### Цели и задачи защиты информации

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Формы представления информации:

* Речевая
* Телекоммуникационная
* Документированная

### Основные характеристики защищаемой информации

К защищаемой информации относится информация, являющаяся предметов собственности и подлежащая защите.

Информационная безопасность – комплекс мероприятий, которые обеспечивают для охватываемой им информации следующие факторы:

* Конфиденциальность
* Целостность
* Доступность

### Угрозы безопасности информации – основные типы угроз

Угрозы безопасности информации – событие или действие, которое может вызвать нарушение в работе информационной системы. Разделяют два вида угроз:

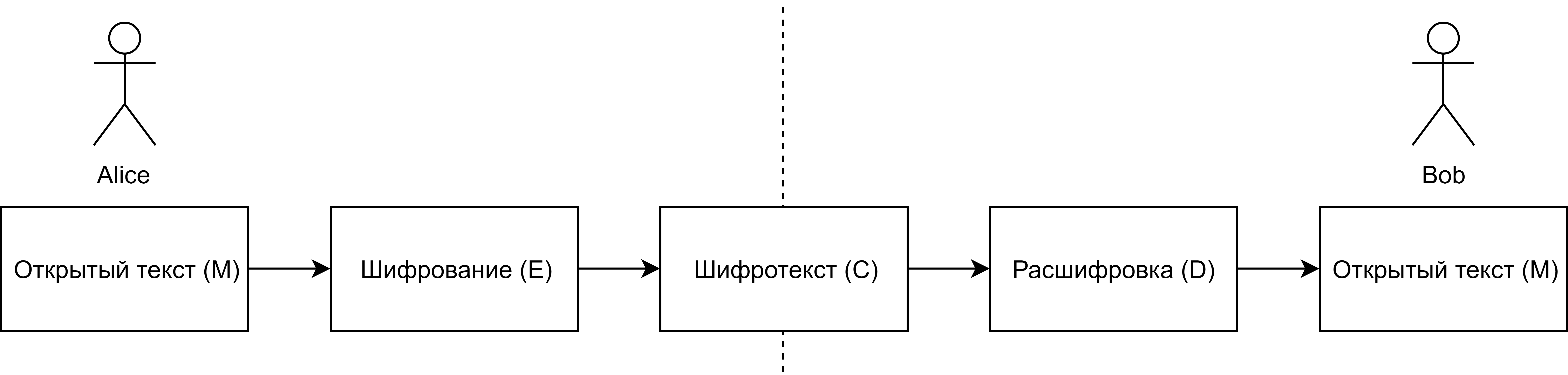
* 1. Естественные угрозы
  2. Искусственные угрозы
* Непреднамеренные
* Преднамеренные

### Основные группы, составляющие методы и средства защиты информации

### Правовое обеспечение информационной безопасности

### Инженерно-технические методы и средства защиты информации

### Основные принципы построения симметричных шифров



Попытка получить открытый текст при неизвестном криптографическом алгоритме называется дешифрацией, а лицо, пытающиеся получить информацию называется атакующим.

Криптографический алгоритм – последовательность математический операций, позволяющих зашифровать открытый тест или расшифровать шифротекст.

Существует два типа криптографических алгоритмов, основанных на использовании ключа: симметричные (один ключ при шифровании и расшифровке) и ассиметричные (разные ключи при шифровании и расшифровке)

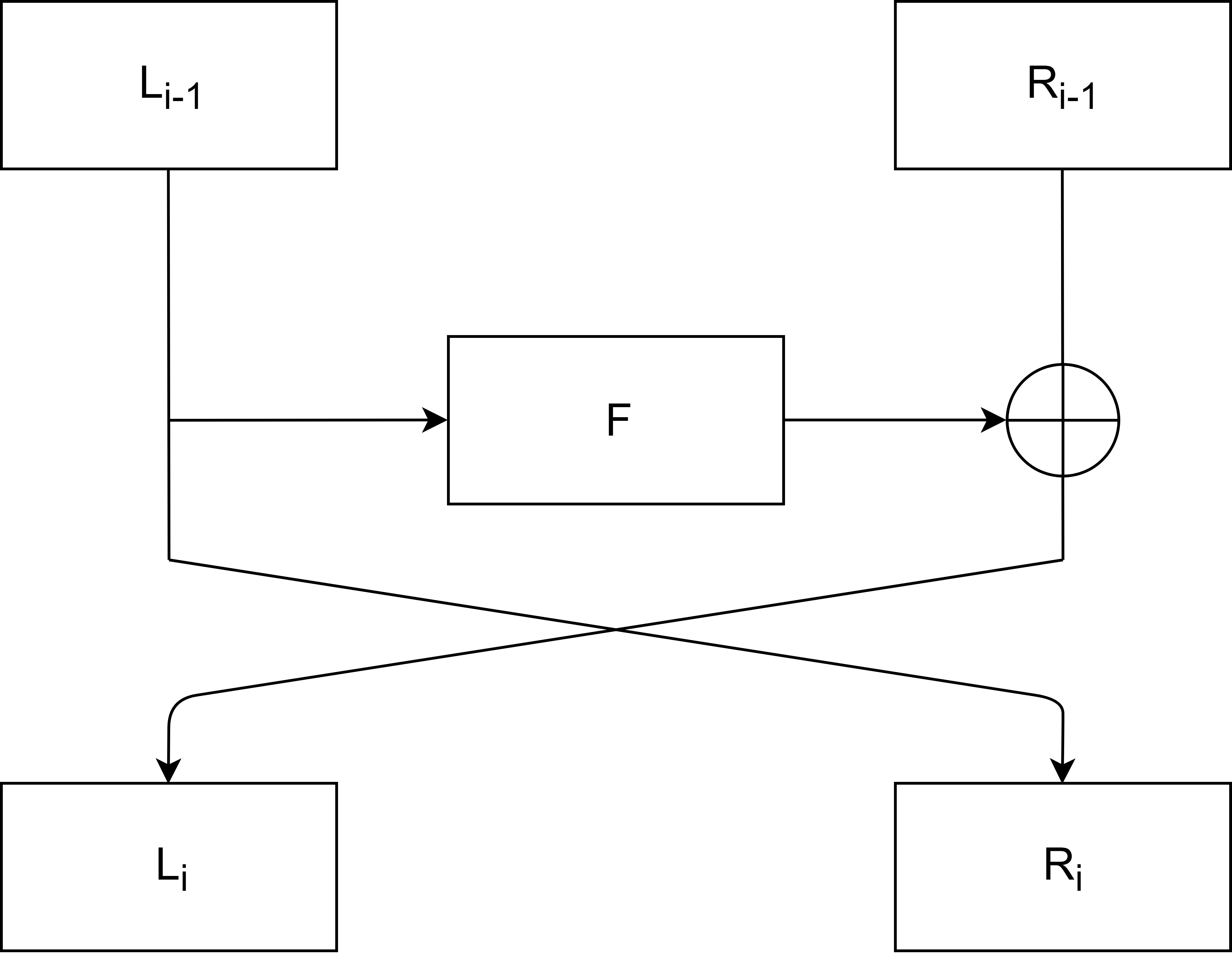
|  |  |  |
| --- | --- | --- |
| Сложение |  |  |
| Сложение по модулю 2 |  |  |
| Умножение по модулю |  |  |
| Циклические сдвиги |  |  |
|  |  |  |
| Табличная подстановка |  |  |

**Надежность схемы шифрования зависит только от секретности ключа и не зависит от алгоритма шифрования (расшифровки)**

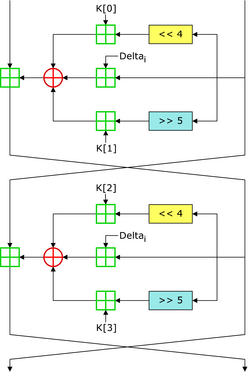
### Законодательные и нормативные документы информационной безопасности

### Алгоритмы симметричного шифрования: основные понятия и определения. Область применения

### Сеть Фейстеля как метод построения алгоритмов симметричного шифрования



### Алгоритм шифрования TEA

Tiny Encryption Algorithm (TEA) — блочный алгоритм шифрования типа «Сеть Фейстеля». Широко используется в ряде криптографических приложений и широком спектре аппаратного обеспечения благодаря крайне низким требованиям к памяти и простоте реализации. Впервые представлен в 1994 году.

Характеристики:

* Основан на сети Фейстеля
* Размер блока 64 бит
* Длина ключа 128 бит
* 32 раунда по умолчанию

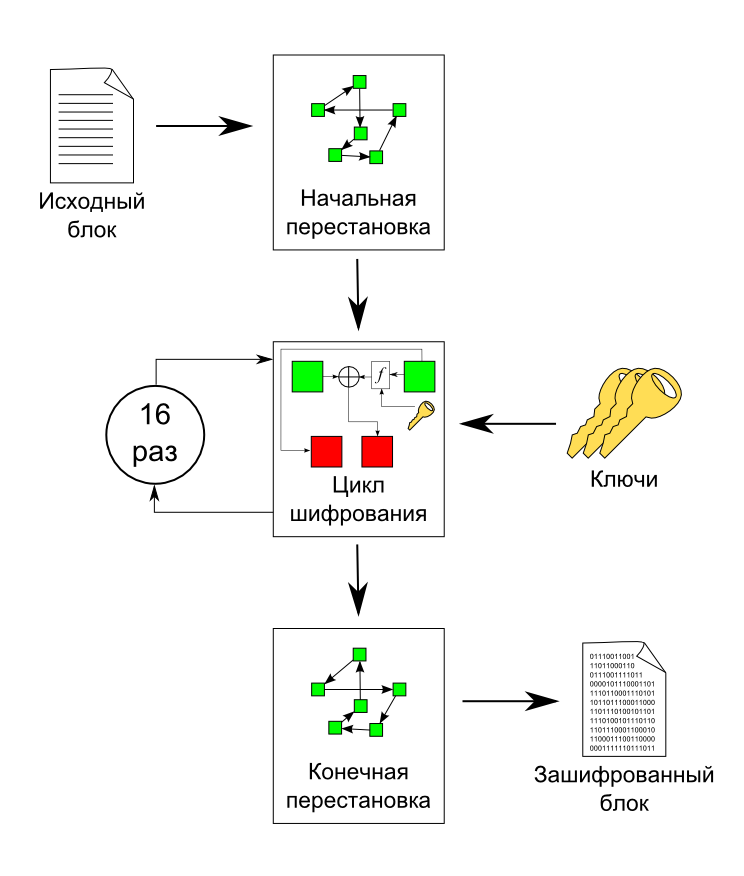
**Шифрование:**

|  |
| --- |
| delta = 2654435769  sum = 0  for i = 1 to 32 do  sum = sum + delta  L = L + ((R << 4) + K[0]) XOR (R + SUM) XOR ((R >> 5) + K[1])  R = R + ((L << 4) + K[2]) XOR (L + SUM) XOR ((L >> 5) + K[3])  return (L, R) |

**Расшифровка:**

|  |
| --- |
| delta = 2654435769  sum = 3337565984  for i = 1 to 32 do  R = R - ((L << 4) + K[2]) XOR (L + SUM) XOR ((L >> 5) + K[3])  L = L - ((R << 4) + K[0]) XOR (R + SUM) XOR ((R >> 5) + K[1])  sum = sum – delta  return (L, R) |

### Алгоритм шифрования DES

Data Encryption Standard (DES) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт.

Характеристики:

* Основан на сети Фейстеля
* Размер блока 64 бит
* Длина ключа 56 бит
* Количество раундов 16

### Режимы выполнения алгоритмов симметричного шифрования

### Алгоритм шифрования ГОСТ 28147-89

### Алгоритм шифрования 3DES

### Алгоритм шифрования DESX

### Алгоритм шифрования AES

### Потоковое шифрование

### Алгоритм RC4

### Криптографические хеш-функции

### Хеш-функции на основе блочных шифров

### Функция хеширования MD4

### Функция хеширования ГОСТ 3411-94

### Основные теоремы теории чисел

### Наибольший общий делитель. Алгоритмы Евклида

### Односторонняя функция

### Криптография с открытым ключом

### Задача распределения ключей

### Метод Диффи – Хеллмана

### Алгоритм шифрования Шамира

### Алгоритм шифрования Эль-Гамаля

### Алгоритм шифрования RSA

### Комбинированной криптосистемы (?)

### Электронная цифровая подпись

### Алгоритм цифровой подписи RSA

### Алгоритм цифровой подписи Эль-Гамаля

### Алгоритм цифровой подписи DSA

### Алгоритм цифровой подписи ГОСТ 3410-94

### Инфраструктура открытых ключей

### Сертификат открытого ключа

### Идентификация, аутентификация, авторизация

### Методы аутентификации, использующие одноразовые и многоразовые пароли

### Методы аутентификации, использующие симметричные и ассиметричные алгоритмы

### Биометрическая аутентификация пользователя

### Межсетевые экраны. Функции межсетевых экранов

### Основные типы межсетевых экранов

### Способы подключения межсетевых экранов

### Виртуальные частные сети

### Виды виртуальных частных сетей

### Протокол SSL/TLS. Применение и основные положения протокола

### Протокол SKIP. Применение и основные положения протокола

### Протокол IPSec. Применение и основные положения протокола

### Протокол SET. Применение и основные положения протокола