АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность

Магистерская программа: «Безопасность автоматизированных систем»

Б1.В.05 «Криптографические методы и средства защиты информации»

№	Индекс	Наименование	Семестр 3											Итого за курс										Каф	Сем
			Контроль	Академических часов								З.е.	Недель	Контроль	Академических часов								З.е.	Недель		
				Всего	Контакт	Лек	Лаб	Пр	КРП	СР	Контроль				Всего	Контакт	Лек	Лаб	Пр	КРП	СР	Контроль	Всего			
8	Б1.В.06	Криптографические методы и средства защиты информации	Экз, КР	180	104	34	34	18	18	40	36	5		Экз, КР	180	104	34	34	18	18	40	36	5		15	3

Формируемые компетенции: ПК-1

Содержание дисциплины

№	Наименование видов занятий и тематик, содержание
1	**Лекционные занятия, количество** - 17 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 шиф-

№	Наименование видов занятий и тематик, содержание
	ров. 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 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.

№	Наименование видов занятий и тематик, содержание
	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 • 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

№	Наименование видов занятий и тематик, содержание
	• 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 Уитсттона, 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 КРП.

Год начала подготовки 2024

Образовательный стандарт № 1455 от «26» ноября 2020 г.