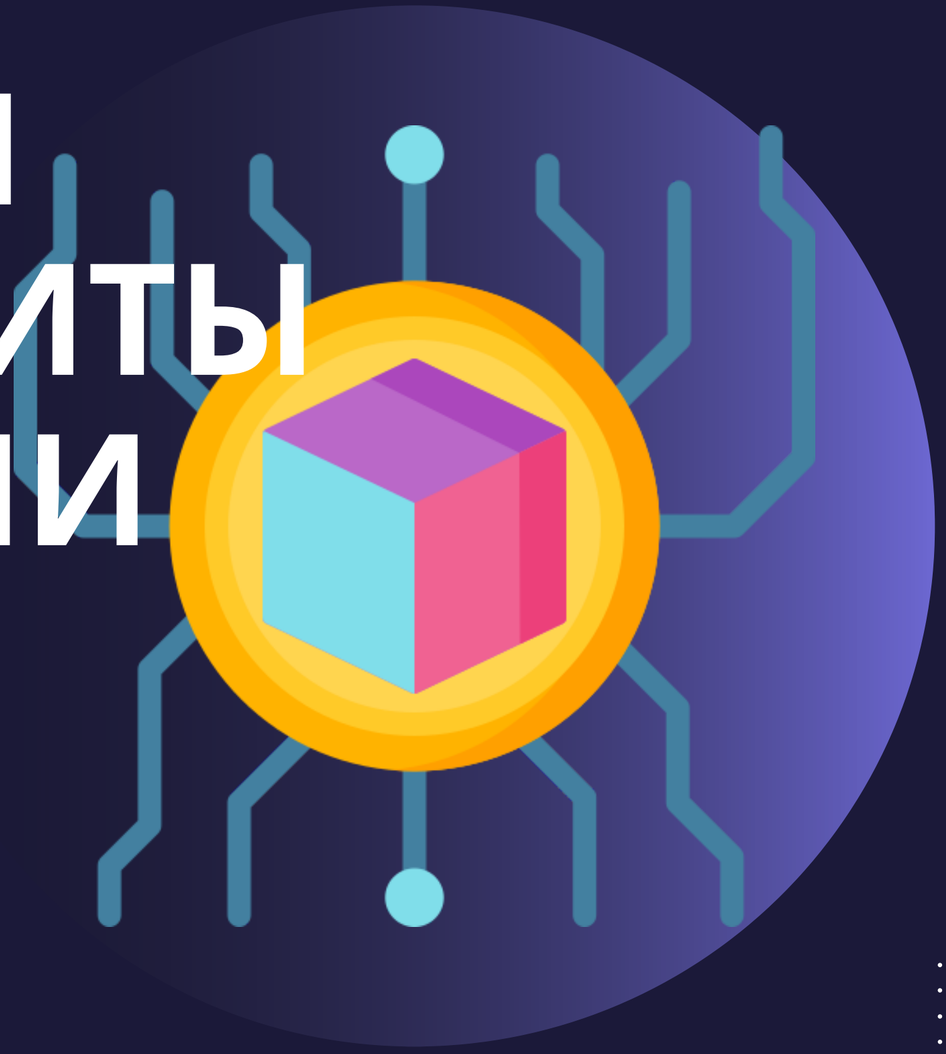
ТЕХНОЛОГИИ КРИПТОЗАЩИТЫ ИНФОРМАЦИИ



ТЕМЫ ДЛЯ РАЗБОРА

Технологии криптозащиты информации

- Симметричная криптосистема
- Асимметричные криптосистемы
- Хэш-функция
- Квантовая криптография

ТЕХНОЛОГИИ КРИПТОЗАЩИТЫ ИНФОРМАЦИИ

Краткое введение

Криптография – это совокупность технических, математических, алгоритмических и программных методов преобразования данных,которая делает их бесполезными для любого пользователя, у которого нет ключа для расшифровки.

БАЗОВЫЕ ЗАДАЧИ

КОНФИДЕНЦИАЛЬНОСТЬ

Невозможность прочитать данные и извлечь полезную информацию

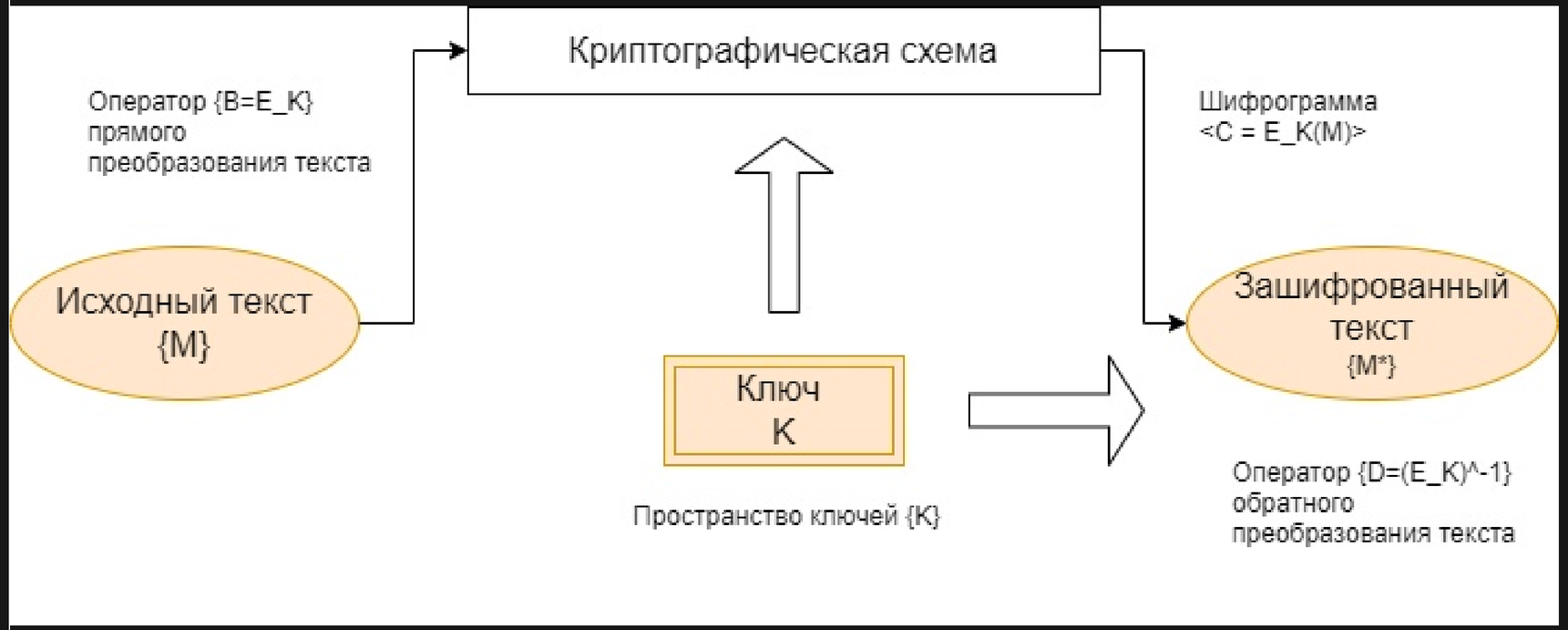
ЦЕЛОСТНОСТЬ

Невозможность модифицировать данные для изменения смысла или внесения ложной информации

ПРОЦЕССЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

1. **ИДЕНТИФИКАЦИЮ ОБЪЕКТА ИЛИ СУБЪЕКТА СЕТИ.**
2. **АУТЕНТИФИКАЦИЮ ОБЪЕКТА ИЛИ СУБЪЕКТА СЕТИ.**
3. **КОНТРОЛЬ ДОСТУПА К РЕСУРСАМ ЛОКАЛЬНОЙ СЕТИ ИЛИ ВНЕСЕТЕВЫМ СЕРВИСАМ.**
4. **ОБЕСПЕЧЕНИЕ И КОНТРОЛЬ ЦЕЛОСТНОСТИ ДАННЫХ.**

СИММЕТРИЧНАЯ КРИПТОСИСТЕМА



Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), RC2, RC5, CAST, Blowfish

Майкл Джон Бобак

АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Rivest Shamir Adleman (RSA), алгоритм Эль Гамаля, криптосистема ECC на эллиптических кривых, алгоритм открытого распределения ключей Диффи – Хеллмана.

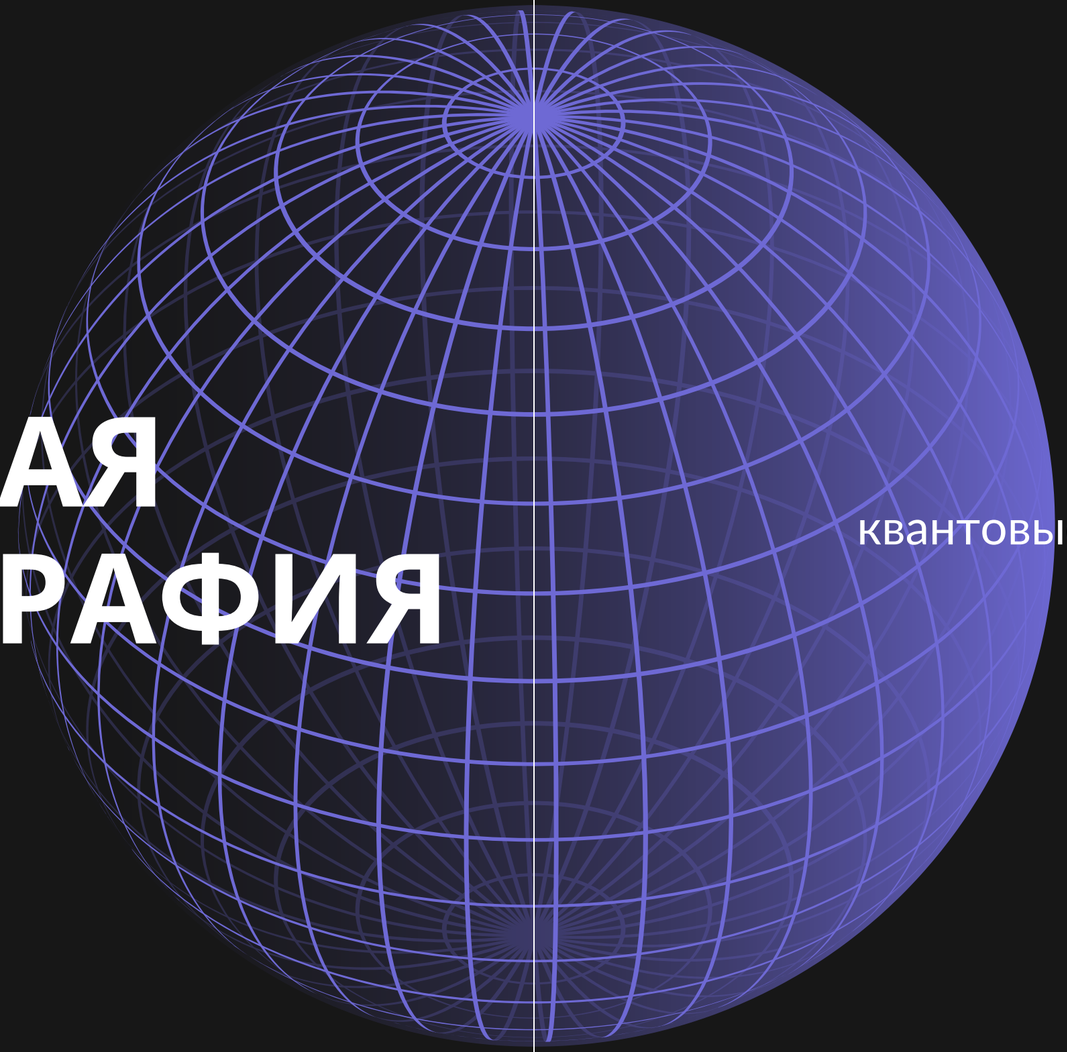
ХЭШ-ФУНКЦИЯ

Отображение, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины h(M) – дайджест сообщения.

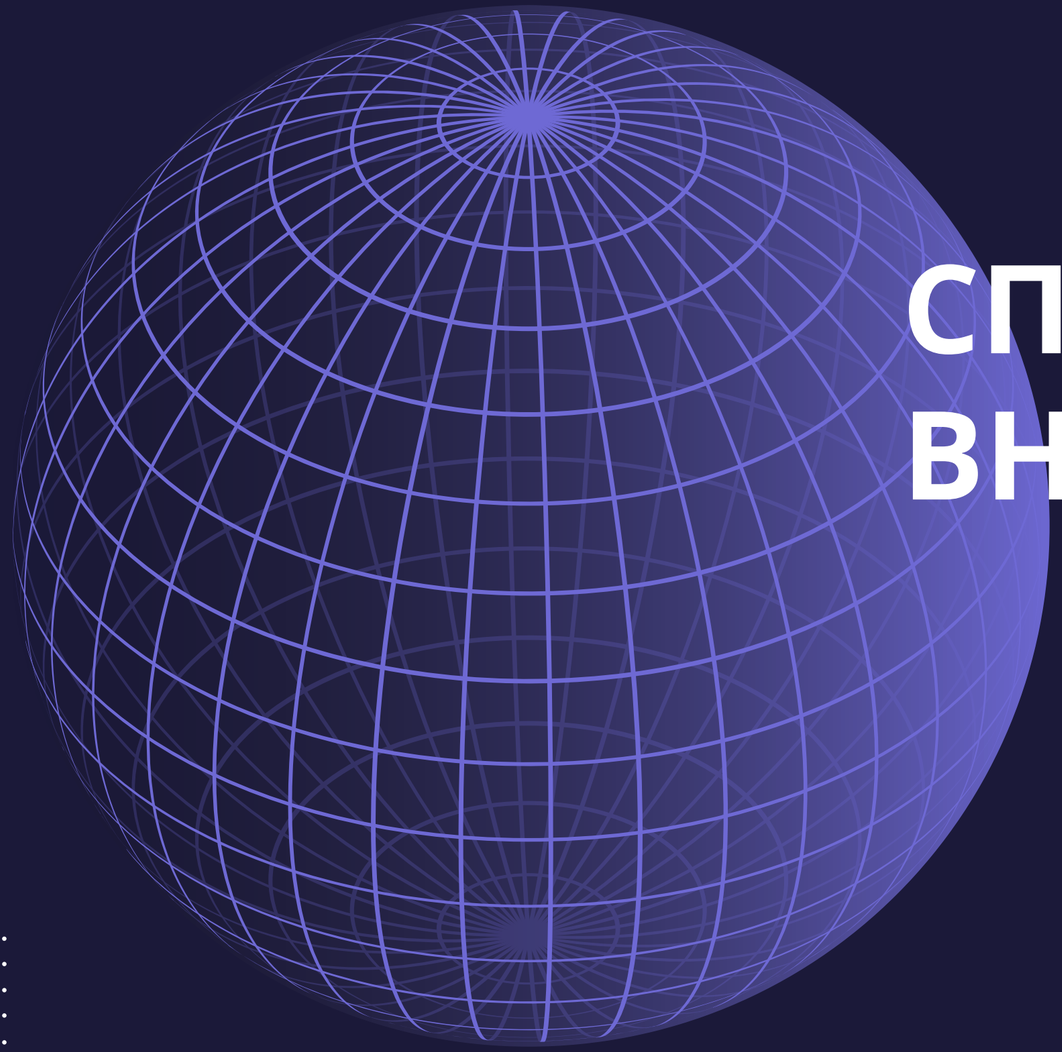
1.Стойкость к восстановлению
2. Стойкость к коллизиям

Message Digest 4 (MD4), Message Digest 5 (MD5),
SHA (Secure Hash Algorithm)

КВАНТОВАЯ КРИПТОГРАФИЯ



квантовые технологии — это будущее



СПАСИБО ЗА ВНИМАНИЕ.