Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе
_____ Н.Г. Кузнецов
«01» июня 2018г.

Рабочая программа дисциплины

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Криптографические методы защиты информации

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Квалификация

Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Недель	17,3			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	36	36	36	36
В том числе инт.	44	44	44	44
Итого ауд.	54	54	54	54
Контактная	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

Рабочая программа составлена по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Учебный план утвержден учёным советом вуза от 27.03.2018 протокол № 10.

Программу составил(и): д.т.н., профессор, Соколов С.В. _____ 10.05.2018

Зав. кафедрой: Тищенко Е.Н. _____ 11.05.2018

Методическим советом направления: к.ф.-м.н., Карасев Д.И. _____ 29.05.2018

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.2018

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.2018

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели дисциплины. Изучение дисциплины направлено на достижение следующих целей: развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением криптографической защиты информации; развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления; привитие стремления к поиску оптимальных, простых и надежных решений; расширение кругозора.
1.2	Задачи дисциплины. Дать знания по вопросам: обеспечения криптографической защиты информации; методологии создания систем криптографической защиты информации; процессов сбора, передачи и накопления информации; методов и средств ведения информационных войн; оценки защищенности и обеспечения криптографической защиты информации компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.Б.16
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Необходимыми условиями для успешного освоения являются навыки, знания и умения, полученные в результате освоения дисциплин:
2.1.2	Информационные технологии
2.1.3	Математические основы обеспечения информационной безопасности
2.1.4	Теория информации
2.1.5	Средства и методы защиты хранилищ и баз данных
2.1.6	Теория информационной безопасности и методология защиты информации
2.1.7	Физико-технические основы обеспечения информационной безопасности
2.1.8	Дискретная математика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информационных процессов и систем
2.2.2	Защита от удаленных сетевых атак
2.2.3	Методы и средства обеспечения информационной безопасности
2.2.4	Модели разграничения доступа
2.2.5	Программно-аппаратные средства защиты информации
2.2.6	Техническая защита информации

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
Знать:
методы определения информационных ресурсов, подлежащие защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
Уметь:
определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
Владеть:
Методами определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
основные понятия криптологии, типы и виды шифрующих преобразований; существующие методы и средства, применяемые для криптографической защиты информации; системные вопросы криптографической защиты информации; симметричный способ шифрования;
Уметь:

проводить анализ информации с целью выработки и принятия решений и мер по обеспечению криптографической защиты информации и эффективному использованию средств обнаружения возможных каналов взлома шифртекстов, представляющих государственную, военную, служебную и коммерческую тайну;
Владеть:
навыками анализа действующих нормативных и методических документов по КЗИ;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интер акт.	Примечание
	Раздел 1. Понятие о традиционных методах шифрования						
1.1	Введение. История развития криптографии. Основные понятия и определения. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
1.2	Моноалфавитные шифры. Полиалфавитные шифры. Роторные шифровальные машины. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
1.3	Разработка криптосистемы на основе шифра Цезаря и системы взлома данного алгоритма. /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
1.4	Разработка криптосистемы на основе традиционных алгоритмов с использованием классов в Net Framework /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
1.5	Криптоанализ традиционных алгоритмов /Ср/	6	12	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
	Раздел 2. Анализ и синтез симметричных криптосистем						
2.1	История создания DES. Структура DES. Дешифрирование DES и режимы его использования. Аппаратная и программная реализация DES. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.2	Информационно - теоретический анализ криптографической стойкости. Анализ криптографической стойкости на основе теории сложности. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.3	Классы симметричных алгоритмов в Net Framework /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
2.4	Разработка криптосистемы на основе симметричного алгоритма DES с использованием классов в Net Framework /Лаб/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
2.5	Криптоанализ симметричных алгоритмов /Ср/	6	8	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
	Раздел 3. Криптосистемы с открытым ключом						
3.1	Делители и простые числа. Арифметика в классах вычетов. Теорема Эйлера. Дискретные логарифмы. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.2	Распределение открытых ключей. Распределение секретных ключей с использованием криптосистемы с открытым ключом. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	

3.3	Требования к цифровым подписям и их классификация. Основные алгоритмы цифровых подписей. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.4	Разработка криптосистемы на основе асимметричного алгоритма RSA с использованием классов в .Net Framework /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.5	Классы асимметричных алгоритмов в Net Framework /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.6	Разработка системы цифровой подписи на основе алгоритма DSA с использованием классов в Net Framework /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
3.7	Классы для работы с цифровыми подписями в Net Framework /Лаб/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
3.8	Принципы распределения ключей. Принципы управления ключами: иерархическое управление, децентрализованное управление, управление использованием.Электронная цифровая подпись и аутентификация в криптосистемах с открытым ключом. Криптоанализ систем с открытым ключом.Взаимная аутентификация. Односторонняя аутентификация. /Ср/	6	22	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	
	Раздел 4. Имитостойкость и помехоустойчивость криптосистем.Криптографические шифраторы.						
4.1	Основные принципы имитозащиты и помехоустойчивости криптосистем. Структура имитозащищенного помехоустойчивого канала связи. Имитозащита на основе режима выработки имитовставки. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
4.2	Функциональные возможности и структура аппаратного шифратора. Принцип действия аппаратного шифратора. Основные типы современных шифраторов. Основные направления развития технологии смарт-карт. /Лек/	6	2	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
4.3	Разработка системы хеширования на основе алгоритма MD5 с использованием классов в Net Framework /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	2	
4.4	Алгоритмы хэширования в Net Framework /Лаб/	6	4	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	4	
4.5	Средства и способы обеспечения помехоустойчивости информации. Способы имитозащиты вычислительных систем.Структура и программное обеспечение проходных шифраторов. Криптозащита информации при ее передаче по каналам специальной связи. /Ср/	6	12	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	

4.6	/Зачёт/	6	0	ОПК-7 ПК-1	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2 Э1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

ВОПРОСЫ К ЗАЧЕТУ:

1. Краткая характеристика основных этапов развития «наивной» и формальной криптографии.
2. Краткая характеристика основных этапов развития научной криптографии.
3. Сформулировать определения криптологии, криптографии и криптоанализа. Основные разделы современной криптографии.
4. Основные направления использования современной криптографии.
5. Сформулировать определения основных понятий криптографической защиты информации (конфиденциальности, аутентичности, алфавита, шифра, ключа, гаммирования, имитозащиты, криптографической защиты).
6. Сформулировать определения основных понятий криптографической защиты информации (электронной (цифровой) подписи, зашифровывания данных, расшифровывания данных, дешифрования, шифрования, гаммы шифра, синхропосылки).
7. Модель традиционного шифрования. Допущения о возможностях криптоаналитика.
8. Основные требования к криптосистемам.
9. Современные показатели криптостойкости. Уровни криптоатаки.
10. Основные направления современного криптоанализа.
11. Классификация методов криптографического преобразования информации.
12. Основные методы статистического криптоанализа моноалфавитных шифров.
13. Шифр Плейфейера: алгоритм шифрования и дешифрования; основные достоинства и недостатки.
14. Шифр Хилла: алгоритм шифрования и дешифрования; основные достоинства и недостатки.
15. Шифр Виженера: алгоритм шифрования и дешифрования; варианты формирования ключей; основные достоинства и недостатки.
16. Шифр Вернама: алгоритм шифрования и дешифрования; варианты формирования ключей; основные достоинства и недостатки.
17. Структурная схема и принцип действия роторной шифровальной машины.
18. Основные виды перестановочных шифров; способы повышения их стойкости.
19. Определение блочного шифра. Общая схема блочного шифрования, особенности ее практического использования.
20. Понятия идеального шифра, диффузии и конфузии. Примеры применения метода диффузии.
21. Структура шифра Файстеля.
22. Анализ конструктивных элементов шифра Файстеля и краткая характеристика алгоритма его дешифрования.
23. Применение блочных шифров в режиме электронной кодировочной книги.
24. Применение блочных шифров в режиме сцепления блоков шифрованного текста.
25. Применение блочных шифров в режиме обратной связи по шифрованному тексту.
26. Применение блочных шифров в режиме обратной связи по выходу.
27. Основные методы композиции шифров. Примеры композиций шифров.
28. Основные требования к стандарту шифрования данных.
29. Структура алгоритма DES. Анализ особенностей блоков начальной и заключительной перестановок.
30. Основные этапы преобразования ключей в алгоритме DES.
31. Анализ структуры блока перестановки с расширением (E−блока) в алгоритме DES и ее особенностей.
32. Анализ структуры подстановки с помощью S−блоков в алгоритме DES и ее особенностей.
33. Анализ структуры перестановки с помощью P−блоков в алгоритме DES и структуры алгоритма его дешифрования.
34. Структура алгоритма шифрования по ГОСТ 28147−89.
35. Теоретическая стойкость криптосистемы. Необходимое и достаточное условие совершенной секретности шифра, анализ размерности совершенно секретного ключа.
36. Практическая стойкость криптосистемы и параметры, ее характеризующие.
37. Классификация алгоритмов по степени их сложности.
38. Принцип построения схемы шифрования с открытым ключом.
39. Принцип построения схемы электронной цифровой подписи.
40. Принцип построения схемы аутентификации в криптосистемах с открытым ключом.
41. Принцип построения схемы шифрования и аутентификации с открытым ключом.
42. Условия применения криптосистем с открытым ключом. Понятие односторонней функции.
43. Основные виды криптоатак на криптосистемы с открытым ключом.
44. Сформулировать определения наибольшего общего делителя и взаимно простых чисел, основную теорему арифметики. Алгоритм Евклида.
45. Сформулировать определения чисел, сравнимых по модулю, вычетов и классов вычетов. Свойства сравнений по модулю.
46. Функция Эйлера − общий случай, для простого числа, для произведения простых чисел. Формулировка теоремы Эйлера и следствие из нее как основа построения алгоритма RSA.
47. Сформулировать определение показателя, которому принадлежит число a по модулю n, и определения, ему эквивалентные; показать их численную реализацию.

48. Сформулировать определение первообразного корня и свойства его степеней, определение дискретного логарифма (индекса числа b по модулю p при основании a), его свойства и особенности вычисления.
49. Структура алгоритма шифрования RSA. Условия его работоспособности и их теоретическое обоснование.
50. Схема формирования ключей в алгоритме RSA.
51. Методы вычислительной реализации процедуры шифрования / дешифрования в алгоритме RSA.
52. Методы вычислительной реализации процедуры формирования ключей в алгоритме RSA.
53. Основные направления и методы криптоанализа алгоритма RSA.
54. Методы повышения криптостойкости алгоритма RSA.
55. Организация криптосистем на основе канального и сквозного шифрования. Основные преимущества и недостатки обоих типов шифрования.
56. Основные способы распределения ключей в симметричных криптосистемах, их преимущества и недостатки. Типовая схема распределения ключей, использующая центр распределения ключей.
57. Схемы иерархического и децентрализованного управления ключами в симметричных криптосистемах.
58. Типы сеансовых ключей. Схема управления использованием ключей на основе управляющего вектора.
59. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием авторитетного источника открытых ключей.
60. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием сертификатов открытых ключей.
61. Основные способы распределения секретных ключей с использованием криптосистемы с открытым ключом. Алгоритм распределения секретных ключей с обеспечением конфиденциальности и аутентификации.
62. Структура и математическое обоснование алгоритма обмена ключами по схеме Диффи–Хеллмана.
63. Определение хэш–функции. Краткая характеристика требований к хэш–функциям.
64. Простые функции хэширования: примеры и их краткий анализ.
65. Парадокс дня рождения и схема основанной на нем атаки.
66. Способы использования хэш–функций.
67. Криптоанализ итерированных функций хэширования.
68. Возможности цифровых подписей и требования к ним. Анализ преимуществ и недостатков непосредственной цифровой подписи.
69. Основные схемы организации арбитражной цифровой подписи.
70. Организация цифровой подписи по схеме RSA. Анализ ее преимуществ и недостатков.
71. Формирование цифровой подписи по алгоритму DSA.
72. Верификация цифровой подписи по алгоритму DSA.
73. Основные виды атак с использованием воспроизведения сообщений и способы защиты от них.
74. Примеры протоколов взаимной аутентификации на основе традиционного шифрования. Анализ их преимуществ и недостатков.
75. Примеры протоколов взаимной аутентификации на основе шифрования с открытым ключом. Анализ их преимуществ и недостатков.
76. Протокол односторонней аутентификации на основе традиционного шифрования. Анализ его преимуществ и недостатков.
77. Примеры протоколов односторонней аутентификации на основе шифрования с открытым ключом. Анализ их преимуществ и недостатков.
78. Сформулировать определения имитозащиты и помехоустойчивости криптосистем.
79. Основные виды алгоритмов помехоустойчивого кодирования. Имитозащита на основе режима выработки имитовставки по ГОСТ 28147–89.
80. Структура имитозащищенного помехоустойчивого канала связи и принцип его функционирования. Решение проблемы синхронизации генераторов ключей.
81. Области применения случайных чисел в криптографии. Требования к случайным числовым последовательностям. Физические источники случайных чисел.
82. Требования к криптографически стойким генераторам псевдослучайных последовательностей и их криптообоснование. Примеры способов генерации псевдослучайных последовательностей.
83. Конгруэнтный способ генерации псевдослучайных последовательностей и анализ его параметров. Критерии качества генераторов псевдослучайных последовательностей.
84. Криптографические генераторы псевдослучайных последовательностей на основе циклического шифрования и режима обратной связи по выходу алгоритма DES.
85. Криптографический генератор псевдослучайных последовательностей ANSI X9.17.
86. Криптографический генератор псевдослучайных последовательностей BBS.
87. Классификация шифраторов и краткая характеристика их основных типов.
88. Функциональные возможности аппаратных шифраторов. Типовая структурная схема аппаратного шифратора.
89. Принцип действия аппаратного шифратора.
90. Аппаратный шифратор "Шипка -1.5" и краткая характеристика его функциональных возможностей.
91. Основные направления развития технологии смарт-карт (цифровых интеллектуальных карт).
92. Функциональные возможности и структура "проходного" шифратора.
93. Программное обеспечение "проходного" шифратора и его взаимодействие с программами компьютера.
94. Сравнительный анализ технических характеристик основных типов современных криптотелефонов.
95. Шифраторы семейства "Криптон" и краткая характеристика их функциональных возможностей.
96. Сравнительный анализ технических характеристик основных типов современных специализированных шифраторов.

5.2. Фонд оценочных средств для проведения текущего контроля
Структура и содержание фонда оценочных средств представлены в Приложении 1 к рабочей программе дисциплины

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
6.1. Рекомендуемая литература				
6.1.1. Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Соколов С. В., Серпенинов О. В., Тищенко Е. Н.	Криптографическая защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность"	Ростов н/Д: Изд-во РГЭУ "РИНХ", 2011	66
Л1.2	Романьков В. А.	Алгебраическая криптография	Омск: Омский государственный университет, 2013	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Соколов С. В.	Защита информационных процессов в компьютерных системах: метод. рекомендации по выполнению лаборатор. работ	Ростов н/Д: Изд-во РГЭУ "РИНХ", 2009	10
Л2.2	Альбов А. С.	Квантовая криптография	Санкт-Петербург: Страта, 2015	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Тищенко Е. Н., Максимов А. М., Тирацуян Е. О.	Криптографическая защита информации: метод. указания для лаборатор. работ	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2013	10
Л3.2	Тищенко Е. Н., Максимов А. М., Тирацуян Е. О.	Криптографическая защита информации: метод. указания для выполнения практ. заданий	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2013	10
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	Сайт ФСТЭК РФ/fstec.ru			
6.3. Перечень программного обеспечения				
6.3.1	Microsoft Word, DallasLock			
6.4 Перечень информационных справочных систем				
6.4.1	Консультант+			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
Методические указания по усвоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины

Приложение 1
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры Информационных
технологий и защиты информации
Протокол №10 от «12» мая 2018 г.
Зав.кафедрой _____ *Тищенко Е.Н.*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Б1.Б.16.4 «Криптографические методы защиты информации»
(наименование дисциплины)

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль подготовки
10.03.01.02 «Организация и технология защиты информации»
(указывается код и наименование профиля подготовки)

Уровень образования
бакалавриат

Составитель _____ Соколов С.В., профессор, дтн, профессор
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Оглавление

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы 3

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания 3

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы 7

4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций 39

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

1.1 Перечень компетенций с указанием этапов их формирования представлен в п. 3. «Требования к результатам освоения дисциплины» рабочей программы дисциплины.

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

2.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
Знать / Уметь / Владеть ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты			
З: методы определения информационных ресурсов, подлежащие защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты			
У: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты			
В: методами определения информационных ресурсов,			

подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты			
ПК-1 - способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в т.ч. криптографических) и технических средств защиты информации			
З: основные понятия криптологии, типы и виды шифрующих преобразований; существующие методы и средства, применяемые для криптографической защиты информации; системные вопросы криптографической защиты информации; симметричный и асимметричный способы шифрования; алгоритмы функционирования криптографических систем с открытым ключом; существующие способы атаки на шифр и подходы к определению стойкости криптографических систем; основные требования к программной и программно-аппаратной реализации методов криптографической защиты информации; виды односторонних функций, смысл и назначение функции хэширования; алгоритмы цифровой подписи сообщений, принцип открытого распределения ключей.	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно коммуникационных технологий и глобальных информационных ресурсов	соответствие поставленной проблеме; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, неполном объеме); соответствие отчета требованиям	ЛР – лабораторная работа

У: проводить анализ информации с целью выработки и принятия решений и мер по обеспечению криптографической защиты информации и эффективному использованию средств обнаружения возможных каналов взлома шифртекстов, представляющих государственную, военную, служебную и коммерческую тайну; анализировать методы и средства криптографической защиты информации и разрабатывать предложения по их совершенствованию и повышению эффективности КЗИ; осуществлять квалифицированный выбор криптографических систем для конкретных практических приложений; строить алгоритмы формирования псевдослучайных последовательностей и осуществлять их реализацию на базе регистров сдвига с обратной связью; строить алгоритмы открытого распределения ключей с использованием односторонних функций различных видов.	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно - коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, неполном объеме); соответствие отчета требованиям	ЛР – лабораторная работа
В: навыками анализа действующих нормативных и методических документов по КЗИ; анализа новых схем аппаратуры криптографической защиты информации и средств ее	поиск и сбор необходимой литературы, использование различных баз данных, использование	соответствие проблеме; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию;	ЛР – лабораторная работа

автоматизации; анализа моделей и систем криптографической защиты информации; оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по КЗИ; аттестации и категорирования объектов криптографической защиты информации.	современных информационно-коммуникационных технологий и глобальных информационных ресурсов	умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям	

2.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляются в рамках накопительной балльно-рейтинговой системы по 100-балльной шкале:

- 84-100 баллов (оценка «отлично») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, выпускник усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 баллов (оценка "удовлетворительно") - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (оценка "неудовлетворительно") - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Вопросы к экзамену

по дисциплине «Криптографические методы защиты информации»
(наименование дисциплины)

1. Краткая характеристика основных этапов развития «наивной» и формальной криптографии.
2. Краткая характеристика основных этапов развития научной криптографии.
3. Сформулировать определения криптологии, криптографии и криптоанализа. Основные разделы современной криптографии.
4. Основные направления использования современной криптографии.
5. Сформулировать определения основных понятий криптографической защиты информации (конфиденциальности, аутентичности, алфавита, шифра, ключа, гаммирования, имитозащиты, криптографической защиты).
6. Сформулировать определения основных понятий криптографической защиты информации (электронной (цифровой) подписи, зашифровывания данных, расшифровывания данных, дешифрования, шифрования, гаммы шифра, синхропосылки).
7. Модель традиционного шифрования. Допущения о возможностях криптоаналитика.
8. Основные требования к криптосистемам.
9. Современные показатели криптостойкости. Уровни криптоатаки.
10. Основные направления современного криптоанализа.
11. Классификация методов криптографического преобразования информации.
12. Основные методы статистического криптоанализа моноалфавитных шифров.
13. Шифр Плейфейера: алгоритм шифрования и дешифрования; основные достоинства и недостатки.
14. Шифр Хилла: алгоритм шифрования и дешифрования; основные достоинства и недостатки.
15. Шифр Виженера: алгоритм шифрования и дешифрования; варианты

формирования ключей; основные достоинства и недостатки.
16. Шифр Вернама: алгоритм шифрования и дешифрования; варианты формирования ключей; основные достоинства и недостатки.
17. Структурная схема и принцип действия роторной шифровальной машины.
18. Основные виды перестановочных шифров; способы повышения их стойкости.
19. Определение блочного шифра. Общая схема блочного шифрования, особенности ее практического использования.
20. Понятия идеального шифра, диффузии и конфузии. Примеры применения метода диффузии.
21. Структура шифра Файстеля.
22. Анализ конструктивных элементов шифра Файстеля и краткая характеристика алгоритма его дешифрования.
23. Применение блочных шифров в режиме электронной кодировочной книги.
24. Применение блочных шифров в режиме сцепления блоков шифрованного текста.
25. Применение блочных шифров в режиме обратной связи по шифрованному тексту.
26. Применение блочных шифров в режиме обратной связи по выходу.
27. Основные методы композиции шифров. Примеры композиций шифров.
28. Основные требования к стандарту шифрования данных.
29. Структура алгоритма DES. Анализ особенностей блоков начальной и заключительной перестановок.
30. Основные этапы преобразования ключей в алгоритме DES.
31. Анализ структуры блока перестановки с расширением (Е–блока) в алгоритме DES и ее особенностей.
32. Анализ структуры подстановки с помощью S–блоков в алгоритме DES и ее особенностей.
33. Анализ структуры перестановки с помощью Р–блоков в алгоритме DES и структуры алгоритма его дешифрования.
34. Структура алгоритма шифрования по ГОСТ 28147–89.
35. Теоретическая стойкость криптосистемы. Необходимое и достаточное условие совершенной секретности шифра, анализ размерности совершенно секретного ключа.
36. Практическая стойкость криптосистемы и параметры, ее характеризующие.
37. Классификация алгоритмов по степени их сложности.
38. Принцип построения схемы шифрования с открытым ключом.
39. Принцип построения схемы электронной цифровой подписи.
40. Принцип построения схемы аутентификации в криптосистемах с открытым ключом.
41. Принцип построения схемы шифрования и аутентификации с открытым ключом.
42. Условия применения криптосистем с открытым ключом. Понятие односторонней функции.
43. Основные виды криптоатак на криптосистемы с открытым ключом.
44. Сформулировать определения наибольшего общего делителя и взаимно простых чисел, основную теорему арифметики. Алгоритм Евклида.
45. Сформулировать определения чисел, сравнимых по модулю, вычетов и классов вычетов. Свойства сравнений по модулю.
46. Функция Эйлера – общий случай, для простого числа, для произведения простых чисел. Формулировка теоремы Эйлера и следствие из нее как основа построения алгоритма RSA.
47. Сформулировать определение показателя, которому принадлежит число a по

модулю n, и определения, ему эквивалентные; показать их численную реализацию.
48. Сформулировать определение первообразного корня и свойства его степеней, определение дискретного логарифма (индекса числа b по модулю p при основании a), его свойства и особенности вычисления.
49. Структура алгоритма шифрования RSA. Условия его работоспособности и их теоретическое обоснование.
50. Схема формирования ключей в алгоритме RSA.
51. Методы вычислительной реализации процедуры шифрования / дешифрования в алгоритме RSA.
52. Методы вычислительной реализации процедуры формирования ключей в алгоритме RSA.
53. Основные направления и методы криптоанализа алгоритма RSA.
54. Методы повышения криптостойкости алгоритма RSA.
55. Организация криптосистем на основе канального и сквозного шифрования. Основные преимущества и недостатки обоих типов шифрования.
56. Основные способы распределения ключей в симметричных криптосистемах, их преимущества и недостатки. Типовая схема распределения ключей, использующая центр распределения ключей.
57. Схемы иерархического и децентрализованного управления ключами в симметричных криптосистемах.
58. Типы сеансовых ключей. Схема управления использованием ключей на основе управляющего вектора.
59. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием авторитетного источника открытых ключей.
60. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием сертификатов открытых ключей.
61. Основные способы распределения секретных ключей с использованием криптосистемы с открытым ключом. Алгоритм распределения секретных ключей с обеспечением конфиденциальности и аутентификации.
62. Структура и математическое обоснование алгоритма обмена ключами по схеме Диффи–Хеллмана.
63. Определение хэш–функции. Краткая характеристика требований к хэш–функциям.
64. Простые функции хэширования: примеры и их краткий анализ.
65. Парадокс дня рождения и схема основанной на нем атаки.
66. Способы использования хэш–функций.
67. Криптоанализ итерированных функций хэширования.
68. Возможности цифровых подписей и требования к ним. Анализ преимуществ и недостатков непосредственной цифровой подписи.
69. Основные схемы организации арбитражной цифровой подписи.
70. Организация цифровой подписи по схеме RSA. Анализ ее преимуществ и недостатков.
71. Формирование цифровой подписи по алгоритму DSA.
72. Верификация цифровой подписи по алгоритму DSA.
73. Основные виды атак с использованием воспроизведения сообщений и способы защиты от них.
74. Примеры протоколов взаимной аутентификации на основе традиционного шифрования. Анализ их преимуществ и недостатков.
75. Примеры протоколов взаимной аутентификации на основе шифрования с открытым ключом. Анализ их преимуществ и недостатков.
76. Протокол односторонней аутентификации на основе традиционного шифрования. Анализ его преимуществ и недостатков.

77. Примеры протоколов односторонней аутентификации на основе шифрования с открытым ключом. Анализ их преимуществ и недостатков.
78. Сформулировать определения имитозащиты и помехоустойчивости криптосистем.
79. Основные виды алгоритмов помехоустойчивого кодирования. Имитозащита на основе режима выработки имитовставки по ГОСТ 28147−89.
80. Структура имитозащищенного помехоустойчивого канала связи и принцип его функционирования. Решение проблемы синхронизации генераторов ключей.
81. Области применения случайных чисел в криптографии. Требования к случайным числовым последовательностям. Физические источники случайных чисел.
82. Требования к криптографически стойким генераторам псевдослучайных последовательностей и их криптообоснование. Примеры способов генерации псевдослучайных последовательностей.
83. Конгруэнтный способ генерации псевдослучайных последовательностей и анализ его параметров. Критерии качества генераторов псевдослучайных последовательностей.
84. Криптографические генераторы псевдослучайных последовательностей на основе циклического шифрования и режима обратной связи по выходу алгоритма DES.
85. Криптографический генератор псевдослучайных последовательностей ANSI X9.17.
86. Криптографический генератор псевдослучайных последовательностей BBS.
87. Классификация шифраторов и краткая характеристика их основных типов.
88. Функциональные возможности аппаратных шифраторов. Типовая структурная схема аппаратного шифратора.
89. Принцип действия аппаратного шифратора.
90. Аппаратный шифратор "Шипка -1.5" и краткая характеристика его функциональных возможностей.
91. Основные направления развития технологии смарт-карт (цифровых интеллектуальных карт).
92. Функциональные возможности и структура "проходного" шифратора.
93. Программное обеспечение "проходного" шифратора и его взаимодействие с программами компьютера.
94. Сравнительный анализ технических характеристик основных типов современных криптотелефонов.
95. Шифраторы семейства "Криптон" и краткая характеристика их функциональных возможностей.
96. Сравнительный анализ технических характеристик основных типов современных специализированных шифраторов.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_1__

по дисциплине Криптографические методы защиты информации

1. Краткая характеристика основных этапов развития «наивной» и формальной криптографии.
2. Структура алгоритма шифрования RSA. Условия его работоспособности и их теоретическое обоснование.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_2__

по дисциплине Криптографические методы защиты информации

1. Краткая характеристика основных этапов развития научной криптографии.
2. Схема формирования ключей в алгоритме RSA.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_3__

по дисциплине Криптографические методы защиты информации

1. Сформулировать определения криптологии, криптографии и криптоанализа. Основные разделы современной криптографии.
2. Методы вычислительной реализации процедуры шифрования/ дешифрования в алгоритме RSA.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_4__

по дисциплине Криптографические методы защиты информации

1. Основные направления использования современной криптографии.
2. Основные направления и методы криптоанализа алгоритма RSA.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_5__

по дисциплине Криптографические методы защиты информации

1. Сформулировать определения основных понятий криптографической защиты информации (конфиденциальности, аутентичности, алфавита, шифра, ключа, гаммирования, имитозащиты, криптографической защиты).
2. Сравнительный анализ технических характеристик основных типов современных специализированных шифраторов.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_6__

по дисциплине Криптографические методы защиты информации

1. Сформулировать определения основных понятий криптографической защиты информации (электронной (цифровой) подписи, зашифровывания данных, расшифровывания данных, дешифрования, шифрования, гаммы шифра, синхропосылки).
2. Методы повышения криптостойкости алгоритма RSA.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко

(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_7__

по дисциплине Криптографические методы защиты информации

1. Модель традиционного шифрования. Допущения о возможностях криптоаналитика.
2. Сформулировать определения имитозащиты и помехоустойчивости криптосистем. Основные виды алгоритмов помехоустойчивого кодирования.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_8__

по дисциплине Криптографические методы защиты информации

1. Основные требования к криптосистемам.

2. Структура имитозащищенного помехоустойчивого канала связи и принцип его функционирования. Решение проблемы синхронизации генераторов ключей.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_9__

по дисциплине Криптографические методы защиты информации

1. Современные показатели криптостойкости. Уровни криптоатаки.
2. Имитозащита на основе режима выработки имитовставки по ГОСТ 28147−89.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_10__

по дисциплине Криптографические методы защиты информации

1. Основные направления современного криптоанализа.
2. Организация криптосистем на основе канального и сквозного шифрования. Основные преимущества и недостатки обоих типов шифрования.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_11__

по дисциплине Криптографические методы защиты информации

1. Классификация методов криптографического преобразования информации.
2. Основные способы распределения ключей в симметричных криптосистемах, их преимущества и недостатки. Типовая схема распределения ключей, использующая центр распределения ключей.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко

(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_12__

по дисциплине Криптографические методы защиты информации

1. Основные методы статистического криптоанализа моноалфавитных шифров.
2. Схемы иерархического и децентрализованного управления ключами в симметричных криптосистемах.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_13__

по дисциплине Криптографические методы защиты информации

1. Шифр Плейфейера: алгоритм шифрования и дешифрования; основные достоинства и недостатки.

2. Шифраторы семейства "Криптон" и краткая характеристика их функциональных возможностей.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_14__

по дисциплине Криптографические методы защиты информации

1. Шифр Хилла: алгоритм шифрования и дешифрования; основные достоинства и недостатки.
2. Типы сеансовых ключей. Схема управления использованием ключей на основе управляющего вектора.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_15__

по дисциплине Криптографические методы защиты информации

1. Шифр Виженера: алгоритм шифрования и дешифрования; варианты формирования ключей; основные достоинства и недостатки.
2. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием авторитетного источника открытых ключей.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_16__

по дисциплине Криптографические методы защиты информации

1. Шифр Вернама: алгоритм шифрования и дешифрования; варианты формирования ключей; основные достоинства и недостатки.
2. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием сертификатов открытых ключей.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования

«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_17__

по дисциплине Криптографические методы защиты информации

1. Структурная схема и принцип действия роторной шифровальной машины.
2. Основные способы распределения секретных ключей с использованием криптосистемы с открытым ключом. Алгоритм распределения секретных ключей с обеспечением конфиденциальности и аутентификации.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_18__

по дисциплине Криптографические методы защиты информации

1. Основные виды перестановочных шифров; способы повышения их стойкости.
2. Структура и математическое обоснование алгоритма обмена ключами по схеме Диффи–Хеллмана.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_19__

по дисциплине Криптографические методы защиты информации

1. Определение блочного шифра. Общая схема блочного шифрования, особенности ее практического использования.
2. Определение хэш−функции. Краткая характеристика требований к хэш−функциям.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_20__

по дисциплине Криптографические методы защиты информации

1. Понятия идеального шифра, диффузии и конфузии. Примеры применения метода диффузии.
2. Простые функции хэширования: примеры и их краткий анализ.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_21__

по дисциплине Криптографические методы защиты информации

1. Структура шифра Файстеля.
2. Парадокс дня рождения и схема основанной на нем атаки.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_22__

по дисциплине Криптографические методы защиты информации

1. Анализ конструктивных элементов шифра Файстеля и краткая характеристика алгоритма его дешифрования.
2. Способы использования хэш−функций.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_23__

по дисциплине Криптографические методы защиты информации

1. Применение блочных шифров в режиме сцепления блоков шифрованного текста.
2. Криптоанализ итерированных функций хэширования.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_24__

по дисциплине Криптографические методы защиты информации

1. Применение блочных шифров в режиме электронной кодировочной книги.
2. Возможности цифровых подписей и требования к ним. Анализ преимуществ и недостатков непосредственной цифровой подписи.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_25__

по дисциплине Криптографические методы защиты информации

1. Применение блочных шифров в режиме обратной связи по шифрованному тексту.
2. Основные схемы организации арбитражной цифровой подписи.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_26__

по дисциплине Криптографические методы защиты информации

1. Применение блочных шифров в режиме обратной связи по выходу.
2. Организация цифровой подписи по схеме RSA. Анализ ее преимуществ и недостатков.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_27__

по дисциплине Криптографические методы защиты информации

1. Основные методы композиции шифров. Примеры композиций шифров.
2. Формирование цифровой подписи по алгоритму DSA.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования

«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_28__

по дисциплине Криптографические методы защиты информации

1. Основные требования к стандарту шифрования данных.
2. Верификация цифровой подписи по алгоритму DSA.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_29__

по дисциплине Криптографические методы защиты информации

1. Структура алгоритма DES. Анализ особенностей блоков начальной и заключительной перестановок.
2. Основные виды атак с использованием воспроизведения сообщений и способы защиты от них.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_30__

по дисциплине Криптографические методы защиты информации

1. Основные этапы преобразования ключей в алгоритме DES.
2. Примеры протоколов взаимной аутентификации на основе традиционного шифрования. Анализ их преимуществ и недостатков.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_31__

по дисциплине Криптографические методы защиты информации

1. Анализ структуры блока перестановки с расширением (Е–блока) в алгоритме DES и ее особенностей.
2. Области применения случайных чисел в криптографии. Требования к случайным числовым последовательностям. Физические источники случайных чисел.

Составитель _____Соколов С.В.

(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_32__

по дисциплине Криптографические методы защиты информации

1. Анализ структуры подстановки с помощью S–блоков в алгоритме DES и ее особенностей.
2. Требования к криптографически стойким генераторам псевдослучайных последовательностей и их криптообоснование. Примеры способов генерации псевдослучайных последовательностей.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_33__

по дисциплине Криптографические методы защиты информации

1. Анализ структуры перестановки с помощью P–блоков в алгоритме DES и структуры алгоритма его дешифрования.
2. Конгруэнтный способ генерации псевдослучайных последовательностей и анализ его параметров. Критерии качества генераторов псевдослучайных последовательностей.

Составитель _____ Соколов С.В.
(подпись)

Заведующий кафедрой _____ Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_34__

по дисциплине Криптографические методы защиты информации

1. Анализ структуры перестановки с помощью P–блоков в алгоритме DES и структуры алгоритма его дешифрования.
2. Конгруэнтный способ генерации псевдослучайных последовательностей и анализ его параметров. Критерии качества генераторов псевдослучайных последовательностей.

Составитель _____ Соколов С.В.
(подпись)

Заведующий кафедрой _____ Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_35__

по дисциплине Криптографические методы защиты информации

1. Принцип построения схемы шифрования с открытым ключом.
2. Криптографический генератор псевдослучайных последовательностей ANSI X9.17.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_36__

по дисциплине Криптографические методы защиты информации

1. Принцип построения схемы электронной цифровой подписи.
2. Криптографический генератор псевдослучайных последовательностей BBS.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_37__

по дисциплине Криптографические методы защиты информации

1. Принцип построения схемы аутентификации в криптосистемах с открытым ключом.
2. Классификация шифраторов и краткая характеристика их основных типов.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_38__

по дисциплине Криптографические методы защиты информации

1. Принцип построения схемы шифрования и аутентификации с открытым ключом.
2. Функциональные возможности аппаратных шифраторов. Типовая структурная схема аппаратного шифратора.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_39__

по дисциплине Криптографические методы защиты информации

1. Условия применения криптосистем с открытым ключом. Понятие односторонней функции.
2. Принцип действия аппаратного шифратора.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_40__

по дисциплине Криптографические методы защиты информации

1. Основные виды криптоатак на криптосистемы с открытым ключом.
2. Аппаратный шифратор "Шипка -1.5" и краткая характеристика его функциональных возможностей.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_41__

по дисциплине Криптографические методы защиты информации

1. Теоретическая стойкость криптосистемы. Необходимое и достаточное условие совершенной секретности шифра, анализ размерности совершенно секретного ключа.
2. Основные направления развития технологии смарт-карт (цифровых интеллектуальных карт).

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_42__

по дисциплине Криптографические методы защиты информации

1. Практическая стойкость криптосистемы и параметры, ее характеризующие.
2. Функциональные возможности и структура "проходного" шифратора.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_43__

по дисциплине Криптографические методы защиты информации

1. Классификация алгоритмов по степени их сложности.
2. Программное обеспечение "проходного" шифратора и его взаимодействие с программами компьютера.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_44__

по дисциплине Криптографические методы защиты информации

1. Сформулировать определения наибольшего общего делителя и взаимно простых чисел, основную теорему арифметики. Алгоритм Евклида.
2. Сравнительный анализ технических характеристик основных типов современных криптотелефонов.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_45__

по дисциплине Криптографические методы защиты информации

1. Сформулировать определения чисел, сравнимых по модулю; вычетов и классов вычетов. Свойства сравнений по модулю.
2. Примеры протоколов взаимной аутентификации на основе шифрования с открытым ключом. Анализ их преимуществ и недостатков.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_46__

по дисциплине Криптографические методы защиты информации

1. Функция Эйлера – общий случай, для простого числа, для произведения простых чисел. Формулировка теоремы Эйлера и следствие из нее как основа построения алгоритма RSA.

2. Протокол односторонней аутентификации на основе традиционного шифрования. Анализ его преимуществ и недостатков.

Составитель _____ Соколов С.В.
(подпись)

Заведующий кафедрой _____ Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_47__

по дисциплине Криптографические методы защиты информации

1. Сформулировать определение показателя, которому принадлежит число a по модулю n, и определения, ему эквивалентные; показать их численную реализацию.

2. Примеры протоколов односторонней аутентификации на основе шифрования с открытым ключом. Анализ их преимуществ и недостатков.

Составитель _____ Соколов С.В.
(подпись)

Заведующий кафедрой _____ Е.Н. Тищенко
(подпись)

«___»_____20 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра _Информационных технологий и защиты информации_

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_48__

по дисциплине Криптографические методы защиты информации

1. Сформулировать определение первообразного корня и свойства его степеней, определение дискретного логарифма (индекса числа b по модулю p при основании a), его свойства и особенности вычисления.
2. Методы вычислительной реализации процедуры формирования ключей в алгоритме RSA.

Составитель _____Соколов С.В.
(подпись)

Заведующий кафедрой _____Е.Н. Тищенко
(подпись)

«____»_____20 г.

Критерии оценивания:

- оценка «отлично» - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- оценка «хорошо» - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- оценка "удовлетворительно" - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- оценка "неудовлетворительно" - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Оформление лабораторных работ

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Лабораторные работы

по дисциплине Криптографические методы защиты информации
(наименование дисциплины)

Тематика лабораторных работ по разделам

Раздел 1 **Понятие о традиционных методах шифрования.**

Лабораторная работа 1 "Разработка криптосистемы на основе шифра Цезаря и системы взлома данного алгоритма". Изучение основных методов криптоанализа. Криптоанализ шифра Цезаря.

Лабораторная работа 2 "Разработка криптосистемы на основе традиционных алгоритмов с использованием классов в Net Framework". Классы традиционных алгоритмов в Net Framework. Анализ криптосистем на основе традиционных методов шифрования. Использование Net Framework.

Раздел 2 **Анализ и синтез симметричных криптосистем**.

Лабораторная работа 1 «Классы симметричных алгоритмов в Net Framework». Анализ криптосистем на основе симметричных алгоритмов. Анализ симметричных алгоритмов в Net Framework.

Лабораторная работа 2 "Разработка криптосистемы на основе симметричного алгоритма DES с использованием классов в Net Framework ". Анализ классов в Net Framework для криптосистемы на основе симметричного алгоритма DES. Использование Net Framework.

Раздел 3 **Криптосистемы с открытым ключом.**

Лабораторная работа 1 "Разработка криптосистемы на основе асимметричного алгоритма RSA с использованием классов в Net Framework". Анализ криптосистем на основе асимметричных алгоритмов. Использование Net Framework.

Лабораторная работа 2 «Классы асимметричных алгоритмов в Net Framework». Анализ асимметричных алгоритмов в Net Framework. Анализ

классов в Net Framework для криптосистемы на основе асимметричного алгоритма.

Лабораторная работа 3 "Разработка системы цифровой подписи на основе алгоритма DSA с использованием классов в Net Framework ". Анализ цифровой подписи на основе асимметричных алгоритмов. Использование Net Framework.

Лабораторная работа 4 «Классы для работы с цифровыми подписями в Net Framework». Анализ систем цифровой подписи в Net Framework. Анализ классов в Net Framework для систем цифровой подписи.

Раздел 4 **Имитостойкость и помехоустойчивость криптосистем. Криптографические шифраторы.**

Лабораторная работа 1 "Разработка системы хеширования на основе алгоритма MD5 с использованием классов в Net Framework ". Анализ системы хеширования на основе алгоритма MD5. Использование Net Framework.

Лабораторная работа 2 «Алгоритмы хэширования в Net Framework». Анализ классов в Net Framework для систем хеширования. Использование Net Framework.

2. Методические рекомендации по выполнению лабораторных работ

Лабораторная работа как вид учебного занятия проводиться в специально оборудованных учебных аудиториях.

Продолжительность не менее 2-х академических часов. Необходимыми структурными элементами лабораторной работы, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

Выполнению лабораторной работы предшествует проверка знаний студентов, их теоретической готовности к выполнению задания.

3. Критерии оценки:

- «зачтено» выставляется студенту, если задание, предусмотренное лабораторной работой, выполнено на компьютере и студент может объяснить ее выполнение;
- «незачтено» выставляется студенту, если задание, предусмотренное лабораторной работой, не выполнено на компьютере или он не может объяснить его выполнение.

4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 2. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры
Информационных технологий и защиты информации
Протокол №10 от «12» мая 2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.16.4 «Криптографические методы защиты информации»
(наименование дисциплины)

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль подготовки
10.03.01.02 «Организация и технология защиты информации»
(указывается код и наименование профиля подготовки)

Уровень образования
бакалавриат

Составитель _____ Соколов С.В., профессор, дтн, профессор
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Криптографические методы защиты информации» адресованы студентам всех форм обучения.

Учебным планом по направлению подготовки «Информационная безопасность» предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия и методы по данной дисциплине, даются рекомендации для самостоятельной работы и подготовки к лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач дисциплины.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом устного опроса, проверки выполненных индивидуальных заданий, проверки подготовленных конспектов по выделенным для самостоятельного изучения темам дисциплины. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников, выделить непонятные термины и найти их значение в энциклопедических словарях.

При реализации различных видов учебной работы используются разнообразные (в т.ч. интерактивные) методы обучения, в частности:

- размещение материалов курса в системе дистанционного обучения http://elearning.rsue.ru/ .

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ВУЗа: http://library.rsue.ru/ . Также обучающиеся могут взять на дом необходимую литературу на абонементе вузовской библиотеки или воспользоваться читальными залами вуза.