Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 10.04.01. «Информационная безопасность»

Профиль: «Безопасность автоматизированных систем»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2023

Смоленск

Направление подготовки 10.04.01 «Информационная безопасность»
Магистерская программа «Безопасность автоматизированных систем»
Методическое обеспечение для РПД Б1.В.06
«Криптографические методы и средства защиты информации»

Методические материалы составил:

_____ к.т.н., доцент А.В. Полячков
подпись ФИО

«20» января 2023 г.

Заведующий кафедрой «Вычислительной техники»:

_____ д.т.н., профессор А.С. Федулов
подпись ФИО

«26» января 2023 г.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 3										Семестр 4										Итого за курс										Каф.	Семестр
			Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель		
				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль	Всего			
1	Б1.В.06	Криптографические методы и средства защиты информации	Эк КР	**216**	104	34	34	18	18	76	36	6													Эк КР	**216**	104	34	34	18	18	76	36	6		15	3

ОБОЗНАЧЕНИЯ:
Виды промежуточной аттестации (виды контроля):
Экз - экзамен;
ЗаО - зачет с оценкой;
За – зачет.

Виды работ:
Контакт. – контактная работа обучающихся с преподавателем;
Лек. – лекционные занятия;
Лаб.– лабораторные работы;
Пр. – практические занятия;
КРП – курсовая работа (курсовой проект);
РГР – расчетно-графическая работа (реферат);
СР – самостоятельная работа студентов;
з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	**Лекционные занятия** - 17 шт. по 2 часа. **Тема 1. Введение в криптографию.** 1.1. Введение в криптографию (2 часа). Основные определения. История криптографии. Классификация криптоалгоритмов. **Тема 2. Математические основы криптографии.** 1.2. Модульная арифметика и алгебраические структуры (2 часа) Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Алгебраические структуры. Поля Галуа. 1.3. Генерация и тестирование псевдослучайных последовательностей (2 часа). Структура генератора псевдослучайных последовательностей (ГПСП). Алгоритмы генерации псевдослучайных последовательностей Криптографические стойкие ГПСП. Тестирование ГПСП. **Тема 3. Симметричная криптография.** 1.4. Современные блочные шифры (2 часа). Стандарт шифрования DES. Режимы работы алгоритма DES. Стандарт шифрования AES. 1.5 Российский стандарт шифрования (2 часа). Стандарт шифрования ГОСТ Р 34. 12-2015 (Магма и Кузнечик) 1.6. Современные шифры потока (2 часа). Шифр одноразового блокнота. Принцип использования ГПСП при поточном шифровании. Шифр RC4. 1.7. Шифрование, использующее современные шифры с симметричным ключом (2 часа). Применение современных блочных шифров. Использование шифров потока. Методы повышения криптостойкости симметричных криптосистем. **Тема 4. Асимметричная криптография**. 1.8. Криптосистема RSA (2 часа). Принцип работы современных асимметричных криптосистем. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина. 1.9. Криптосистемы на основе метода эллиптических кривых (2 часа). Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа, криптография эллиптической кривой, моделирующая криптосистему Эль-Гамаля **Тема 5. Целостность и установление подлинности.** 1.10. Обеспечение целостности передаваемых данных (2 часа). Целостность сообщения. Случайная модель Oracle. Установление подлинности сообщения 1.11. Криптографические хеш-функции (2 часа). Итеративные хеш-функции. Схема Меркеля-Дамгарда. Хеш- функции, основанные на блочных шифрах. Схема Рабина. Алгоритм безопасного хеширования SHA. Шифр Whirlpool. Российский стандарт хеширования ГОСТ Р 34.11-2012. 1.12. Электронная цифровая подпись (2 часа). Алгоритм формирования электронной цифровой подписи (ЭЦП). Схема ЭЦП RSA. ЭЦП Эль-Гамаля. ЭЦП Шнорра. Стандарт цифровой подписи DSS. Схема ЭЦП эллиптической кривой. Российский стандарт ЭЦП ГОСТ Р 34.10-2012. 1.13. Установление подлинности объекта (2 часа). Аутентификация на основе пароля. Одноразовый пароль. Система установления подлинности «запрос-ответ». Подтверждение с нулевым разглашением. Протокол Фиата-Шамира. Биометрия. Физиологические и поведенческие методы биометрии. **Тема 6. Управление криптографическими ключами**. 1.14. Генерация и хранение криптографических ключей (2 часа). Стандарт ANSI. X9.17. Методы хранения ключевой информации. 1.15. Алгоритмы безопасного распределения ключей (2 часа). Прямой обмен ключами

№	Наименование видов занятий и тематик, содержание
	между пользователями. Система «запрос-ответ». Алгоритм Ниидома-Шредера. Алгоритм Диффи-Хеллмана. Использование Центра распределения ключей. Инфраструктура PKI. Стандарт X.509. Система Kerberos. Тема 7. Основы современной стеганографии. 1.16. Основы современной стеганографии (2 часа). Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии. Цифровые метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами. **Тема 8. Основы криптоанализа.** 1.17. Обзор методов криптоанализа (2 часа). Методы криптоанализа. Криптоанализ блочных шифров. Частотный криптоанализ. Современные методы криптоанализа. Дифференциальный криптоанализ. Линейный криптоанализ. Интерполяционный криптоанализ. Методы криптоанализа, основанные на слабости ключевых разверток.
2	**Лабораторные работы**, количество - 8 по 4 (2) часа. 2.1. Разработка классических криптоалгоритмов. 2.2. Генерация и тестирование псевдослучайных последовательностей. 2.3 Программные средства реализации современные симметричные криптосистемы. 2.4. Современные симметричные криптосистемы. Программная реализация существующих симметричных криптоалгоритмов 2.5 Асимметричные криптосистемы. Изучение принципов работы асимметричных криптосистем; Изучение реализаций асимметричной криптографии в среде .NET Framework; Реализация существующих асимметричных криптоалгоритмов. 2.6. Хеширование и электронная цифровая подпись. Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП); Изучение реализаций хэш-функций и ЭЦП в среде .NET Framework; Реализация существующих хэш-функций и алгоритмов ЭЦП. 2.7. Безопасное распределение ключей. Изучение методов безопасного распределения ключей в небезопасной среде. Изучение свойств и методов класса ECDiffieHellmanCng пространства имен System.Security.Cryptography для создания ключей по алгоритму Диффи-Хеллмана. Использование алгоритма шифрования RSA для безопасного распределения ключей симметричной криптосистемы 2.8. Разработка стеганографической системы. Разработка системы для скрытой передачи сообщений.
3	**Практические работы**, количество - 9 по 2 часа. 3.1. Шифры перестановки 3.2. Симметричные криптосистемы 3.3. Ассиметричные криптосистемы 3.4. Технологии цифровой подписи 3.5. Разработка стеганографической системы. 3.6. Разработка системы для скрытой передачи сообщений. 3.7. Частотный криптоанализ. 3.8. Криптоанализ шифра Вижинера
3	**Курсовая работа** «Криптографические методы и средства защиты информации». Выполнение индивидуального задания, предполагающего разработку программы. Примерная тематика: • Криптоанализ блочных симметричных шифров • Криптоанализ поточных симметричных шифров

№	Наименование видов занятий и тематик, содержание
	• Криптоанализ хэш-функций • Исследование безопасности генераторов ПСЧ • Разработка системы аутентификации пользователей с нулевым разглашением • Идентификация пользователя по клавиатурному почерку • Разработка криптосистемы на основе метода эллиптических кривых • Библиотека криптографических функций ГОСТ Р 34.12-2015 • Программная реализация криптосистемы Хилла • Исследование методов реализации безопасных и эффективных постквантовых криптосистем • Разработка системы атрибуции документов • Разработка стеганографической системы • Защита информации с помощью цифровых водяных знаков • Система тестирование псевдослучайных последовательностей с помощью статистического теста «Стопка книг» • Генератор псевдослучайных чисел на основе клеточных автоматов
4	**Самостоятельная работа** студентов: 4.1. Подготовка к защите лабораторных работ. 4.2. Подготовка к практическим занятиям. 4.2. Самостоятельное изучение теоретических материалов по следующим вопросам. Тема 1. Изучение классических криптосистем (Шифр Цезаря, Полибианский квадрат, Двойной квадрат Уитстона, Одноразовая система шифрования, диск Альберти, шифр Вижинера, роторные машины). Тема 2. Изучение следующих материалов: вычисление мультипликативных обратных величин, расширенный алгоритм Евклида, китайская теорема об остатках, квадратичные вычеты, вычисления в конечных полях. Тема 3. Режимы работы алгоритма DES. Алгоритмы 3DES, EDE, IDEA, Blowfish. Формирование ключей алгоритма AES. Тема 4. Ранцевая криптография. Тема 5. Протокол Фейге-Фиата-Шамира. Протокол Кискатера-Гийу. Тема 6. Принцип работы системы Kerberos. Тема 7. Стеганография в современных кибератаках. Тема 8. Математические методы криптоанализа асимметричных криптосистем. 4.3. Выполнение курсовой работы.

Текущий контроль:
- проверка конспектов лекций и дополнительных теоретических материалов;
- проверка отчетов по лабораторным работам;
- защита лабораторных работ;
- контрольный опрос и выполнение контрольных заданий на практических занятиях;
- консультации по курсовой работе.

Результаты текущего контроля фиксируются с использованием трехбалльной системы (0, 1, 2) при проведении контрольных недель по графику филиала в течение семестра, а также учитываются преподавателем при осуществлении промежуточной аттестации по настоящей дисциплине.

К промежуточной аттестации студентов по дисциплине могут привлекаться представители работодателей, преподаватели последующих дисциплин, заведующие кафедрами.

Оценка качества освоения дисциплины включает как текущий контроль успеваемости, так и промежуточную аттестацию.

Оценочные средства текущего контроля успеваемости:

Вопросы для защиты лабораторных работ

Лабораторная работа 1 на тему «*Разработка классических криптоалгоритмов*».

1. К какому классу шифров относится шифр Вижинера
2. К какому классу шифров относится диск Альберти
3. К какому шифру наиболее близок алгоритм работы роторной машины
4. Дана фраза «HQFUBSWGHFUBSW», зашифрованная шифром Цезаря. Криптоаналитику известно, что ключ представляет собой число в диапазоне от 2 до 4. Выполните дешифрование
5. Дана фраза «GQSUGAAC», зашифрованная методом Гронсфельда. Криптоаналитику известно, что длина ключа равна 3 и ключ представляет собой сочетание цифр 1 и 2. Выполните дешифрование

Лабораторная работа 2 на тему «*Генерация и тестирование псевдослучайных последовательностей*».

1. Перечислите способы получения случайных чисел
2. Какие числа называются псевдослучайными
3. В чем заключается сущность мультипликативного конгруэнтного метода формирования последовательности равномерно распределенных псевдослучайных чисел
4. Какие тесты используются для проверки генераторов псевдослучайных чисел.
5. Объясните метод проверки генераторов псевдослучайных чисел, основанный на использовании критерия хи-квадрат

Лабораторная работа 3 на тему «*Программные средства реализации современные симметричные криптосистемы*».

1. Перечислите основные классы пространства имен System.Security.Cryptography. Кратко опишите назначение каждого класса
2. Перечислите основные методы класса System.Security.Cryptography. SymmetricAlgorithm
3. Перечислите классы, производные от класса System.Security.Cryptography. SymmetricAlgorithm. Кратко опишите назначение каждого класса
4. С помощью какого метода пространства имен System.Security.Cryptography производится проверка ключей криптографическую слабость

Лабораторная работа 4 на тему «*Современные симметричные криптосистемы*».

1. Сравните DES и AES. Какой из них ориентирован на работу с битом, а какой с байтом
2. Сравните подстановку в DES и AES. Почему в AES только одна таблица перестановки (S-блок), а в DES- несколько
3. Сравните ключи раунда в DES и AES. В каком шифре размер ключа раунда равен размеру блока.
4. Для каких целей используется режим выработки имитовставки в алгоритме Магма (ГОСТ Р 34.12-2015
5. Сравните алгоритмы ГОСТ 8147-89 и Магма (ГОСТ Р 34.12-2015)
6. Сравните алгоритмы AES и Кузнечик (ГОСТ Р 34.12-2015)

***Лабораторная работа 5 на тему «*Асимметричные криптосистемы».**

1. Для числа a=5 найдите обратное число по модулю n=7. Имеет ли данная задача решение? Приведите примеры криптосистем, использующих правила модулярной арифметики.
2. Для числа a=72 найдите обратное число по модулю n=8. Имеет ли данная задача решение? Приведите примеры криптосистем, использующих правила модулярной арифметики.
3. Для числа N=7*11 с помощью функции Эйлера φ(N) определите количество положительных целых чисел, меньших N и взаимно простых с N. В каких криптосистемах используется функция Эйлера?
4. Определите хотя бы одно возможное значение открытого ключа алгоритма RSA, если P=3 Q=11.
5. Определите значение закрытого ключа для алгоритма RSA, если открытый ключ E=7, а функция Эйлера имеет значение φ(N)=20
6. В криптосистеме RSA дано N=221 и E=5, найдите D.
7. В криптосистеме RSA дано N=3937 и E=17, найдите D.
8. В криптосистеме RSA дано P=19, Q=23 и E=3, найдите N, φ(N) и D.
9. В криптосистеме RSA дано E=13 и N=100. Зашифруйте сообщение «HOW ARE YOU», кодируя английский алфавит числами от 00 до 25 и используя число 26 для пробела. Используйте различные блоки, чтобы сделать P <N

***Лабораторная работа 6 на тему «*Хеширование и электронная цифровая подпись».**

1. Что называется «электронной цифровой подписью»?
2. Для чего используется электронная цифровая подпись?
3. Что такое дайджест сообщения?
4. Используя схему RSA, при P=809, Q=751 и секретный ключ D=23, вычислите открытый ключ E, затем, подпишите и проверьте сообщение M_1=100. Получите подпись S_1.
5. Используя схему RSA, при P=809, Q=751 и секретный ключ D=23, вычислите открытый ключ E, затем, подпишите и проверьте сообщение M_2=50. Получите подпись S_2.
6. Используя схему RSA, при P=809, Q=751 и секретный ключ D=23, вычислите открытый ключ E, затем, покажите, что если M=M_1x M_2=5000, то S=S_1xS_2.

***Лабораторная работа 7 на тему «*Безопасное распределение ключей».**

1. В протоколе Диффи-Хеллмана g=7, p=23, секретный ключ пользователя A =3, секретный ключ пользователя B =5. Какое значение имеет симметричный ключ? Какие значения имеют открытые ключи пользователей A и B?
2. Что случится в протоколе Диффи-Хеллмана, если секретные ключи пользователей A и B имеют одно и то же значение? Будут ли совпадать открытые ключи пользователей A и B? Будут ли совпадать симметричные ключи, вычисленные пользователями A и B? Приведите пример, для доказательства Ваших умозаключений.
3. В протоколе Диффи-Хеллмана значение p=53. Найдите соответствующее значение для g.
4. Какие классы содержит пространство имен System.Net.Sockets. Опишите назначение, особенности и функциональные возможности каждого класса.
5. Укажите преимущества и недостатки протокола UDP. Ответ обоснуйте.
6. Укажите преимущества и недостатки протокола TCP. Ответ обоснуйте.
7. Дайте определение сокета. Какую информацию должен содержать сокет?

***Лабораторная работа 8 на тему «*Разработка стеганографической систем».**

1. Перечислите базовые принципы компьютерной стеганографии

2. Особенности упаковки информации в файлы формата JPEG
3. Какие звуковые файлы рекомендуется выбирать в качестве контейнеров
4. Какие графические файлы рекомендуется выбирать в качестве контейнеров
5. Изменяются ли размеры файлов-контейнеров разных типов после сокрытия в них информации
6. Как происходит сокрытие информации в текстовых и html-файлах

Оценочные средства для промежуточной аттестации – защита КР

Когда курсовая работа полностью выполнена (т.е. курсовая работа выполнена и оформлена, проверена руководителем, продемонстрирована работающая программа), она допускается к защите. Требования к содержанию и оформлению КР приведены в методических указаниях по КР.

Дата, место защиты и состав членов комиссии назначаются заранее распоряжением по кафедре.

На защиту представляется:

курсовая работа в печатном виде, в обложке и переплетенная (сшитая);

курсовая работа в электронном виде;

программа в исходной форме;

программа откомпилированная.

Студент должен подготовить краткий доклад по курсовой работе, в котором должен коротко изложить:

особенности своего задания;

способы реализации;

выбор средств реализации;

функциональные особенности и логическую структуру разработанных средств,

а также подтвердить работоспособность программы на практике.

Доклад должен подкрепляться показом соответствующих материалов из курсовой работы и демонстрацией разработанных средств.

По итогам доклада студенту могут быть заданы вопросы, на которые необходимо получить ответы.

Оценка курсовой работы определяется коллегиально членами назначенной комиссии.

Критерии оценивания результатов уровня сформированности компетенции в процессе выполнения и защиты курсовой работы представлены в таблице.

Таблица

Оценочный лист курсовой работы по дисциплине «Криптографические методы и средства защиты информации»

Критерии оценки (компетенции)	Уровень освоения компетенций (оценка в баллах)				Баллы
	эталонный (5)	продвинутый (4)	пороговый (3)	ниже порогового (2)	
Актуальность темы	Актуальность темы работы аргументирована.	Актуальность темы работы сравнительно аргументирована.	Актуальность темы работы недостаточно аргументирована.	Актуальность темы работы не аргументирована.	
Содержание (раскрытие темы, достижение цели, выполнение задач	Теоретическое содержание темы полностью раскрыто; проведен полный анализ практического материала; аргументиро-	Теоретическое содержание темы в основном раскрыто; анализ практического материала недостаточно полный; выводы недо-	Теоретическое содержание темы раскрыто поверхностно; анализ практического материала не полный; выводы сформулированы	Теоретическое содержание темы не раскрыто; достаточно поверхностный анализ практического материала; выводы и пред-	

	ваны выводы, обоснованы предложения. Цель достигнута. Задачи выполнены.	статочно аргументированы, предложения в основном обоснованы. Цель достигнута. Задачи выполнены.	в общей форме и не конкретны; неполное обоснование предложений. Цель достигнута частично. Некоторые задачи не выполнены.	ложения не сформулированы. Поставленная цель не достигнута. Задачи не выполнены.	
Сроки выполнения курсовой работы	Строгое выполнение графика	График выполнения курсовой работы в основном выполнялся (в 2-х контрольных неделях по 1 баллу)	Незначительные нарушения графика (в одной контрольной неделе 0 баллов)	Значительные нарушения графика (в 2-х контрольных неделях по 0 баллов)	
Оформление работы	Строго в соответствии с требованиями.	Допущено несколько незначительных неточностей.	Оформление с допустимыми погрешностями.	Значительные нарушения требований.	
Публикации	Имеются публикации по теме работы	***При отсутствии публикации проставляется оценка – 0 баллов***			
Доклад	Доклад содержателен, логичен; отражает результаты работы, лимит времени не превышен. Студент не читает доклад с листа, показывает высокое владение профессиональным языком.	Доклад относительно содержателен, логичен, в основном отражает результаты работы, лимит времени превышен незначительно. Студент не читает доклад с листа, хорошо владеет профессиональным языком.	Доклад логически не проработан, плохо отражает результаты работы, лимит времени превышен значительно. Студент в основном читает доклад с листа, удовлетворительно владеет профессиональным языком.	Доклад не содержателен, логически не выстроен, не отражает результаты работы, лимит времени превышен значительно. Студент читает доклад с листа, слабо владеет профессиональным языком.	
Презентация	Не повторяет текст доклада, содержит графики, схемы, иллюстрирующие результаты работы. Информация отлично читаема с экрана; цветовое оформление не мешает восприятию информации, текст не содержит ошибок.	Незначительно повторяет текст доклада, содержит графики, схемы, в основном иллюстрирующие результаты работы. Информация хорошо читаема с экрана; цветовое оформление не способствует хорошему восприятию информации, текст не содержит ошибок	Значительно повторяет текст доклада, содержит графики, схемы, недостаточно полно иллюстрирующие результаты работы. Информация удовлетворительно читаема с экрана; цветовое оформление неудачное, текст содержит небольшое количество ошибок	Значительно повторяет текст доклада; содержит в основном текстовые слайды слабо иллюстрирующие результаты работы. Информация плохо читаема с экрана; цветовое оформление мешает восприятию информации, текст содержит большое количество ошибок	
Ответы на вопросы	Ответы правильные, полные, логичные, убедительные; высокое владение профессиональным языком, аргументированная защита своей точки зрения.	Ответы в основном правильные, полные, логичные; хорошее владение профессиональным языком, средняя аргументация и защита своей точки зрения	Не на все вопросы даны полные, логичные ответы; удовлетворительное владение профессиональным языком, низкая способность защиты своей точки зрения	Отсутствие правильных ответов на вопросы; плохое владение профессиональным языком, неспособность защиты своей точки зрения	

Оценочные средства для промежуточной аттестации:

Примеры вопросов к экзамену по дисциплине

1. Криптография. Основные термины и определения. Задачи криптографии. Классификация алгоритмов шифрования
2. Этапы развития криптографии
3. Стеганография
4. Американский стандарт шифрования DES
5. Режимы работы алгоритма DES
6. Симметричная криптосистема AES
7. Российский стандарт шифрования ГОСТ 28147-89

8. Российский стандарт шифрования ГОСТ Р 34.12-2015
9. Шифр одноразового блокнота. Принцип использования ГПСП при поточном шифровании.
10. Шифр RC4
11. Применение современных блочных шифров. Использование шифров потока.
12. Методы повышения криптостойкости симметричных криптосистем
13. Асимметричные системы шифрования. Основной принцип работы. Однонаправленные функции
14. Система шифрования RSA.
15. Криптосистема Эль-Гамаля.
16. Криптосистема Рабина.
17. Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа
18. Криптография эллиптической кривой, моделирующая криптосистему Эль-Гамаля.
19. Хэш-функции. Основные требования и примеры построения.
20. Целостность сообщения. Случайная модель Oracle.
21. Схема Меркеля-Дамгарда.
22. Хеш- функции, основанные на блочных шифрах. Схема Рабина.
23. Алгоритм хеширования SHA
24. Шифр Whirlpool.
25. Российский стандарт хеширования ГОСТ Р 34.11-2012.
26. Электронная цифровая подпись RSA.
27. ЭЦП Эль-Гамаля.
28. ЭЦП Шнорра.
29. Стандарт цифровой подписи DSS.
30. Схема ЭЦП эллиптической кривой. Российский стандарт ЭЦП ГОСТ Р 34.10-2012.
31. Аутентификация на основе пароля. Одноразовый пароль.
32. Система установления подлинности «запрос-ответ».
33. Подтверждение с нулевым разглашением. Протокол Фиата-Шамира.
34. Биометрия. Физиологические и поведенческие методы биометрии.
35. Управление ключами. Генерация ключей и хранение ключей. Стандарт ANSI. X9.17.
36. Алгоритм Ниидома-Шредера.
37. Алгоритм безопасного распределения ключей Диффи-Хэллмана
38. Сертификаты открытых ключей.
39. Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии.
40. Цифровые метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами.
41. Методы криптоанализа. Криптоанализ блочных шифров.
42. Частотный криптоанализ.
43. Дифференциальный криптоанализ.
44. Линейный криптоанализ.
45. Интерполяционный криптоанализ.
46. Методы криптоанализа, основанные на слабости ключевых разверток.

Пример практических заданий, выносимых на экзамен, для проверки практических умений и навыков студентов по дисциплине

Задача к билету № 1

Алгоритм шифрования RSA. Пользователь выбирает P=5, Q=9. Определите, можно ли использовать в качестве открытого ключа E число 11. Если возможно, то определите значение секретного ключа D.

Задача к билету № 2

Для числа N=7*11 с помощью функции Эйлера φ(N) определите количество положительных целых чисел, меньших N и взаимно простых с N.

Задача к билету № 3

Фраза «КОМПАНИЯ «ЛЮЦИФЕР» ИСПОЛЬЗУЕТ ЕДКИЙ НАТР, ТЯЖЕЛЫЕ ГРУЗИЛА, ОСТРОГУ ТРЕХЗУБУЮ, ОБВЕТШАЛЫЙ ВАТНИК» содержит скрытую информацию. Для сокрытия информации используется стеганографический метод. Прочитайте скрытую информацию.

Задача к билету № 4

Даны восемь чисел: 128,192, 224, 240, 248, 252, 254, 255. Как расположить эти числа на плоскости, чтобы образовалось два прямоугольных треугольника

Формы промежуточной аттестации по настоящей дисциплине – экзамен.

Основная литература.

1 Лапонина О.Р. Криптографические основы безопасности [Электронный ресурс]. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 244 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=429092.

2 Аверченков В.И. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. — Москва : ФЛИНТА, 2017. — 215 с. — Режим доступа: https://e.lanbook.com/book/92914..

3 Кирпичников А.П. Криптографические методы защиты компьютерной информации [Электронный ресурс] : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. — Казань : КНИТУ, 2016. — 100 с. — Режим доступа: https://e.lanbook.com/book/101905.

4. Методические указания к лабораторным работам по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А., Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 112 с.

5. Методические указания по выполнению курсовой работы по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А., Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 8 с.

Дополнительная литература

1 Ищукова Е.А. Криптографические протоколы и стандарты [Электронный ресурс] : учебное пособие / Е.А. Ищукова, Е.А. Лобова. — Таганрог : Издательство Южного федерального университета, 2016. — 80 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=493059.

2 Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / авт.-сост. И.А. Калмыков, Д.О. Науменко, Т.А. Гиш ; Министерство образования и науки Российской Федерации и др. —- Ставрополь : СКФУ, 2015. — 109 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=458059.

3 Фороузан Б.А. Математика криптографии и теория шифрования [Электронный ресурс] : — 2-е изд., испр. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 511 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=428998.

4 Рябко Б.Я. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / Б.Я. Рябко, А.Н. Фионов. — Москва : Горячая линия-Телеком, 2017. — 230 с. — Режим доступа: https://e.lanbook.com/book/111097.

5 Бутакова Н.Г. Криптографические методы защиты информации, учебное пособие [Электронный ресурс] : учебное пособие / Н.Г. Бутакова, Н.В. Федоров. — Санкт-Петербург : ИЦ Интермедия, 2016. — 384 с. — Режим доступа: https://e.lanbook.com/book/90270.

6 Стеганографические и криптографические методы защиты информации [Электронный ресурс] : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: https://e.lanbook.com/book/90963.

Список авторских методических разработок.

Методическое обеспечение по дисциплине «Криптографические методы и средства защиты информации» включает также следующие авторские разработки преподавателей кафедры вычислительной техники:

1. Методические указания к лабораторным работам по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А., Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 112 с.

2. Методические указания по выполнению курсовой работы по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А., Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 8 с.

– комплект лекций в формате мультимедийных презентаций;

- учебно-методические материалы размещены на ресурсах кафедры.