АННОТАЦИЯ

Дисциплины

«Криптография»

Направление подготовки – 38.03.05 «Бизнес-информатика»

Квалификация (степень) выпускника – бакалавр

Профиль – «Архитектура предприятия»

**1. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Криптография» (Б1.В.ОД.19) относится к вариативной части и является обязательной для изучения.

**2. Цель и задачи дисциплины**

Целью изучения дисциплины является формирование у обучающихся компетенций в соответствии с учебным планом за счет освоения теоретических основ криптографической защиты информации в автоматизированных системах.

Для достижения поставленной цели решаются следующие задачи:

* формирование у обучающихся понятийного аппарата в области криптографии и информационной безопасности;
* освоение обучающимися методики определения актуальных угроз для криптографических систем;
* формирование у обучающихся знаний о методах криптографической защиты информации в автоматизированных информационно-управляющих системах.
* формирование у обучающихся начальных навыков построения и использования криптографических методов защиты информации;

**3. Перечень планируемых результатов обучения по дисциплине**

Изучение дисциплины направлено на формирование следующих компетенций: ОК - 7, ПК- 9.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ**:

* функции криптосистем (обеспечение конфиденциальности, целостности, подлинности информации);
* математическую модель системы шифрования (дешифрования);
* безусловно-стойкие шифры, способы и условия их реализации;
* классификацию шифров (блоковые, потоковые, с открытым ключом);
* основные методы криптоанализа блоковых шифров (переборный, на основе анализа статистики криптограммы);
* примеры построения блоковых шифров AES, ГОСТ Р 34.12-15;
* принципы построения потоковых шифров;
* модель системы аутентификации сообщений;
* безусловно и вычислительно стойкие системы аутентификации;
* принципы построения хэширующих функций;
* принципы построения криптосистем с открытымключем;
* аппарат теории чисел, алгебры в части построения и анализа криптосистем с открытымключем;
* принципы построения криптосистем с открытымключем Эль-Гамаля, РША;
* модель цифровой подписи сообщения. Виды ЭЦП. Основные схемы ЭЦП, включая ЭЦП на основе эллиптических кривых;
* управления ключами в симметричных криптографических системах;
* этапы жизненного цикла ключа;
* способы распределения ключа с использованием центра распределения ключей.
* модель управления открытыми ключами. Принципы построения PKI. Назначение и порядок использования сертификатов открытых ключей.

**УМЕТЬ**:

* пользоваться методами теории чисел;
* рассчитывать основные характеристики и параметры криптографических алгоритмов защиты информации;
* оценивать (в первом приближении) стойкость основных криптосистем и их элементов;
* шифровать и дешифровать информацию с помощью симметричных и асимметричных криптосистем;
* генерировать и проверять электронную подпись при передаче и получении электронных сообщений и документов;

**ВЛАДЕТЬ**:

* навыками использования типовых криптографических алгоритмов;
* навыками анализа основных характеристик систем с открытыми ключами;
* программной реализации элементов криптосистем с открытым ключем.

**4. Содержание и структура дисциплины**

1. Введение.
2. Алгоритмы шифрования информации в симметричных криптосистемах.
3. Аутентификация сообщений .
4. Криптографические системы с открытыми ключами.
5. Управление криптографическими ключами.

**5. Объем дисциплины и виды учебной работы**

Объем дисциплины – 3 зачетные единицы (108часов), в том числе:

лекции – 16 часов;

лабораторные работы – 32 часов;

самостоятельная работа – 51 час.

контроль – 9 часов.

Формы контроля знаний – зачет.