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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Методы и средства криптографической защиты информации

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2024 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Практические	32	32	32	32
Итого ауд.	96	96	96	96
Контактная работа	96	96	96	96
Сам. работа	12	12	12	12
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): д.э.н., профессор, декан, Тищенко Е.Н.

Зав. кафедрой: к.э.к., доц. Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	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.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

В результате освоения дисциплины обучающийся должен:
Знать:
Алгоритмы и методы криптографической и технической защиты информации для решения задач профессиональной деятельности (соотнесено с индикатором ОПК-9.1)
Уметь:
Настраивать и эксплуатировать алгоритмы и методы криптографической и технической защиты информации для решения задач профессиональной деятельности (соотнесено с индикатором ОПК-9.2)
Владеть:
Навыками конфигурирования алгоритмов и методов криптографической и технической защиты информации для решения задач профессиональной деятельности (соотнесено с индикатором ОПК-9.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Понятие о традиционных методах шифровании

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Введение. История развития криптографии. Основные понятия и определения / Лек /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.2	Моноалфавитные шифры. Полиалфавитные шифры. Роторные шифровальные машины / Лек /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.3	Разработка криптосистемы на основе шифра Цезаря и системы взлома данного алгоритма / Лаб /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.4	Разработка криптосистемы на основе традиционных алгоритмов с использованием классов / Пр /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
1.5	Криптоанализ традиционных алгоритмов / Ср /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

Раздел 2. Анализ и синтез симметричных криптосистем

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	История создания DES. Структура DES. Дешифрирование DES и режимы его использования. Аппаратная и программная реализация DES / Лек /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.2	Информационно - теоретический анализ криптографической стойкости. Анализ криптографической стойкости на основе теории сложности / Лек /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.3	Классы симметричных алгоритмов / Лаб /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.4	Разработка криптосистемы на основе симметричного алгоритма DES с использованием классов / Пр /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
2.5	Криптоанализ симметричных алгоритмов / Ср /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

Раздел 3. Криптосистемы с открытым ключом					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
3.1	Делители и простые числа. Арифметика в классах вычетов. Теорема Эйлера. Дискретные логарифмы. / Лек /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
3.2	Распределение открытых ключей. Распределение секретных ключей с использованием криптосистемы с открытым ключом / Лек /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
3.3	Требования к цифровым подписям и их классификация. Основные алгоритмы цифровых подписей / Лек /	6	4	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
3.4	Разработка криптосистемы на основе асимметричного алгоритма RSA с использованием классов / Лаб /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
3.5	Классы асимметричных алгоритмов / Пр /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
3.6	Разработка системы цифровой подписи на основе алгоритма DSA с использованием классов / Лаб /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
3.7	Классы для работы с цифровыми подписями / Пр /	6	6	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
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	2	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
Раздел 4. Имитостойкость и помехоустойчивость криптосистем. Криптографические шифраторы					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
4.1	Понятие помехоустойчивости криптосистем. Структура имитозащищенного помехоустойчивого канала связи. Имитозащита на основе режима выработки имитовставки / Лек /	6	2	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
4.2	Функциональные возможности и структура а аппаратного шифратора. Принцип действия аппаратного шифратора. Основные типы современных шифраторов. Основные направления развития технологии смарт-карт / Лек /	6	2	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
4.3	Разработка системы хеширования на основе алгоритма MD5 с использованием классов / Лаб /	6	8	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
4.4	Алгоритмы кэширования / Пр /	6	8	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
4.5	Средства и способы обеспечения помехоустойчивости информации. Способы имитозашиты вычислительных систем. Структура и программное обеспечение проходных шифраторов. Криптозащита информации при ее передаче по каналам специальной связи / Ср /	6	2	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3
4.6	/ Зачёт /	6	0	ОПК-9	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Масленников М.	Практическая криптография	Санкт-Петербург: БХВ-Петербург, 2015	https://ibooks.ru/reading.php?short=1&productid=335092 неограниченный доступ для зарегистрированных пользователей
Л1.2	Фороузан, Б. А., Берлина, А. Н.	Криптография и безопасность сетей: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021	https://www.iprbookshop.ru/102017.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2014	https://biblioclub.ru/index.php?page=book&id=238446 неограниченный доступ для зарегистрированных пользователей
Л2.2	Грибунин, В. Г., Мартынов, А. П., Николаев, Д. Б., Фомченко, В. Н., Астайкин, А. И.	Криптография и безопасность цифровых систем: учебное пособие	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011	https://www.iprbookshop.ru/60851.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Гисин В. Б.	Криптография и распределенные реестры: учебное пособие	Москва: Прометей, 2022	https://biblioclub.ru/index.php?page=book&id=700941 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Информационная справочная правовая система "Консультант Плюс"
Информационная справочная правовая система "Гарант" https://internet.garant.ru

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
Офисный пакет LibreOffice (кроссплатформенное свободно распространяемое программное обеспечение)

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);

- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности			
Знать алгоритмы и методы криптографической и технической защиты информации для решения задач профессиональной деятельности	Описывает способы решения стандартных задач профессиональной деятельности в области криптографической защиты при формировании системы защиты информации при ответе на вопросы	Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное	Опрос (вопросы 1-23) Вопросы к зачету (вопросы 1-96)
Уметь настраивать и эксплуатировать алгоритмы и методы криптографической и технической защиты информации для решения задач профессиональной деятельности	Анализирует состояние системы криптографической защиты информации, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного и практического задания	Полнота и правильность решения практико-ориентированного задания или практического задания	Лабораторные работы (работы 1-4) Практические задания (задания 1-4) Практико-ориентированные задания к зачету (задания 1-9)
Владеть навыками конфигурирования алгоритмов и методов криптографической и технической защиты информации для решения задач профессиональной деятельности	Использует методы и средства криптографической защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного и практического задания	Обоснованность и правильность обращения к нормативным источникам, методам и средствам при выполнении практико-ориентированного и практического задания	Лабораторные работы (работы 1-4) Практические задания (задания 1-4) Практико-ориентированные задания к зачету (задания 1-9)

1.2 Шкалы оценивания:

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

50-100 баллов (зачтено)

0-49 баллов (не зачтено)

2 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

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.

Практико-ориентированные задания к зачету

1. Разработка концепции, программы и плана исследования.
2. Выбор метода исследования на различных этапах работы.
3. Получение первичной информации об объекте исследования с использованием инструментальных методов.
4. Обработка первичной информации об объекте исследования.
5. Разработка модели криптографической системы электронного документооборота
6. Разработка модели атаки на криптографическую защиту системы электронного документооборота
7. Разработка комплекта типовых эксплуатационных документов системы электронного документооборота
8. Подбор и обоснование выбора средств криптографической защиты информации и их компонентов.
9. Проведение аудита защищенности системы электронного документооборота по требованиям контролирующих органов

Зачетное задание включает 2 теоретических вопроса (раздел «Вопросы к зачету») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к зачету»).

Критерии оценивания:
Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:
- 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
- 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
- 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
- 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:
- 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
- 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
- 11-24 балла выставляется, если задание решено частично.
- 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:
- 50-100 баллов (зачтено);
- 0-49 баллов (не зачтено).

Опрос

Вопросы для опроса:
1. Определение криптографии.
2. Функции криптографии.
3. Понятие криптографической системы, ключа криптографической системы, криптостойкости, криптографа, криптоаналитика.
4. Простейшие криптографические преобразования.
5. Функция Шеннона.
6. Функция циклического сдвига.
7. Блочные криптоалгоритмы.
8. Блочные криптоалгоритмы с обратной связью.
9. Понятие одноразового блокнота. Области его применения.
10. Классы криптосистем.
11. Основные характеристики и особенности классов криптосистем. Области применения.
12. Основные свойства симметричных криптоалгоритмов.

13. Структура алгоритмов семейства DES и алгоритма ГОСТ 28147-89.
14. Процедуры управления ключами в симметричных криптосистемах. Основные характеристики каждой из процедур.
15. Понятие однонаправленной функции.
16. Схема Диффыи-Хеллмана.
17. Основные свойства асимметричных криптоалгоритмов.
18. Понятие однонаправленной функции с черным входом.
19. Структура алгоритма RSA.
20. Понятие, структура и алгоритм реализации электронной подписи.
21. Определение и классификация хэш-функций.
22. Алгоритмы FIPS PUB 113-1985 (MAC), ГОСТ 28147-89.
23. Уровни раскрытия схем цифровой подписи.

Критерии оценивания*:*
Максимальное количество баллов, которые обучающийся может набрать – 20 баллов (за 20 ответов).
Ответ на вопрос оценивается:

- 1 балл – правильный и полный ответ;
- 0 баллов – неправильный ответ или ответ не представлен.

Лабораторные работы

Лабораторная работа 1.
Программная разработка криптосистемы на основе шифра Цезаря и системы взлома данного алгоритма.

Лабораторная работа 2
Программная разработка симметричной криптосистемы.

Лабораторная работа 3.
Программная разработка криптосистемы на основе асимметричного алгоритма RSA.

Лабораторная работа 4.
Программная разработка системы цифровой подписи на основе алгоритма DSA.

Критерии оценивания:
Максимальное количество баллов, которые обучающийся может набрать – 40 баллов (за 4 лабораторные работы).
Каждое задание оценивается:

- 10 баллов. – задание выполнено верно;
- 9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 6-3 баллов. – при выполнении задания были допущены ошибки;
- 2- 1 баллов. – при выполнении задания были допущены существенные ошибки;
- 0 баллов. – задание не выполнено.

Практические задания

Задание 1.
Разработка криптосистемы на основе традиционных алгоритмов с использованием классов.

Задание 2
Разработка криптосистемы на основе симметричного алгоритма DES с использованием классов.

Задание 3.
Анализ классов асимметричных алгоритмов.

Задание 4.
Анализ классов для работы с цифровыми подписями

Критерии оценивания:
Максимальное количество баллов, которые обучающийся может набрать – 40 баллов (за 4 заданий).
Каждое задание оценивается:
- 10 баллов. – задание выполнено верно;
- 9-7 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 6-3 баллов. – при выполнении задания были допущены ошибки;
- 2- 1 баллов. – при выполнении задания были допущены существенные ошибки;
- 0 баллов. – задание не выполнено.

3 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. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные работы;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области криптографической защиты информации, методы криптографии и криптоанализа, даются рекомендации для самостоятельной работы и подготовки к лабораторным работам и практическим занятиям.

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

При подготовке к лабораторным работам и практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной или практической работы;
- подготовить ответы на контрольные вопросы по изучаемой теме.

В процессе подготовки к лабораторным работам и практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях, лабораторных работах и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. 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.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.