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

УТВЕРЖДАЮ
Директор Института магистратуры
_____ Иванова Е.А.
«29» 08 2022 г.

Рабочая программа дисциплины
Криптографические протоколы

Направление 10.04.01 Информационная безопасность
магистерская программа 10.04.01.02 "Программно-аппаратные методы расследования компьютерных преступлений"

Для набора 2022 года

Квалификация
магистр

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	10	10	10	10
Лабораторные	10	10	10	10
Практические	10	10	10	10
Итого ауд.	30	30	30	30
Контактная работа	30	30	30	30
Сам. работа	105	105	105	105
Часы на контроль	9	9	9	9
Итого	144	144	144	144

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 22.02.2022 протокол № 7.

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

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. _____

Методическим советом направления: д.э.н., проф., Тищенко Е.Н. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением криптографической защиты информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-1:Способен разрабатывать программно-аппаратные системы и комплексы обеспечения информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

криптографические протоколы, типы и виды шифрующих преобразований; существующие методы и средства, применяемые для криптографической защиты информации; системные вопросы криптографической защиты информации; симметричный способ шифрования.(соотнесено с индикатором ПК-1.1)

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.(соотнесено с индикатором ПК-1.2)

Владеть:

навыками применения криптографических протоколов(соотнесено с индикатором ПК-1.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Традиционные и классические методы шифрования				
1.1	Тема 1 "Введение в криптографию". Введение. История развития криптографии. Основные понятия и определения. /Лек/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
1.2	Тема 1 "Введение в криптографию". Программная реализация шифра замены. Разработка ПО шифра замены. Дешифрация шифротекста. Частотный криптоанализ с использованием LibreOffice /Лаб/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
1.3	Тема 1 "Введение в криптографию". Программная реализация шифра замены. Разработка ПО шифра замены. Дешифрация шифротекста. Частотный криптоанализ с использованием LibreOffice /Пр/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.4	Тема 1 "Введение в криптографию". История криптографии. Этапы развития криптологии и ее основные понятия и определения. Роль математики в развитии методов защиты информации. Смежные области криптографии. Основная классификация криптосистем. /Ср/	1	10	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.5	Тема 2 "Понятие о традиционных методах шифрования". Модель традиционного шифрования. Требования к криптографическим системам. Краткие сведения о криптоанализе. Классификация методов криптографического закрытия информации. /Лек/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.6	Тема 2 "Понятие о традиционных методах шифрования". Генерирование и тестирование псевдослучайных шифрующих последовательностей. Программная реализация генератора М- последовательности на основе полинома обратной связи. Тестирование М-последовательности длиной N бит ($N \leq 10000$) с помощью сериального теста. Тестирование М-последовательности с помощью корреляционного теста. Тестирование исходного и зашифрованного файла с помощью статистических тестов. /Лаб/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

1.7	Тема 2 "Понятие о традиционных методах шифрования". Криптоанализ традиционных алгоритмов. Коэффициент автокорреляции. Критерий x^2. Свойства шифрующей ключевой последовательности. М-последовательность. /Ср/	1	6	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
1.8	Тема 3 "Классические методы шифрования". Моноалфавитные шифры. Полиалфавитные шифры. Роторные шифровальные машины. Методы перестановки. Блочные шифры. Режимы применения блочных шифров. Композиции (комбинации) шифров. /Лек/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.9	Тема 3 "Классические методы шифрования". Шифр Виженера. Получение навыков создания зашифрованного сообщения при помощи алгоритма шифрования Виженера. /Лаб/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
1.10	Тема 3 "Классические методы шифрования". Алгоритм Цезаря. Секретная система "Рубикон“. Схема поблочной подстановки n-битовых блоков. Шифр Файстеля. Шифр Плейфейера. Шифр Хилла. /Ср/	1	6	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
1.11	Тема 4 "Стандарт шифрования данных DES (Data Encryption Standard)". История создания стандарта. Структура DES. Дешифрование DES. Режимы DES. Аппаратные и программные реализации DES /Лек/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
1.12	Тема 4 "Стандарт шифрования данных DES (Data Encryption Standard)". Алгоритм шифрования DES. Функция шифрования f для алгоритма DES. Формирование подключей для алгоритма DES. /Лаб/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.13	Тема 4 "Стандарт шифрования данных DES (Data Encryption Standard)". Схема алгоритма. Начальная перестановка. Преобразования ключа. Перестановка с расширением. Подстановка с помощью S-блоков. Перестановка с помощью P-блоков. Заключительная перестановка. Дешифрование DES. /Ср/	1	6	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
	Раздел 2. Асимметричное шифрование				
2.1	Тема 1 "Криптосистемы с открытым ключом". Общая схема шифрования с открытым ключом. Электронная цифровая подпись и аутентификация в криптосистемах с открытым ключом. Особенности применения криптосистем с открытым ключом. Криптоанализ систем с открытым ключом. /Ср/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.2	Тема 1 "Криптосистемы с открытым ключом". Изучение принципов работы асимметричных алгоритмов шифрования с открытым ключом. Методика создания комбинированных алгоритмов шифрования, совмещающая достоинства методов симметричной и асимметричной криптографии. /Лаб/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.3	Тема 1 "Криптосистемы с открытым ключом". Проблемы традиционного шифрования. Аутентификация с использованием открытого ключа. Криптосистема с открытым ключом: защита и аутентификация. /Пр/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.4	Тема 2 "Основные понятия теории чисел". Делители и простые числа. Арифметика в классах вычетов. Теорема Эйлера. Дискретные логарифмы. /Лек/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
2.5	Тема 2 "Основные понятия теории чисел". Алгоритм Евклида. Создание в MS Excel «машину» для автоматического вычисления НОД двух чисел по алгоритму Евклида. /Ср/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

2.6	Тема 2 "Основные понятия теории чисел". Арифметика в классах вычетов. Алгоритм Евклида. Дискретные логарифмы. /Пр/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.7	Тема 3 "Алгоритм шифрования RSA". Структура алгоритма RSA. Вычислительная реализация алгоритма RSA. Криптоанализ алгоритма RSA. /Ср/	1	12	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
2.8	Тема 3 "Алгоритм шифрования RSA". Асимметричный алгоритм шифрования RSA. Вычисление ключей. Шифрование с помощью этих ключей. Дешифрование. /Ср/	1	12	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
2.9	Тема 3 "Алгоритм шифрования RSA". Схема Райвеста-Шамира-Адлемана (RSA). Компоненты схемы RSA. Шифрование и дешифрование. /Пр/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.10	Тема 4 "Управление ключами в асимметричных криптосистемах". Распределение открытых ключей. Распределение секретных ключей с использованием криптосистемы с открытым ключом. /Ср/	1	12	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.11	Тема 4 "Управление ключами в асимметричных криптосистемах". Асимметричные криптосистемы. Исследование основных характеристик алгоритма шифрования. /Ср/	1	12	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.12	Тема 4 "Управление ключами в асимметричных криптосистемах". Методы распределения открытых ключей. Сертификаты открытых ключей. Распределение секретных ключей с помощью системы с открытым ключом. /Ср/	1	12	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.13	Тема 5 "Электронная цифровая подпись". Требования к цифровым подписям и их классификация. Основные алгоритмы цифровых подписей. /Пр/	1	2	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.3 Л2.4 Л2.5
2.14	Тема 5 "Электронная цифровая подпись". Электронная цифровая подпись Эль-Гамаля. Исследование процесса построения электронной подписи Эль-Гамаля. /Ср/	1	5	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.15	Тема 5 "Электронная цифровая подпись". Непосредственная цифровая подпись. Арбитражная цифровая подпись. Электронная цифровая подпись (ЭЦП) Эль-Гамаля. Электронная цифровая подптсь Шнорра. Стандарт ЭЦП DSS. /Ср/	1	8	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.16	/Экзамен/	1	9	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

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, 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/index.php?page=book&id=238045 неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.3	Котов, Ю. А.	Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017	http://www.iprbookshop.ru/91227.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Котов, Ю. А.	Криптографические методы защиты информации. Шифры: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016	http://www.iprbookshop.ru/91377.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2012	https://biblioclub.ru/index.php?page=book&id=211299 неограниченный доступ для зарегистрированных пользователей
Л2.2		Криптографические методы защиты информации: лабораторный практикум: практикум	Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015	https://biblioclub.ru/index.php?page=book&id=458059 неограниченный доступ для зарегистрированных пользователей
Л2.3	Альбов А. С.	Квантовая криптография	Санкт-Петербург: Страта, 2015	http://biblioclub.ru/index.php?page=book&id=477631 неограниченный доступ для зарегистрированных пользователей
Л2.4	Смирнов, А. Э., Пономарёва, Ю. А.	Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации	Москва: Московский технический университет связи и информатики, 2015	http://www.iprbookshop.ru/61738.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Шелухин, О. И.	Учебно-методическое пособие по выполнению курсовой работы по дисциплине Криптографические методы защиты информации	Москва: Московский технический университет связи и информатики, 2015	http://www.iprbookshop.ru/63335.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант+

ЭБС «IPR Books» http://www.iprbookshop.ru/

Библиоклуб.ру http://biblioclub.ru/

5.4. Перечень программного обеспечения

LibreOffice

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 (МОДУЛЯ)

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/или свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
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
ПК-1 - способен разрабатывать программно-аппаратные системы и комплексы обеспечения информационной безопасности			
криптографические ротоколы, типы и виды ифрующих реобразований; уществующие методы и редства, применяемые ля криптографической ащиты информации; истемные вопросы риптографической ащиты информации; имметричный способ ифрования.(соотнесено индикатором ПК-1.1)	знает основные понятия криптологии, типы и виды шифрующих преобразований; методы и средства, применяемые для криптографической защиты информации; симметричный способ шифрования при подготовке ответов к теста и зачету	сформировавшееся систематическое знание основных понятий криптологии, типов и видов шифрующих преобразований; методов и средств, применяемых для криптографической защиты информации; симметричного способа шифрования при ответе на вопросы теста и зачета	Т (Раздел 1 тема Э вопрос 1-3; Раздел 2 тема 2 вопрос 1-3, тема 5 вопрос 1-3),
: проводить анализ нформации с целью ыработки и принятия ешений и мер по беспечению риптографической ащиты информации и ффективному спользованию средств бнаружения озможных каналов злома шифртекстов, редставляющих осударственную, оенную, служебную и оммерческую айну.(соотнесено с ндикатором ПК-1.2)	анализирует информацию 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 при выполнении лабораторных и практико-ориентированных заданий	сформированные умения анализа 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 при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (Раздел 1 ЛЗ4); ПОЗЗ (1-5)

: навыками рименения риптографических ротоколов(соотнесен с индикатором ПК-3)	анализирует действующие нормативные и методические документы по КЗИ при выполнении лабораторных и практико-ориентированных заданий	сформировавшееся систематическое владение навыками анализа действующих нормативных и методических документов по КЗИ при выполнении лабораторных и практико-ориентированных заданий	ЛЗ (Раздел 2 ЛЗ5); ПОЗЗ (1-5)

Т – тест, ЛЗ – лабораторные задания, ПОЗЗ - практико-ориентированные задания к зачету, Э – *вопросы к экзамену*

1.2 Шкалы оценивания:

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

84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

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 экзамену

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 Виженера: алгоритм шифрования и дешифрования; варианты

формирования ключей; основные достоинства и недостатки.

14. Структурная схема и принцип действия роторной шифровальной машины.

15. Основные виды перестановочных шифров; способы повышения их стойкости.

16. Определение блочного шифра. Общая схема блочного шифрования, особенности ее практического использования.

17. Понятия идеального шифра, диффузии и конфузии. Примеры применения метода диффузии.

18. Применение блочных шифров в режиме электронной кодировочной книги.

19. Применение блочных шифров в режиме сцепления блоков шифрованного текста.

20. Применение блочных шифров в режиме обратной связи по шифрованному тексту.

21. Применение блочных шифров в режиме обратной связи по выходу.

22. Основные методы композиции шифров. Примеры композиций шифров.

23. Основные требования к стандарту шифрования данных.

24. Структура алгоритма DES. Анализ особенностей блоков начальной и заключительной перестановок.

25. Основные этапы преобразования ключей в алгоритме DES.

26. Анализ структуры блока перестановки с расширением (E−блока) в алгоритме DES и ее особенностей.

27. Анализ структуры подстановки с помощью S−блоков в алгоритме DES и ее особенностей.

28. Анализ структуры перестановки с помощью P−блоков в алгоритме DES и структуры алгоритма его дешифрования.

29. Теоретическая стойкость криптосистемы. Необходимое и достаточное условие совершенной секретности шифра, анализ размерности совершенно секретного ключа.

30. Практическая стойкость криптосистемы и параметры, ее характеризующие.

31. Классификация алгоритмов по степени их сложности.

32. Принцип построения схемы шифрования с открытым ключом.

33. Принцип построения схемы электронной цифровой подписи.

34. Принцип построения схемы аутентификации в криптосистемах с открытым ключом.

35. Принцип построения схемы шифрования и аутентификации с открытым ключом.

36. Условия применения криптосистем с открытым ключом. Понятие односторонней функции.

37. Основные виды криптоатак на криптосистемы с открытым ключом.

38. Сформулировать определения наибольшего общего делителя и взаимно простых чисел, основную теорему арифметики. Алгоритм Евклида.

39. Сформулировать определения чисел, сравнимых по модулю, вычетов и классов вычетов. Свойства сравнений по модулю.

40. Функция Эйлера − общий случай, для простого числа, для произведения простых чисел. Формулировка теоремы Эйлера и следствие из

нее как основа построения алгоритма RSA.

41. Структура алгоритма шифрования RSA. Условия его работоспособности и их теоретическое обоснование.

42. Схема формирования ключей в алгоритме RSA.

43. Методы вычислительной реализации процедуры шифрования / дешифрования в алгоритме RSA.

44. Методы вычислительной реализации процедуры формирования ключей в алгоритме RSA.

45. Основные направления и методы криптоанализа алгоритма RSA.

46. Методы повышения криптостойкости алгоритма RSA.

47. Схемы иерархического и децентрализованного управления ключами в симметричных криптосистемах.

48. Типы сеансовых ключей. Схема управления использованием ключей на основе управляющего вектора.

49. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием авторитетного источника открытых ключей.

50. Основные способы распределения открытых ключей. Алгоритм распределения открытых ключей с использованием сертификатов открытых ключей.

51. Возможности цифровых подписей и требования к ним. Анализ преимуществ и недостатков непосредственной цифровой подписи.

52. Основные схемы организации арбитражной цифровой подписи.

53. Организация цифровой подписи по схеме RSA. Анализ ее преимуществ и недостатков.

54. Формирование цифровой подписи по алгоритму DSA.

55. Примеры протоколов взаимной аутентификации на основе традиционного шифрования. Анализ их преимуществ и недостатков.

56. Примеры протоколов взаимной аутентификации на основе шифрования с открытым ключом. Анализ их преимуществ и недостатков.

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

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

Типовые практико-ориентированные задания к зачету

Задание 1. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ЯБЛОКО – ЗЙФЧУЧ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Задание 2. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ГРУША – ЮЛОУЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Задание 3. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ВИНОГРАД – ШЯДЕЩЖЦЪ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Задание 4. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: АБРИКОС – ЛМЬФЦЪЭ

(исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Задание 5. Расшифруйте сообщение ЖКИЛШЪОБМ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ. Ответ запишите заглавными русскими буквами без пробелов

Ключи для проверки правильности выполнения практико-ориентированного задания

Задание 1. 23
Задание 2. 28
Задание 3. 12
Задание 4. 16
Задание 5. Компьютер

Критерии оценивания:

- 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; усвоена основная литература, рекомендованная в рабочей программе дисциплины;
- 50-66 баллов (оценка «удовлетворительно») - наличие основных знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, исправленными после дополнительных вопросов; выполняются в целом корректные действия по применению знаний на практике;
- 0-49 баллов (оценка «неудовлетворительно») - ответы не связаны с вопросами, наличие грубых ошибок в ответе, демонстрирующие непонимание сущности излагаемого вопроса и неумение применять знания на практике; отсутствие уверенности и неточность ответов на дополнительные и наводящие вопросы.

Пример теста

1. Банк тестов по модулям и (или) темам

Раздел 1 «Традиционные и классические методы шифрования»

Тема 1 " **Введение в криптографию** "

1. Что в переводе с греческого языка означает слово «криптография»?
   1) шифр
   2) тайнопись
   3) преобразование
   4) расшифровка
2. Когда в криптографии стало использоваться асимметричное шифрование?
   1) в первой половине XIX
   2) во второй половине XIX
   3) в первой половине XX.
   4) во второй половине XX
3. Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?
   1) алгоритм
   2) ключ
   3) протокол
   4) шифр

Тема 2 «**Понятие о традиционных методах шифрования**».

1. Шифрование – это…
   1) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого.
   2) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
   3) удобная среда для вычисления конечного пользователя

2. Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?
   1) алгоритм
   2) ключ
   3) протокол
   4) шифр

3. Как называется сообщение, полученное после преобразования с использованием любого шифра?
   1) закрытым текстом
   2) имитовставкой
   3) ключом
   4) открытым текстом

Тема 3. «**Классические методы шифрования**».

1. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?
   1) шифр Маркова
   2) шифр Цезаря
   3) шифр Энигма
   4) шифр Бэбиджа

2. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования
   1) 1
   2) 2
   3) 3

3. Из скольки последовательностей состоит расшифровка текста по таблице Вижинера
   1) 3
   2) 4
   3) 5

Тема 4. «**Стандарт шифрования данных DES (Data Encryption Standard)».**

1.Для чего использовался DES-алгоритм из-за небольшого размер ключа
   1) закрытия коммерческой информации
   2) шифрования секретной информации
   3) нет правильного ответа

2.Основные области применения DES-алгоритма
   1) хранение данных на компьютере
   2) электронная система платежей
   3) аутентификация сообщений

3.Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма
   1) отсутствием начальной перестановки и числом циклов шифрования

2) длиной ключа
3) методом шифрования

Раздел 2 «**Асимметричное шифрование»**
Тема 1 «**Криптосистемы с открытым ключом»**
1. Как связаны ключи друг с другом в системе с открытым ключом
1) математически
2) логически
3) алгоритмически
2. Какие ключи используются в системах с открытым ключом
1) открытый
2) закрытый
3) нет правильного ответа
3. Сколь ключей используется в системах с открытым ключом
1) 2
2) 3
3) 1

Тема 2 «**Основные понятия теории чисел»**
1.Какой остаток от деления на 5 имеет число $2437 \times 578 - 1035 \times 4733457$?
1) 4
2) 3
3) 1
4) 2
5) 0
2.Найти остаток при делении на 9 числа 65 $6k$, $k \in N$
1) 7
2) 3
3) 6
4) 1
5) 2
3.Решениями сравнения $339x \equiv 452(\mathrm{mod}7)$ являются классы:
1) 6
2) 5
3) 10
4) 2
5) 4

Тема 3. **«Алгоритм шифрования RSA».**
1.Верны ли утверждения?
А) Алгоритм шифрования RSA является первым алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи.
В) Надежность алгоритма шифрования RSA основывается на трудности факторизации больших чисел и вычисления дискретных логарифмов в конечном поле.
Подберите правильный ответ.
1) А – да, В – да
2) А – да, В – нет
3) А – нет, В – нет

4) А – нет, В – да

2.Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA Пользователь Б имеет следующие параметры: P=7, Q=11, d=47. Вычислите значение с зашифрованного сообщения.

1) c=53
2) c=54
3) c=55
4) c=56

3. Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA Пользователь Б имеет следующие параметры: P=11, Q=17, d=71. Вычислите значение с зашифрованного сообщения.

1) c=173
2) c=175
3) c=155
4) c=153

Тема 4. «**Управление ключами в асимметричных криптосистемах».**

1.Блок управления – это…

1) аппаратно реализованная программа, управляющая вычислителем
2) язык описания данных
3) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

2. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:

1) оно обеспечивает проверку целостности и правильности данных
2) оно требует внимательного отношения к процессу управления ключами
3) оно не требует большого количества системных ресурсов
4) оно требует передачи ключа на хранение третьей стороне

3. Гарантирование невозможности несанкционированного изменения информации - это:

1) обеспечение целостности
2) обеспечение конфиденциальности
3) обеспечение аутентификации
4) обеспечение шифрования

Тема 5. **«Электронная цифровая подпись».**

1.Электронной подписью называется…

1) присоединяемое к тексту его криптографическое преобразование
2) текст
3) зашифрованный текст

2.Какие функции выполняет ЭЦП?

1) помогает гарантировать, что поставивший подпись — тот, кем он является в действительности
2) помогает гарантировать, что содержимое документа не менялось и не подделывалось после ввода цифровой подписи
3) помогает доказать любой из сторон авторство подписанного содержимого;
4) все функции, перечисленные выше.

3.Какая информация хранится в ЭЦП?

1) имя файла закрытого ключа подписи;
2) только информация о лице, сформировавшем подпись;

3) дата формирования подписи, информация о лице, сформировавшем подпись и имя файла открытого ключа подписи.

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его взгляд, варианта ответа. Тестовое задание содержит 20 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается. Время прохождения тестирования 20 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

Критерии оценки:

Максимальное количество баллов – 10 баллов.

- 1-10 баллов выставляется обучаемому в зависимости от правильного ответа на вопросы теста. За один правильный ответ обучаемый получает 0,5 балла.

Лабораторные задания

Раздел 1 **Традиционные и классические методы шифрования**

Тема 1 **«Введение в криптографию»**

Лабораторное работа 1 **«Программная реализация шифра замены».** Разработка ПО шифра замены. Дешифрация шифротекста. Частотный криптоанализ.

Тема 2 **«Понятие о традиционных методах шифрования»**

Лабораторная работа 2 **«Генерирование и тестирование псевдослучайных шифрующих последовательностей».** Программная реализация генератора М-последовательности на основе полинома обратной связи. Тестирование М-последовательности длиной N бит ($N \leq 10000$) с помощью сериального теста. Тестирование М-последовательности с помощью корреляционного теста. Тестирование исходного и зашифрованного файла с помощью статистических тестов.

Тема 3 **«Классические методы шифрования».**

Лабораторная работа 3 **«Шифр Виженера».** Получение навыков создания зашифрованного сообщения при помощи алгоритма шифрования Виженера.

Тема 4. «**Стандарт шифрования данных DES (Data Encryption Standard)».**

Лабораторная работа 4 «**Алгоритм шифрования DES».** Функция шифрования f для алгоритма DES. Формирование подключей для алгоритма DES.

Раздел 2 **Асимметричное шифрование**

Тема 1 «**Криптосистемы с открытым ключом»**

Лабораторная работа 1 **«Изучение принципов работы асимметричных алгоритмов шифрования с открытым ключом».** Методика создания комбинированных алгоритмов шифрования, совмещающая достоинства методов симметричной и асимметричной криптографии.

Тема 2 «**Основные понятия теории чисел»**

Лабораторная работа 2 **«Алгоритм Евклида».** Создание в MS Excel «машину» для автоматического вычисления НОД двух чисел по алгоритму Евклида.

Тема 3. **«Алгоритм шифрования RSA».**

Лабораторная работа 3 **«Асимметричный алгоритм шифрования RSA».** Вычисление ключей. Шифрование с помощью этих ключей. Дешифрование.

Тема 4. «**Управление ключами в асимметричных криптосистемах».**

Лабораторная работа 4 «**Асимметричные криптосистемы».** Исследование основных характеристик алгоритма шифрования.

Тема 5. **«Электронная цифровая подпись».**

Лабораторная работа 5. **«Электронная цифровая подпись Эль-Гамаля».** Исследование процесса построения электронной подписи Эль-Гамаля.

Критерии оценки:

Максимальное количество баллов – 90 баллов.

(для каждого задания)

10 б. – задание выполнено верно;

9-8 б. – при выполнении задания были допущены неточности, не влияющие на результат;

7-5 б. – при выполнении задания были допущены ошибки;

4-1 б. – при выполнении задания были допущены существенные ошибки.

0 б. – 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.

Экзамен проводится по расписанию промежуточной аттестации.

Количество вопросов – 3 (2 –теоретических вопроса и одно практико-ориентированное задание).

Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются криптографические методы защиты информации, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки применения криптографических протоколов.

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме.

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

Вопросы, не рассмотренные на лекциях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий. 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 первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лабораторному занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

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.