	22			22	42,1	77,1
15 Соловьева Олеся Вадимовна	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	22			22	42,1	77,1
16 Транкова Мария Сергеевна	1	1	1	1	1	5	12,5	16,0	17,0	33,0	16,0	82	20,00	8	34		21	40,1	72,6
17 Федорин Василий Сергеевич	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	27	34		30,5	58,3	93,3
18 Янтикова Анна Максимовна	1	1	1	1	2	6	15	16,0	17,0	33,0	16,0	82	20,00	15	29		22	42,1	77,1

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы безопасности при работе в сети Интернет	1.Обобщенная схема асимметричной криптосистемы 2.Принципы построения криптосистемы RSA 3.Принципы построения криптосистемы Эль-Гамаля 4.Хэш функции 5.Электронно-цифровая подпись RSA 6.Комбинированный метод шифрования 7.**Протоколы с нулевым разглашением**
Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения	1.**Концепция криптосистемы с открытым ключом**
Уметь: использовать современные инструментальные средства и технологии программирования	1.Контрольные вопросы на умения при регистрации присутствия не предусматриваются. 2.построить схему шифрования RSA 3.построить схему шифрования RSA 4.применить встроенные хэш - функции системы Mathematica 5.проверить документ с ЭЦП RSA 6.определить секрет в схеме интерполяционных полиномов Лагранжа

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 6 лекций модуля 3 равно 15. Оценка 5 находится в диапазоне 14 -15 баллов.

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 6 лекций модуля 3 равно 15. Оценка 4 находится в диапазоне 11 -13 баллов.

Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Максимальное число набранных баллов при при посещении всех 6 лекций модуля 3 равно 15. Оценка 3 находится в диапазоне 6 -12 баллов.

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 5 баллов. При отсутствии на всех лекциях по неуважительным причинам проставляется 0.

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: 6,06
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:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы безопасности при работе в сети Интернет	1.**Криптоаналитическая атака при возможности выбора открытого текста.** 2.**Криптоаналитическая атака с адаптивным выбором открытого текста.** 3.**Криптоаналитическая атака методом полного перебора всех возможных ключей.**
Знать: этапы проведения эксперимента по	1.Подмена

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
проверке корректности принимаемого проектного решения	2.Повтор 3.Криптоаналитическая атака при наличии только известного шифртекста. 4.Криптоаналитическая атака при наличии известного открытого текста.
Знать: основные алгоритмы и стандарты криптографической защиты информации	1.Комплексные вопросы на знания и умения задаются на контрольно-зачетном занятии по модулю 3 - КЗЗ3 2.Активный перехват 3.Маскарад 4.Ренегатство 5.Алгоритм шифрования ГОСТ 28147-89
Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации	1.Атака “человек посередине” (Man in the middle) 2.Криптосистема RSA 3.Электронно-цифровая подпись RSA 4.Системы с несколькими открытыми ключами
Уметь: осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности	1.Проверить ЭЦП RSA
Уметь: использовать современные информационные технологии при решении задач защиты информации	1.Сформировать системные параметры алгоритма RSA
Уметь: использовать современные инструментальные средства и технологии программирования	1.Комплексные вопросы на знания и умения задаются на контрольно-зачетном занятии по модулю 3 - КЗЗ2 2.Инсталлировать систему Crypton на виртуальной машине 3.Создать ключ пользователя 4.Расшифровать заданный текст в системе Crypton 5.Подписать документ на секретном ключе RSA 6.Найти секрет в (k,n) пороговой схеме на базе интерполяционных многочленов Лаганжа

Описание шкалы оценивания:

Оценка: 5 («отлично»)
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 4-х лабораторных работ модуля 3 равно 82. Оценка 5 находится в диапазоне 74 - 82 балла.

Оценка: 4 («хорошо»)
Нижний порог выполнения задания в процентах: 70

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

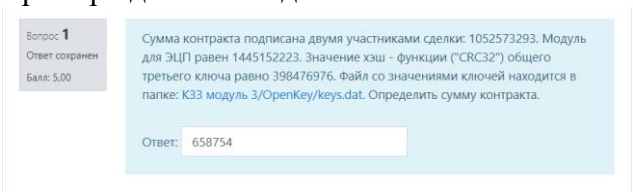
Оценка: 3 («удовлетворительно»)
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Максимальное число набранных баллов при при успешном выполнении всех 4-х лабораторных работ модуля 3 равно 82. Оценка 3 находится в диапазоне 33 - 57 балла.

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 32 баллов. При отсутствии отчета по лабораторной работе по неуважительным причинам проставляется 0 баллов, и в соответствии с настройками системы Moodle студент не допускается к КЗЗ, пока не погасит задолженность.

КМ-9. Контрольно-зачетное занятие (КЗЗ3) по курсу ЗИ Модуль 3 (65%)

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 19,7
Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенном 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 КЗЗ3:



Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы безопасности при работе в сети Интернет	1.**КЗЗ3 OpenKey. Число баллов за правильно выполненное задание = 5. Число вариантов задания 500.** 2.**КЗЗ3 Схемы разделения секрета. Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.**
Знать: этапы проведения эксперимента по проверке корректности принимаемого проектного решения	1.**КЗЗ3 ЭЦП RSA.Число баллов за правильно выполненное задание = 7. Число вариантов задания 500.**

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности	1.**КЗЗ3 RSA+Цезарь. Число баллов за правильно выполненное задание = 3. Число вариантов задания 48.** 2.**КЗЗ3 КОД 16 -- Криптон. Число баллов за правильно выполненное задание = 5. Число вариантов задания 48.** 3.**КЗЗ3 Умножение байтов AES. Число баллов за правильно выполненное задание = 7. Число вариантов задания 250.**

Описание шкалы оценивания:

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

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 13 баллов. Оценка 2 проставляется при участии в контрольной, при отсутствии по неуважительным причинам проставляется 0.

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 анщъдщцъчзъдмнщзъмнкзъд 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+x17+x20. Начальное состояние РСЛОС составляет CBCDB 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.

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.

I. 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.***Вопросы к экзамену ЗИ***

Принципы криптографической защиты информации.
Обобщенная схема симметричной, асимметричной криптосистемы. Основные типы криптоаналитических атак.
Традиционные симметричные криптосистемы.
Шифры перестановки.
Шифрующие таблицы.

Шифры простой замены.
Полибианский квадрат.
Система шифрования Цезаря.
Математический анализ шифра простой замены (подстановки).
Система Цезаря с ключевым словом.
Шифрующие таблицы Трисемуса.
Биграммный шифр Плейфейра.
Система омофонов.

Шифры сложной замены.
Шифр Гронсфельда.
Система шифрования Вижинера.
Шифр "двойной квадрат" Уитстона.
Одноразовая система шифрования.
Шифрование методом Вернама.
Роторные машины.
Шифрование методом гаммирования.

Методы генерации псевдослучайных последовательностей чисел.
Регистры сдвига с линейной обратной связью.

Современные симметричные криптосистемы.
Стандарт шифрования данных DES.
Режим "Электронная кодовая книга".
Режим "Сцепление блоков шифра".
Режим "Обратная связь по шифру".
Режим "Обратная связь по выходу".

Алгоритм шифрования данных IDEA.
Стандарт шифрования данных ГОСТ 28147-89.
Режим простой замены.
Режим гаммирования.
Режим гаммирования с обратной связью.
Режим выработки имитовставки.

Асимметричные криптосистемы.
Концепция криптосистемы с открытым ключом.
Однонаправленные функции.
Криптосистема шифрования данных RSA.
Схема шифрования Эль Гамаля.

Управление криптографическими ключами.
Метод генерации сеансового ключа в стандарте ANSI X9.17.
Хранение ключей.
Концепция иерархии ключей.
Распределение ключей с участием центра распределения для симметричных криптосистем.
Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
Алгоритм открытого распределения ключей Диффи–Хеллмана.

Трехпроходный протокол Шамира.
Скрытый канал на основе схемы Эль - Гамаля .
Криптография с несколькими открытыми ключами.
Схема интерполяционных полиномов Лагранжа.

Протокол Фиата—Шамира. Монетная система Чаума (David Chaum).
Структура шифра AES. Функция x-time шифра AES.

Алгоритм ГОСТ Р 34.12-2015 «Кузнечик». Основные параметры алгоритма ГОСТ Р 34.12-2015 «Кузнечик». Раундовое преобразование R. Полнораундовый алгоритм зашифрования ГОСТ Р 34.12-2015 «Кузнечик».
Алгоритм развертки ключа шифра ГОСТ Р 34.12-2015 «Кузнечик».

2.Задания уровня 3
Простая перестановка
Номер Цезарь
РСЛОС последовательность
RSA+Цезарь

3.Задания уровня 5
Ключевое слово
Афинная система подстановок
Криптосистема Хилла
Расшифрование RC4
OpenKey
4.Задания уровня 7
Система шифрования Вижинера
Столбцовая перестановка
Система Вернама зашифровать
РСЛОС состояние
Шифрование RC4
ЭЦП RSA
Схемы разделения секрета
КОД 16 -- Криптон
Умножение байтов AES

Материалы для проверки остаточных знаний

1.Режим работы шифров ... позволяет шифровать сообщение блоками, отличными от размера блока алгоритма шифрования

Ответы:

электронная кодовая книга ECB сцепление блоков шифротекста CBC обратная связь по шифротексту CFB

Верный ответ: обратная связь по шифротексту CFB

2.Если число *N* является простым, то значение функции Эйлера от *N* равно

Ответы:

N! N N/2 N-1

Верный ответ: N-1

3.Криптосистема Диффи — Хеллмана является протоколом

Ответы:

шифрования распределения ключей электронной подписи взаимной аутентификации

Верный ответ: распределения ключей

4.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

5.Модификация и подмена сообщений, передаваемых по каналу шифрованной связи, а также навязывание ложных сообщений называется

Ответы:

помехами атакой на основе сбоев имитацией

Верный ответ: имитацией

6.Алгоритм шифрования ... не имеет слабых ключей

Ответы:

DES AES ГОСТ 28147-89

Верный ответ: AES

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

Ответы:

«встреча посередине» бумеранга грубой силы

Верный ответ: грубой силы

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

Вопросы, задания

1.Режим простой замены.
2.Режим гаммирования с обратной связью.
3. Режим выработки имитовставки.
4.Асимметричные криптосистемы.
5.Концепция криптосистемы с открытым ключом.
6.Однонаправленные функции.
7.Криптосистема шифрования данных RSA.
8.Схема шифрования Эль Гамаля.
9.Управление криптографическими ключами.
10. Метод генерации сеансового ключа в стандарте ANSI X9.17.
11.Хранение ключей.
12.Концепция иерархии ключей.
13.Распределение ключей с участием центра распределения для симметричных криптосистем.

Материалы для проверки остаточных знаний

1.Безопасность криптосистемы RSA основана на вычислительной сложнос-ти задачи ... больших чисел

Ответы:

дискретного логарифмирования факторизации вычисления степени по модулю

Верный ответ: факторизации

2.Наиболее распространенной на практике системой шифрования с откры-тым ключом является шифр

Ответы:

RSA Эль-Гамаля Шамира

Верный ответ: RSA

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.Блочными являются классические шифры

Ответы:

простой замены сложной замены перестановки

Верный ответ: перестановки

6.Шифром замены является:

Ответы:

«скитала» «квадрат Полибия» «решетка Кардано»

Верный ответ: «квадрат Полибия»

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.Режим гаммирования.
2.Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
3.Трехпроходный протокол Шамира.
4.Скрытый канал на основе схемы Эль - Гамаля .
5.Криптография с несколькими открытыми ключами.
6.Схема интерполяционных полиномов Лагранжа.
7.Протокол Фиата—Шамира.
8.Система аутентификации Шнорра.
9.Монетная система Чаума (David Chaum).
10.Структура шифра AES.
11.Функция x-time шифра AES.
12.Алгоритм ГОСТ Р 34.12-2015 «Кузнечик».
13.Основные параметры алгоритма ГОСТ Р 34.12-2015 «Кузнечик».
14. Раундовое преобразование R.
15.Алгоритм открытого распределения ключей Диффи–Хеллмана.

16.Полнораундовый алгоритм зашифрования ГОСТ Р 34.12-2015 «Кузнечик».
17.Алгоритм развертки ключа шифра ГОСТ Р 34.12-2015 «Кузнечик».
18.Алгоритм шифрования данных IDEA
19.Принципы криптографической защиты информации.
20. Обобщенная схема симметричной, асимметричной криптосистемы.
21.Основные типы криптоаналитических атак.

Материалы для проверки остаточных знаний

1.Процесс извлечения открытого текста из криптограммы при условии знания ключа называется

Ответы:

расшифрованием дешифрованием зашифрованием

Верный ответ: расшифрованием

2.Предметом криптоанализа являются методы:

Ответы:

имитозащиты сообщений шифрования данных вскрытия шифров

Верный ответ: вскрытия шифров

3.Число раундов алгоритма AES определяется

Ответы:

размером входного блока длиной ключа содержимым входного блока

Верный ответ: размером входного блока длиной ключа содержимым входного блока

4.Какое равенство применяется при проверке электронно-цифровой подписи по схеме Эль-Гамаля

Ответы:

(y^a ·x^b)mod p =(g^M)mod p (a^y ·a^b)mod p =(g^M)mod p (y^a ·a^b)mod p =(g^M)mod p (y^a ·a^b)mod p =(M^g)mod p

Верный ответ: (y^a ·a^b)mod p =(g^M)mod p

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

Ответы:

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

Верный ответ: атака "человек посередине"

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. Шифры перестановки.
2.Шифрующие таблицы.
3.Шифры простой замены.
4. Полибианский квадрат.
5.Система шифрования Цезаря.
6.Математический анализ шифра простой замены (подстановки).
7. Система Цезаря с ключевым словом.
8. Шифрующие таблицы Трисемуса.
9. Биграммный шифр Плейфейра.
10. Стандарт шифрования данных ГОСТ 28147-89.
11. Система омофонов.
12. Система шифрования Вижинера.
13. Одноразовая система шифрования.
14. Шифрование методом Вернама.
15. Роторные машины.
16. Шифрование методом гаммирования.
17. Регистры сдвига с линейной обратной связью.
18.Современные симметричные криптосистемы.
19. Стандарт шифрования данных DES.
20.Режим "Электронная кодовая книга".
21. Режим "Сцепление блоков шифра".
22. Режим "Обратная связь по шифру".
23.Режим "Обратная связь по выходу".
24.Шифры сложной замены.

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 2n-1 2^n 2^n - 1 2^(n-1)

Верный ответ: 2^n - 1

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

Вопросы, задания

1.Тест-задание: OpenKey
2.Тест-задание: Схемы разделения секрета
3.Тест-задание: ЭЦП RSA
4.Тест-задание: Шифрование RC4
5.Тест-задание: РСЛОС состояние
6.Тест-задание: Система Вернама зашифровать
7.Тест-задание: Столбцовая перестановка
8.Тест-задание: Система шифрования Вижинера
9.Тест-задание: КОД 16 -- Криптон
10.Тест-задание: Умножение байтов AES
11.Тест-задание: Криптосистема Хилла
12.Тест-задание: Афинная система подстановок
13.Тест-задание: Ключевое слово
14.Тест-задание: RSA+Цезарь
15.Тест-задание: РСЛОС последовательность
16.Тест-задание: Номер Цезарь
17.Тест-задание: Простая перестановка
18.Тест-задание: Расшифрование RC4
19.Алгоритм цифровой подписи RSA .
20.Электронно-цифровая подпись DSA .
21.Электронная цифровая подпись
на основе схемы Эль - Гамаля
22.Методы генерации псевдослучайных последовательностей чисел.
23.Регистры сдвига с линейной обратной связью.
24.Методы оценки качества псевдослучайных последовательностей.
25.Оценка результатов тестирования статистических свойств генератора ПСП.
26.Анализ прохождения статистических тестов.
27.Анализ статистической безопасности криптоалгоритмов.

Материалы для проверки остаточных знаний

1. 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;

2. 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.

3.Алгоритмы DES и ГОСТ 28147 89 имеют структуру

Ответы:

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

Верный ответ: сеть Фейстеля

II. Описание шкалы оценивания

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

Оценка: 2 («неудовлетворительно»)
Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 2 находится в интервале от 0 до 59 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 бальной 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.