Криптографические методы защиты информации

История развития. Современное состояние. Перспективы.

Исторически сложившиеся подходы к защите информации при ее передаче

- Физические методы (охрана, технические средства, нестандартные средства связи) **защищенные каналы**
- Стеганографические методы (сокрытие факта передачи информации) **скрытые каналы**
- Криптографические методы (использование шифров) **открытые каналы**

Различие между шифрованием и кодированием

- **Кодирование** – жесткое правило замены одних символов другими, предназначенное для удобства хранения и передачи информации
- **Шифрование** – правило замены одних символов другими, предполагающее использование ключа, предназначенное для сокрытия смысла передаваемой и хранимой информациии

Правило Керкгоффса

«… компрометация системы не должна причинять неудобств корреспондентам…»

Жан-Вильгельм-Губерт-Виктор-Франсуа-Александр-Огюст Керкгоффс ван Ньювенгоф

«Военная криптография». Конец 19 века.

Стойкость (надежность) шифра определяется только секретностью ключа.

Постулаты разработки криптосистем

Противник может иметь в своем распоряжении:

- ***Алгоритм***
- ***Шифратор***
- ***Образцы*** шифрованных и открытых ***сообщений***

и при этом не должен иметь возможности:

- **Восстановить применяемый *ключ***
- **Установить *содержание* остальных криптограмм**

…располагая ***средствами***, не превышающими ***стоимость*** защищаемой информации, за ***время*** в течение которого эта информация ***актуальна***.

Теория секретной связи Клода Шеннона (1944 г.)

- Концепция ***избыточности открытого текста*** и переноса ее в шифртекст.
- ***Теоретическая и практическая стойкость***. Мера теоретической стойкости – энтропийная характеристика неопределенности шифра по открытому сообщению (расстояние единственности). Мера практической стойкости – рабочая характеристика шифра. (Временные затраты, количество операций, сложностные оценки вскрытия.)
- Принцип ***рассеивания и перемешивания***. Рассеивание – зависимость шифрованного текста от открытого текста и ключа должна быть сложной и неочевидной. Каждый элемент ключа и открытого текста должны влиять на каждый элемент шифрованного текста.

В России этими проблемами занимались А. А. Марков, Б. Б. Пиотровский, А. Н. Колмогоров. Множество их трудов до сих пор засекречено.

Математические модели шифров

Пусть:

i и *j* – номера шифрвеличины/шифробозначения и ключа
C, *p* и *k* – шифрвеличина, шифробозначение и ключ
E и *D* – операции шифрования и расшифрования

Модель де Виари
для шифра Виженера:

$$C_i = E(p_i) = (p_i + k_j) \bmod 26$$
$$P_i = D(C_i) = (C_i - k_j) \bmod 26,$$

Модель де Виари
для шифра Бофора:

$$C_i = E(p_i) = (k_j - p_i) \bmod 26$$
$$p_i = D(C_i) = (k_j - C_i) \bmod 26,$$

Модель шифра Вернама:

$$C_i = E(p_i) = p_i \oplus k_j$$
$$p_i = D(C_i) = c_i \oplus k_j$$

$\oplus$ - операция XOR.

При $j \to \infty$ и равновероятном *k* – имеем совершенный шифр Дж. Моборна

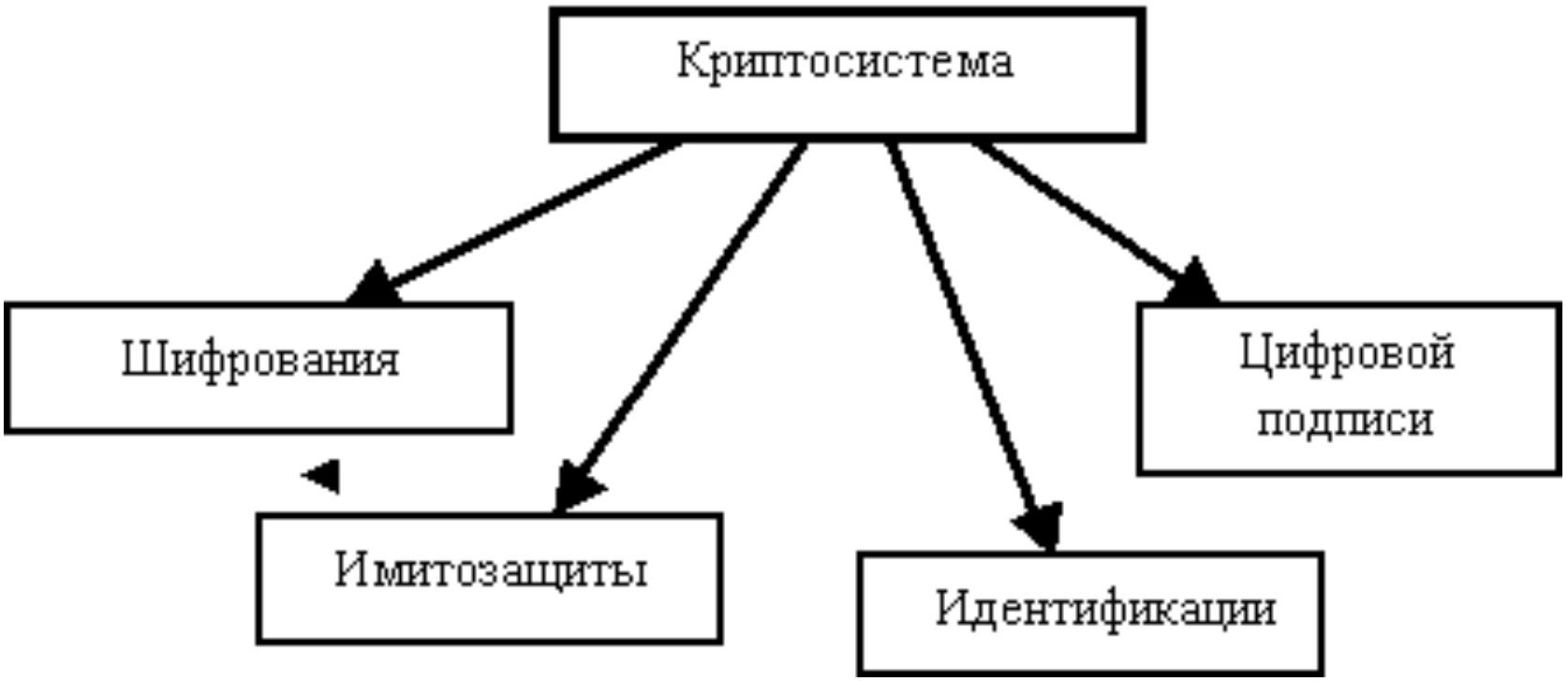
Методы криптографии

- Криптографические алгоритмы:
  - Классическое шифрование
    - Поточные алгоритмы, криптографические генераторы
    - Блочные алгоритмы
  - Шифрсистемы с открытым ключом
    - RSA, шифрование на эллиптических кривых
  - Криптографические хэш-функции и пр.
- Криптографические протоколы:
  - Аутентификация
  - Обмен ключами
  - Разделение секрета и пр.

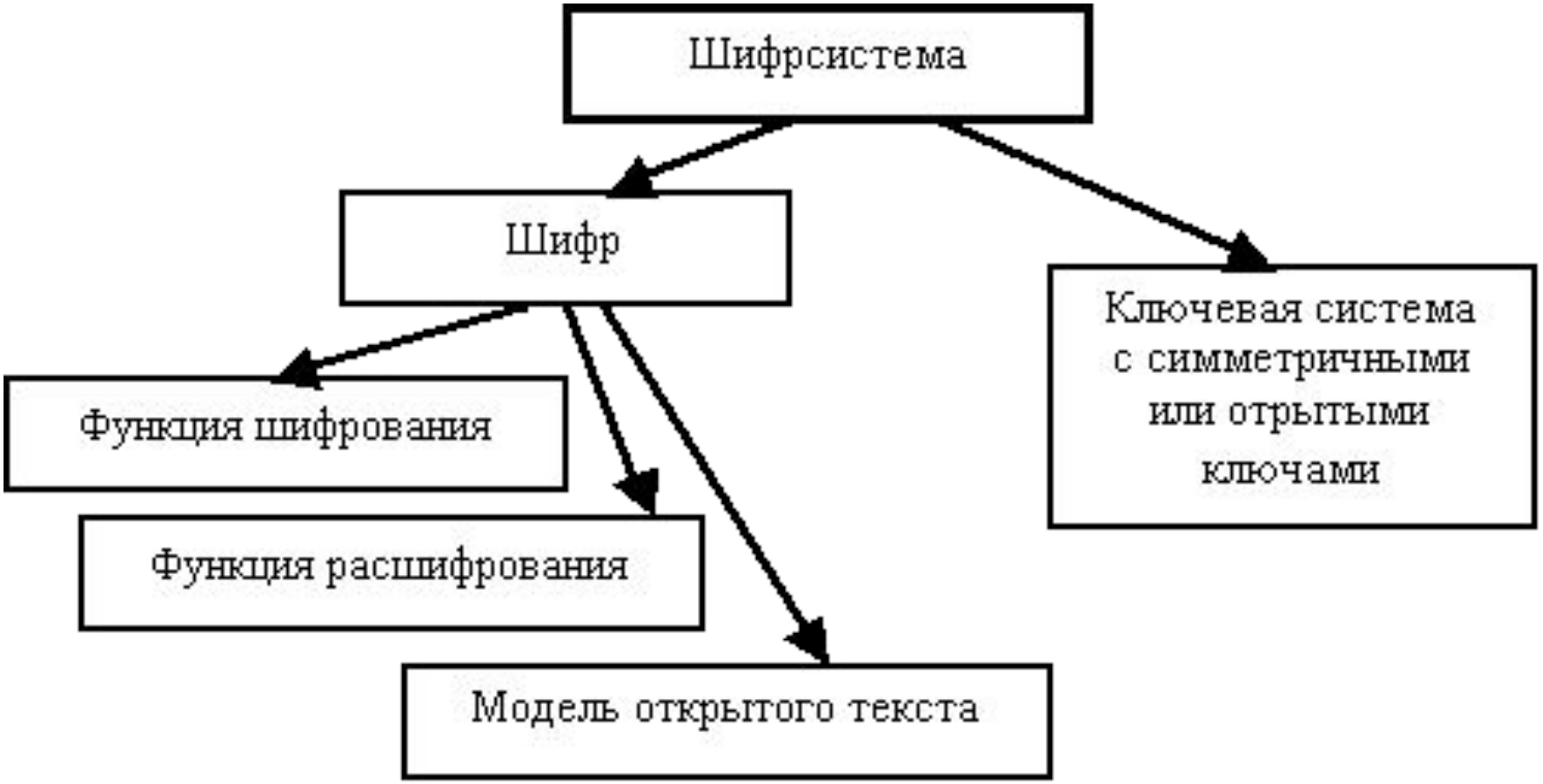
Категории защиты информации обеспечиваемые современными криптографическими методами

Категория защиты	Виды атак	Средства обеспечения
Конфиденциальность	Перехват, раскрытие содержимого, анализ потока данных.	Симметричные и асимметричные шифры
Целостность	Модификация	Ключевые и бесключевые хеш-функции
Доступность	Прерывание, постановка помех	*Алгоритмы помехоустойчивого кодирования*
Аутентичность	Фальсификация	MAC-коды, алгоритмы ЭЦП
Апеллируемость	Отказ от авторства, приписывание авторства	Алгоритмы и протоколы электронно-цифровой подписи (ЭЦП)

Классификация криптосистем



Состав шифрсистемы



Классификация шифров

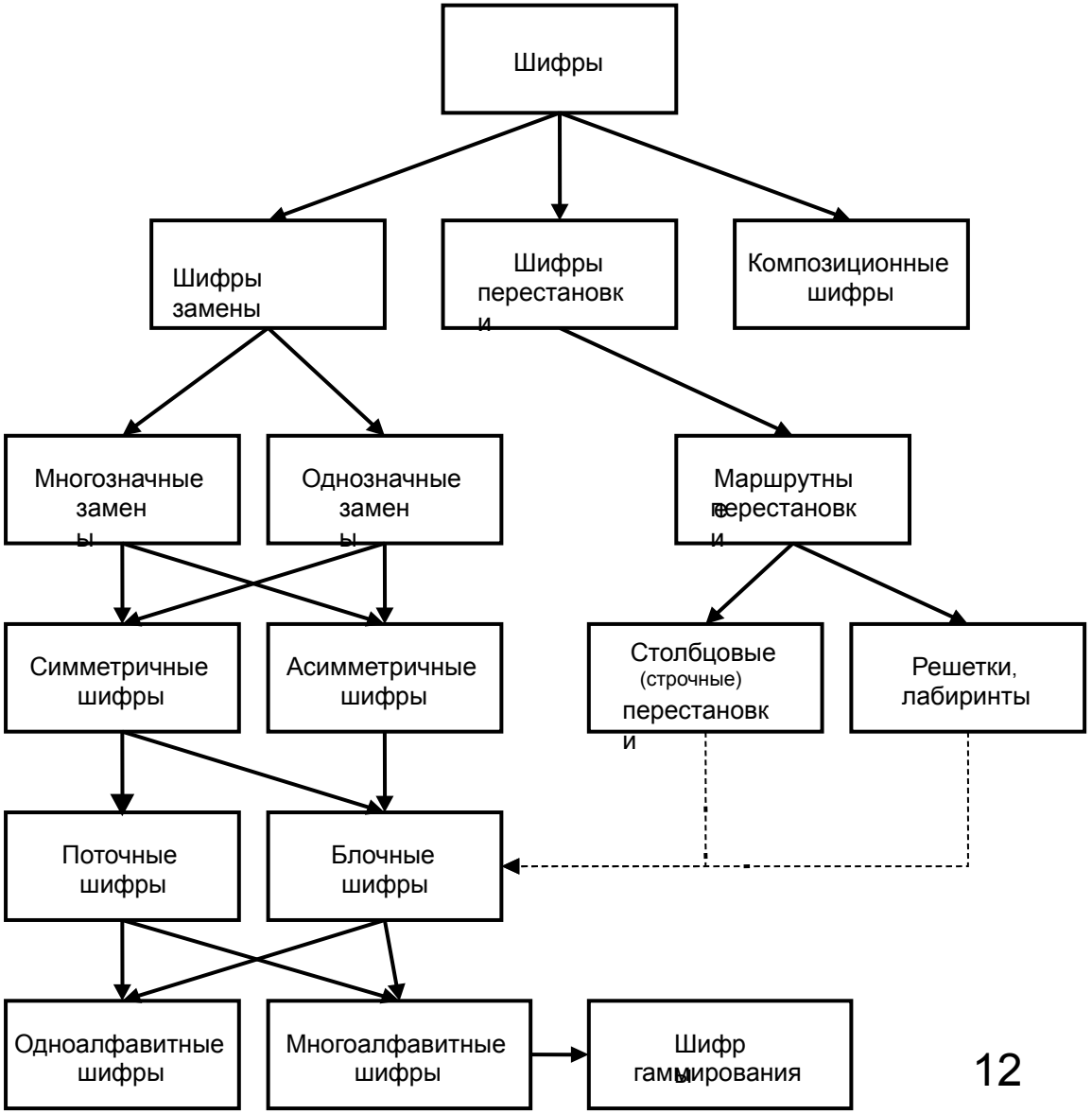
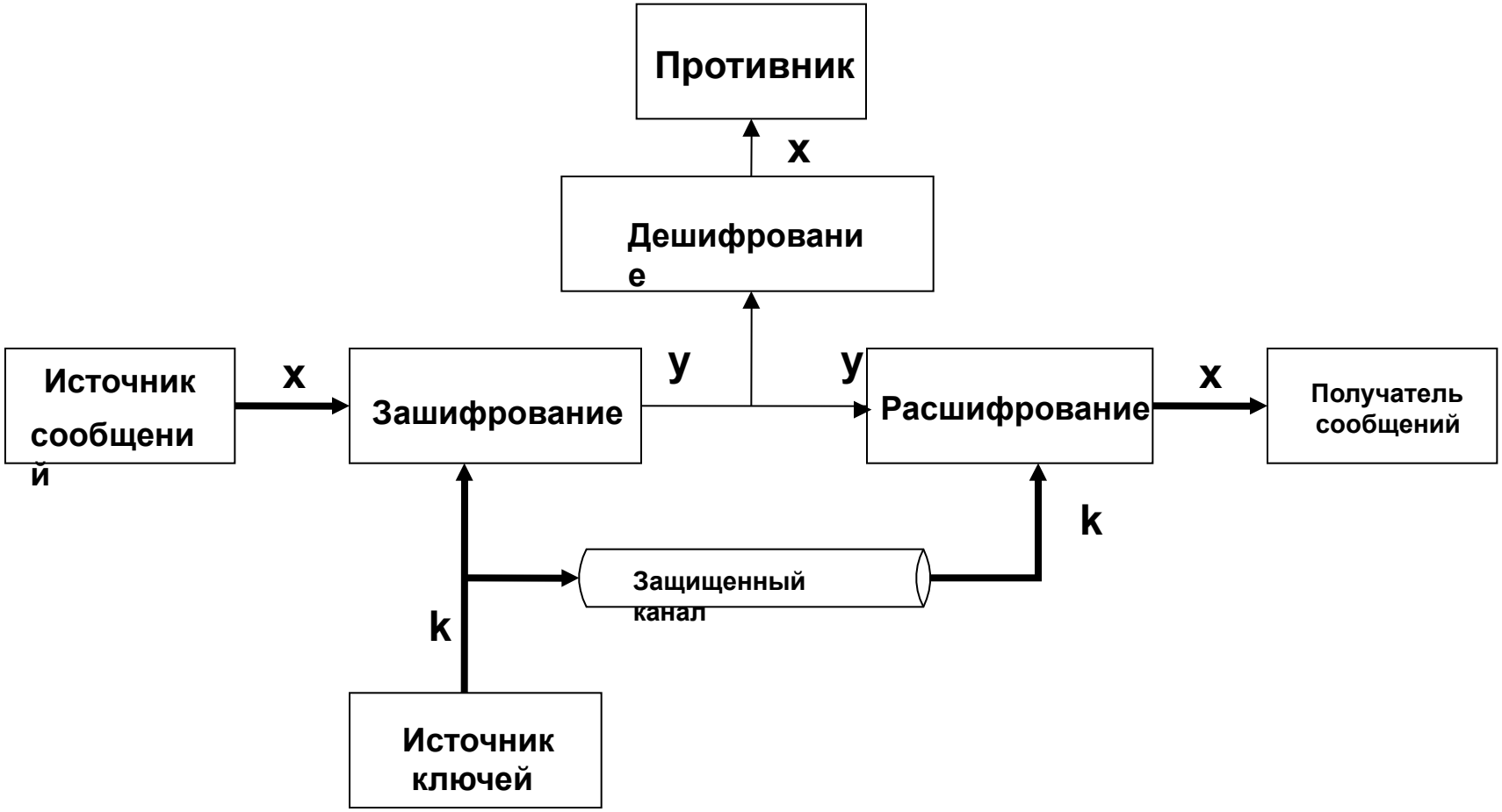
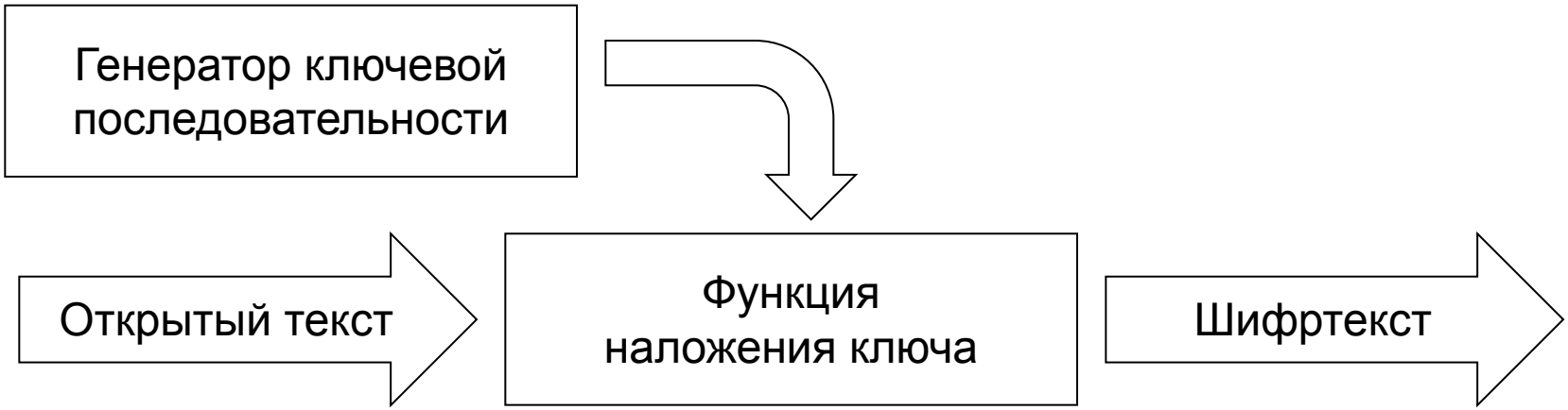


Схема симметричного шифрования



Поточные алгоритмы



- На основе датчиков (генераторов) ИСП
- На основе датчиков (генераторов) ПСП

  - На основе регистров сдвига с линейной обратной связью РСЛОС.

  - На основе регистров сдвига с обратной связью по переносу РСОСП.

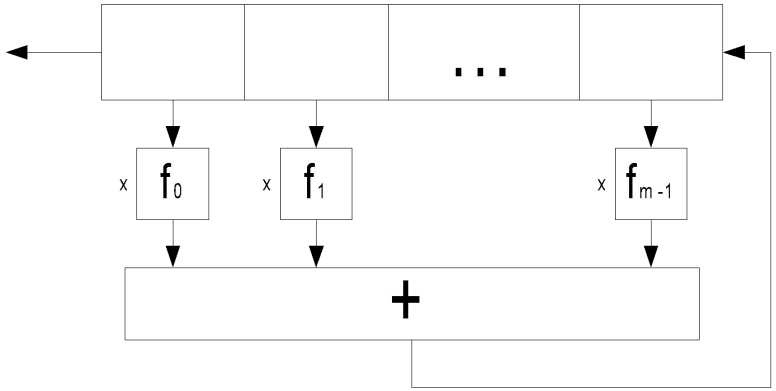
Генераторы ИСП

- На основе шумящих диодов
- На основе счетчика Гейгера
- Программные реализации по статистике нажатия клавиш на клавиатуре.
- На основе таймера компьютера
- Таблицы случайных чисел

Основное назначение – **генерация ключей и одноразовых блокнотов**.

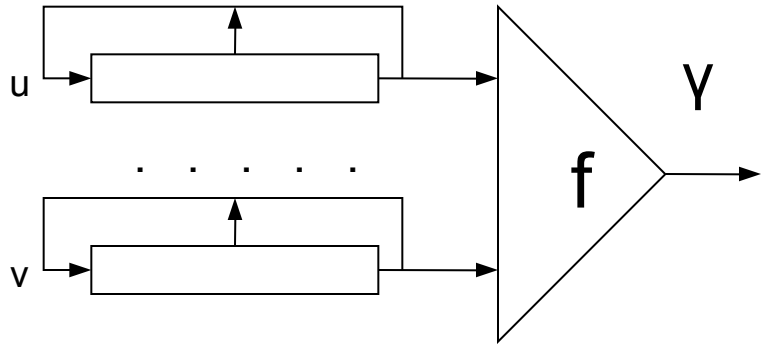
Генераторы ПСП

РСЛОС



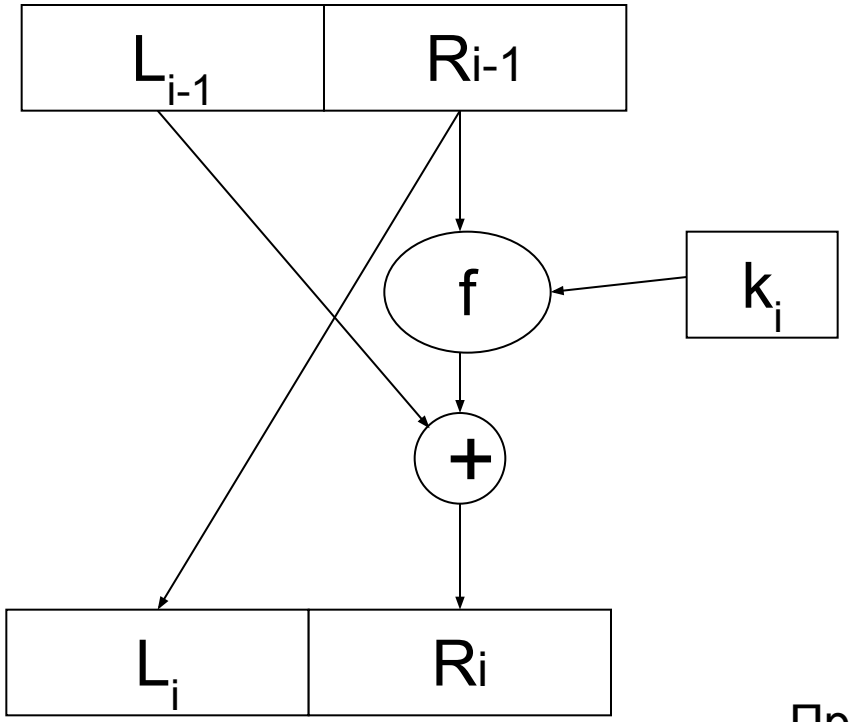
$$u(i+m)=\sum_{j=0}^{m-2} f_j \cdot u(i+j), i \geq 0$$

Комбинирующий генератор



$$f(x_1 \ldots x_t)=\sum_{k=1}^{t} \sum_{1 \leq i_1 < \ldots < i_k < t} C_{i_1 \ldots i_k} \cdot x_{i_1} \cdot \ldots \cdot x_{i_k}$$

Блочные алгоритмы (сеть Файстеля)



Зашифрование:

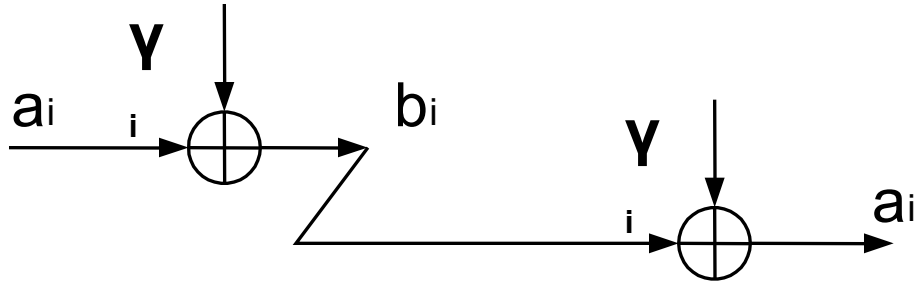
$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f_i(R_{i-1}, k_i) \end{cases}$$

Расшифрование:

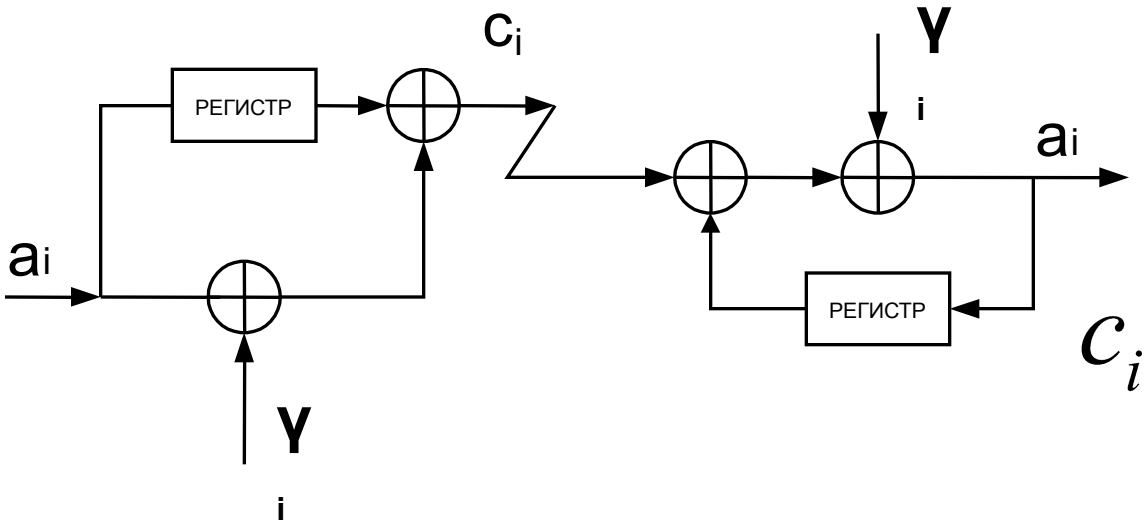
$$\begin{cases} L_{i-1} = R_i \oplus f_i(R_{i-1}, k_i) \\ R_{i-1} = L_i \end{cases}$$

Преобразование обратимо даже при использовании необратимой функции f

Режимы работы шифров



$$b_i = a_i \oplus \gamma_i$$

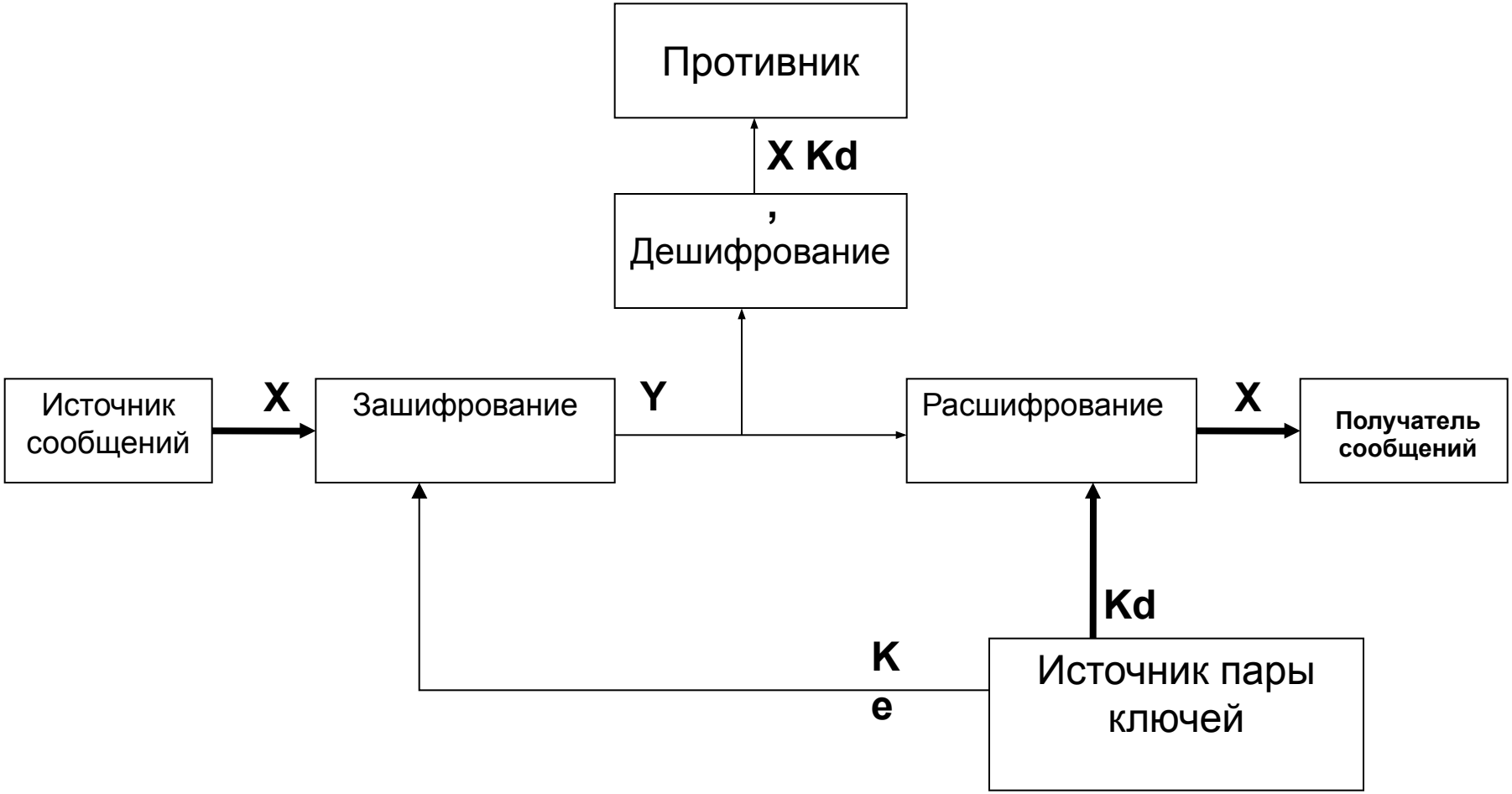


$$c_i = a_i \oplus \gamma_i \oplus a_{i-1}$$

Сравнительная характеристика блочных и поточных шифров

Блочные шифры	**Поточные шифры**
Работают во всех режимах шифрования	Поддерживают не все режимы шифрования
Тяжелы для математического анализа	Простое проектирование и математический анализ.
Легко реализуются как аппаратно, так и программно	Практически непригодны к программной реализации для битового потока.
Имеют не очень высокое быстродействие	Имеют высокое быстродействие
Стойкость шифра зависит от длины ключа, количества раундов шифрования, размера блока и рассеивающих и перемешивающих характеристик алгоритма.	Стойкость шифра зависит от статистических характеристик и периода переполнения генератора ключевой последовательности

Схема шифрования с открытым ключом



Основные методы построения ассиметричных криптосистем

- Использование однонаправленных функций
- Использование однонаправленных функций с секретом
- Использование маскировки вычислительно простых задач под вычислительно сложные
- Использование кодов, исправляющих ошибки

Однонаправленная функция

Функция f: $U \rightarrow V$, обладающая двумя свойствами:

1. Для любого аргумента $u \in U$ существует алгоритм вычисления значения $f(u)$ полиномиальной сложности.
2. Не существует алгоритма инвертирования f (решения уравнения $f(x) = v$ относительно $x \in U$), имеющего полиномиальную сложность.

Кандидаты на однонаправленную функцию

1. Умножение натуральных чисел:

   $f(a,b) = a \cdot b,\ a,b \in \mathbf{N}$

Обратная задача: $\mathbf{n = a \cdot b}$ (задача факторизации)

Модульное экспоненцирование с фиксированным основанием и модулем:

$f_{a,n}: Z_n \rightarrow Z_n$, где $f_{a,n}(m) = a^m \bmod n,\ a,m,n \in Z$

Обратная задача: $a^x = b \bmod n$ (задача дискретного логарифмирования)

3. Скалярное умножение точек эллиптической кривой над конечным полем.

Однонаправленная функция с лазейкой (секретом) k

Функция f_k: $U \rightarrow V$, обладающая двумя свойствами:

1. Для любого аргумента $u \in U$ существует алгоритм вычисления значения $f_k(u)$ полиномиальной сложности.
2. При неизвестном k не существует полиномиального алгоритма инвертирования f_k.
3. При известном k существует полиномиальный алгоритм инвертирования f_k.

Кандидат на однонаправленную функцию с секретом

Модульное экспоненцирование с фиксированной степенью и модулем:

$g_{a,n}: Z_n \rightarrow Z_n$, где $g_{a,n}(m)=a^m \bmod n$, $a,m,n \in Z$

Обратная задача: $x^m = b \bmod n$ (вычисления корня степени *m* по модулю *n*)

Секрет – разложение числа *n*.

Реализовано в системе **RSA**

Криптосистема ЭЦП

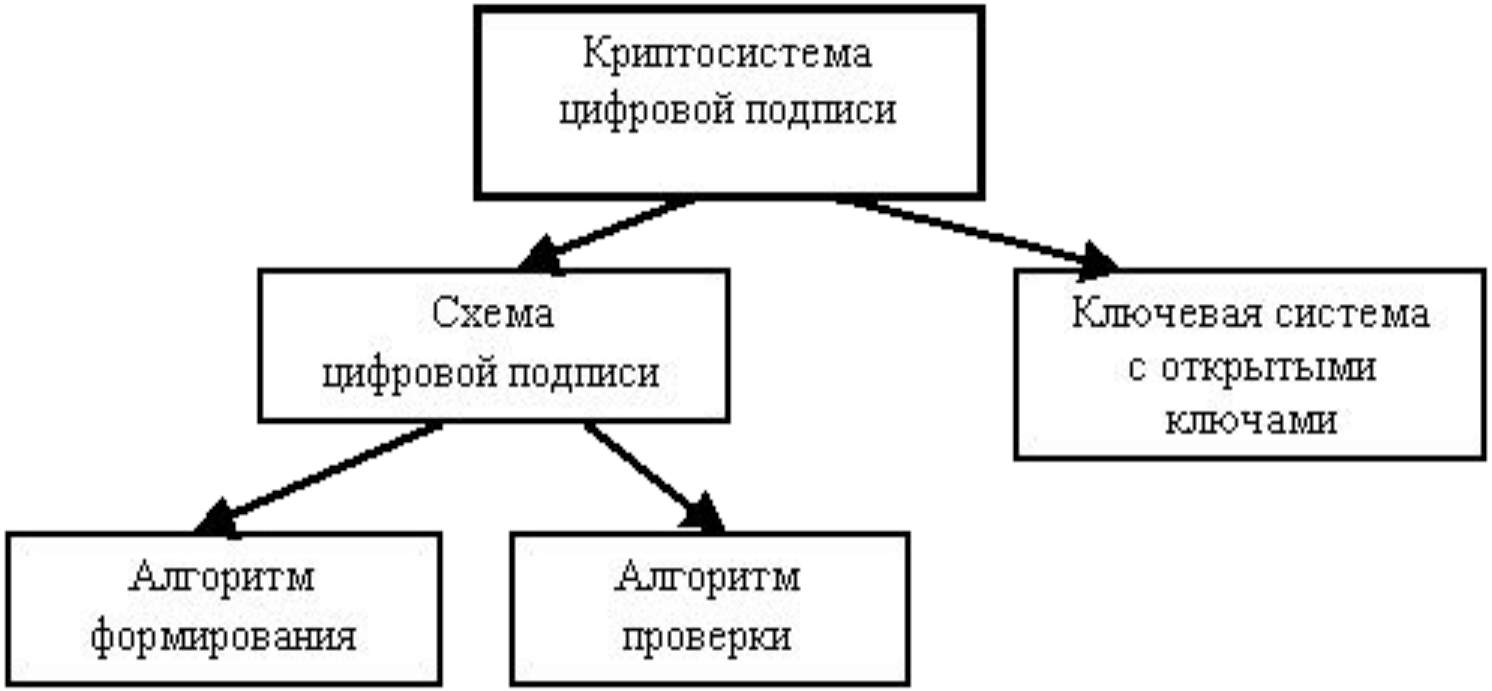
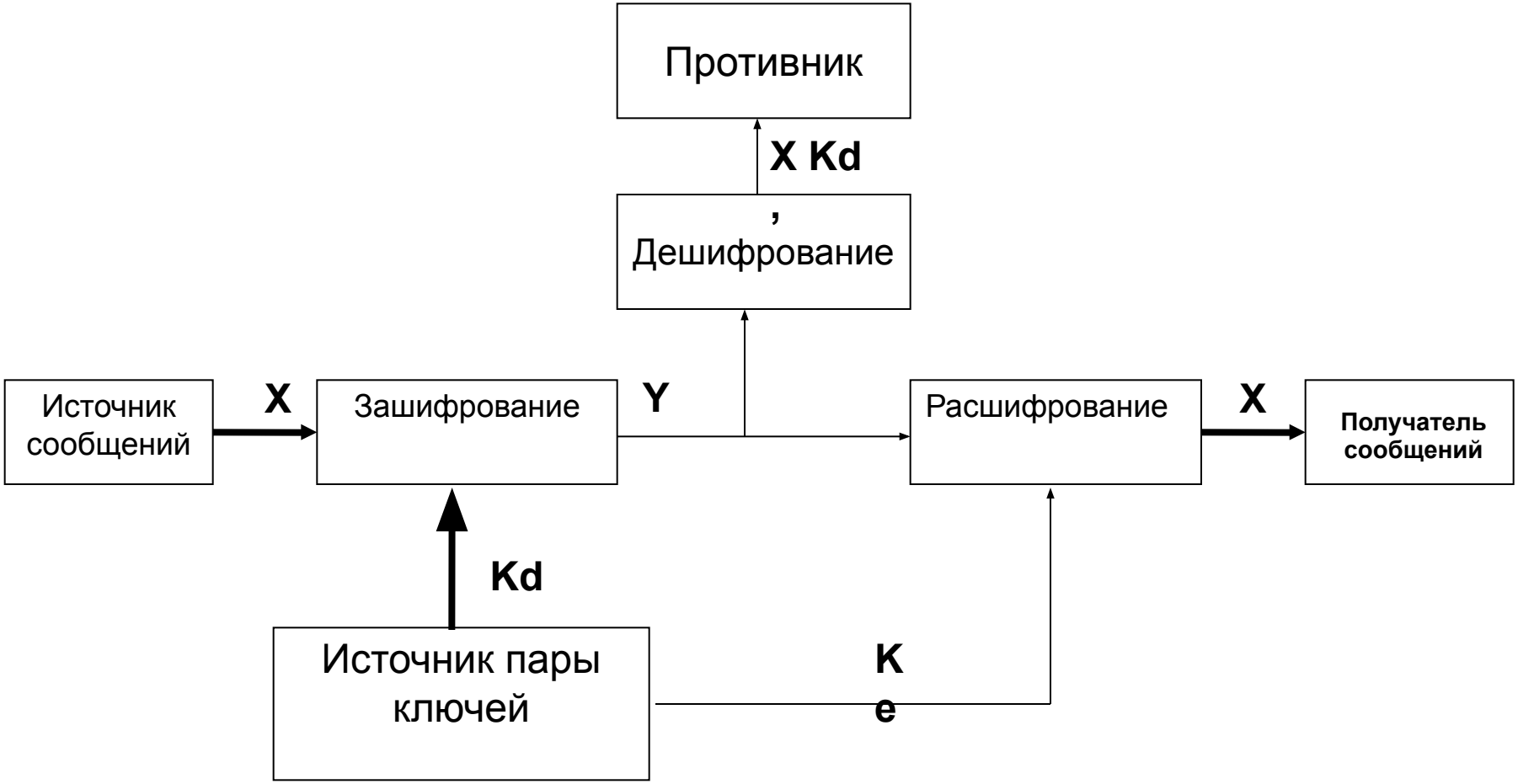


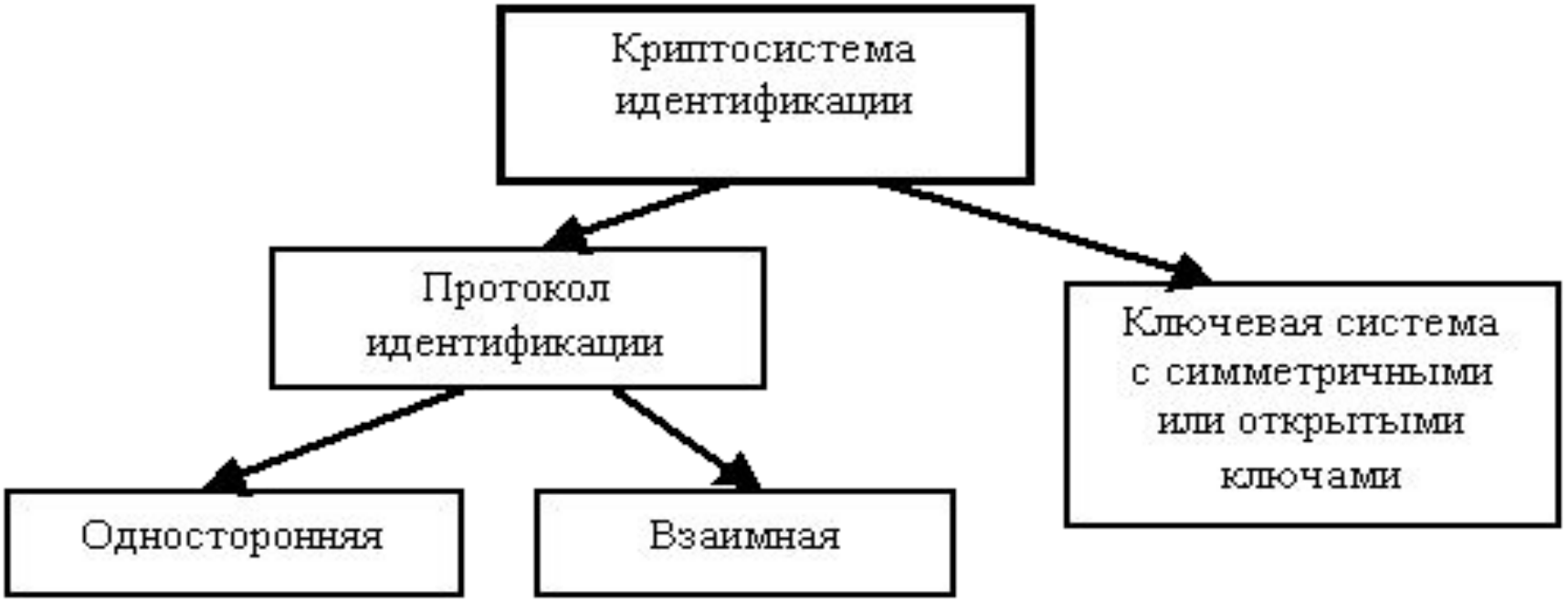
Схема ЭЦП


Противник
X Kd
,
Дешифрование
Источник сообщений
X
Зашифрование
Y
Расшифрование
X
Получатель сообщений
Kd
Источник пары ключей
K
e

Сравнение электронной и собственноручной подписей

Собственноручная подпись	Электронно-цифровая подпись
Не зависит от подписываемого текста, всегда одинакова	Зависит от подписываемого текста, всегда разная
Неразрывно связана с подписывающим лицом, однозначно определяется его психофизическими свойствами, не может быть утеряна	Определяется секретным ключом, принадлежащим подписывающему лицу, может быть утеряна владельцем
Неотделима от носителя, бумаги, поэтому отдельно подписывается каждый экземпляр документа	Легко отделима от документа и поэтому верна для всех его копий
Не требует для реализации дополнительных механизмов	Требует дополнительных механизмов, реализующих алгоритмы ее вычисления и проверки
Не требует создания поддерживающей инфраструктуры	Требует создания доверенной инфраструктуры сертификатов открытых ключей

Криптосистема идентификации



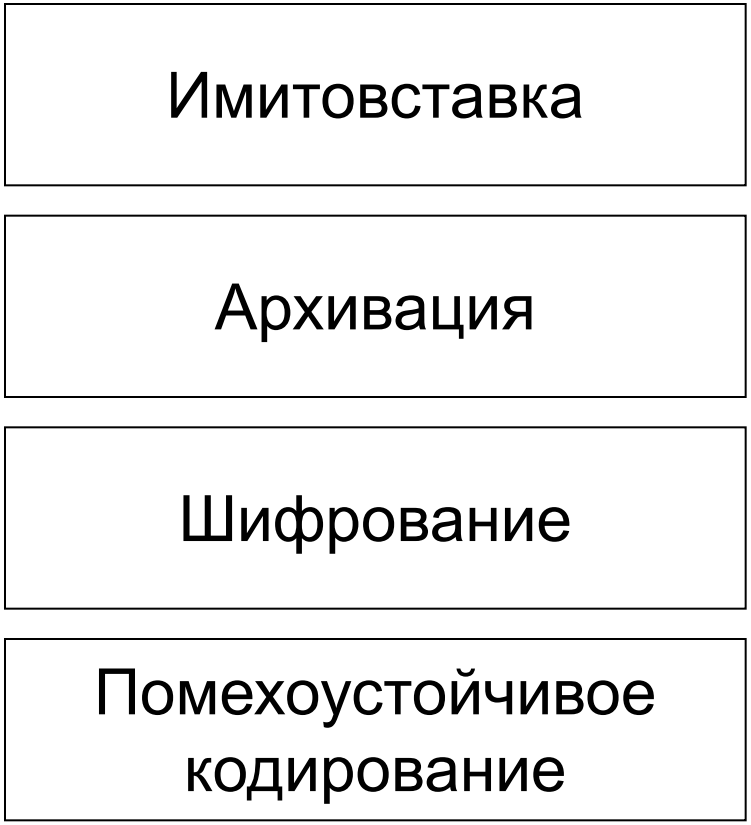
Криптографические хэш-функции

Хэш-функцией называется всякая функция $h: X \rightarrow Y$,
легко вычислимая и такая, что для любого сообщения M
значение $h(M) = H$ *(свертка)* имеет фиксированную битовую длину.

Ключевые Называются *кодами аутентификации сообщений (КАС) (message authentication code (MAC)).*
Дают возможность без дополнительных средств гарантировать как правильность источника данных, так и целостность данных в системах с доверенной средой.
Применяются в системах с симметричными ключами.

Бесключевые. Называются *кодами обнаружения ошибок (modification detection code (MDC) или manipulation detection code, message integrity code (MIC)).*
Дают возможность с помощью дополнительных средств (например, шифрования, использования защищенного канала или цифровой подписи) гарантировать целостность данных.
Могут применяться в системах как с доверенной, так и не доверенной средой.

Порядок подготовки сообщения к передаче



Криптографические протоколы

Виды криптографических протоколов:

- Протоколы с посредником
- Протоколы с арбитром
- Самодостаточные протоколы

Задачи, решаемые протоколами:

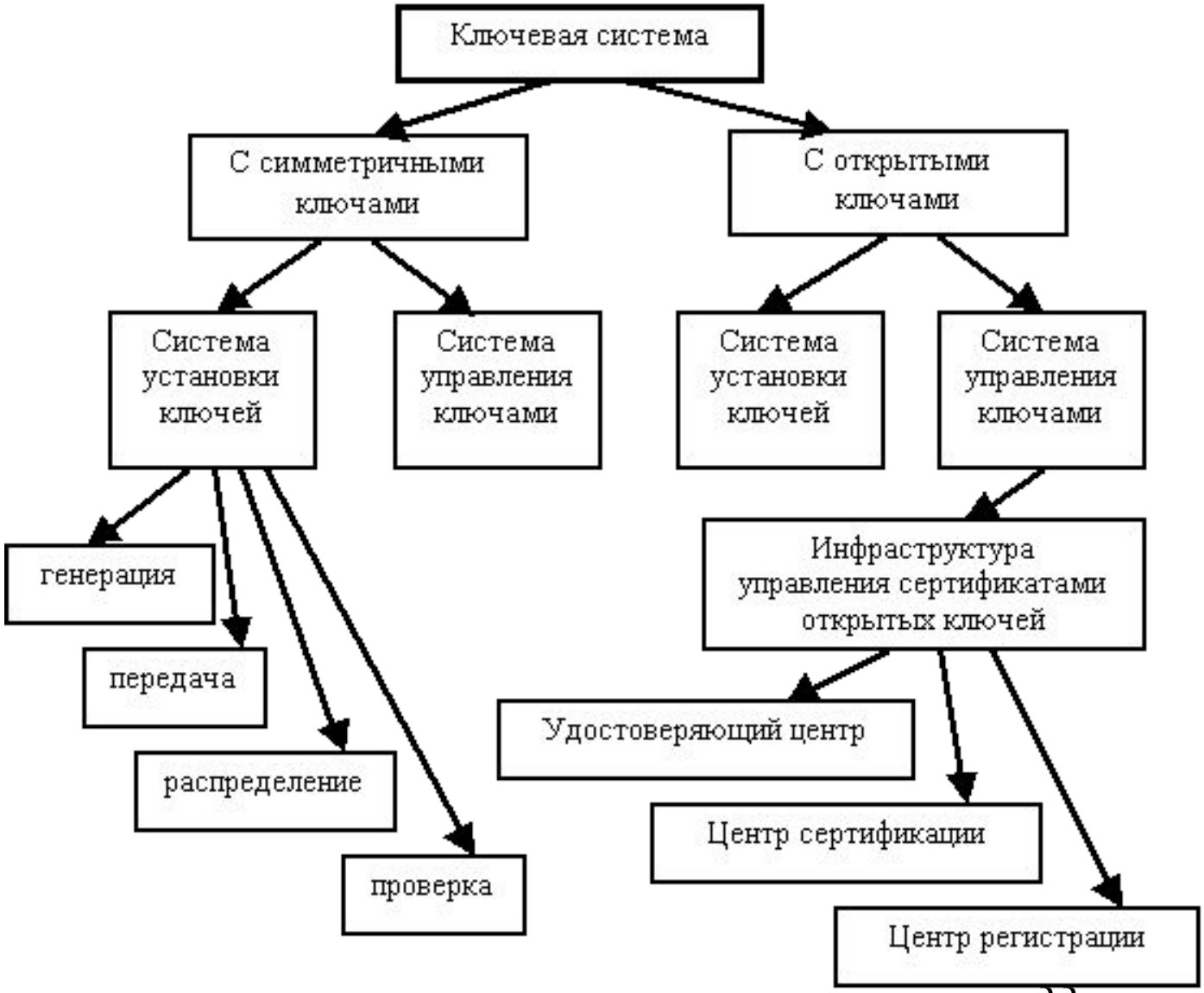
Основные протоколы: Обмен ключами и распределение ключей, аутентификация, разделение секрета.

Промежуточные протоколы: неоспоримые цифровые подписи, метки времени, групповые подписи, подбрасывание монеты по телефону, мысленный покер и пр.

Развитые протоколы: доказательства с нулевым разглашением, одновременное подписание контракта, передача с забыванием, одновременный обмен секретами, подписи вслепую и пр.

Эзотерические протоколы: тайное голосование, цифровые деньги, тайные многосторонние вычисления и пр.

Ключевые системы



Отечественные криптографические стандарты

- **ГОСТ 28147-89** (Алгоритм блочного шифрования)
- **ГОСТ Р 34.10-95, -2001** (Алгоритм цифровой подписи на основе шифрования с открытым ключом)
- **ГОСТ Р 34.11-95** (Криптографическая хэш-функция на основе алгоритма блочного шифрования)

Методы криптоанализа

- **Статистические** (исторические шифры)
- **Дифференциальные** (блочные шифры)
- **Бесключевого чтения** (поточные шифры)
- **Линейные** (блочные и поточные шифры)
- **Вероятностные** (шифрсистемы с открытым ключом)
- **Прямые** (все виды шифров)

Перспективные направления в криптографии

- **Вероятностное шифрование**

Основная цель – устранение утечки информации в криптосистемах с открытым ключом

- **Квантовая криптография**

Основная идея – создание канала связи, в котором невозможно прослушивание без нарушения в передаче (поляризованные фотоны)