**Этап 1. Идентификация криптосистемы:**

- по доступности информации о криптоалгоритме;

* Криптосистемы ограниченного использования √
* Криптосистемы общего использования

- по числу ключей;

- бесключевые

- одноключевые

- двухключевые

- многоключевые √

- по стойкости криптоалгоритма;

- безусловно стойкие

- доказуемо стойкие – наверное это, <https://eprint.iacr.org/2018/426> , возможно нужен доп анализ

- предположительно стойкие ?

- по используемым средствам шифрования;

- программные√

- аппаратные

- программно-аппаратные

- по наличию сертификата.

- сертифицированные√

- несертифицированные

**Этап 2. Определение потенциальных взломщиков**

- по технической оснащенности;

- персональный компьютер

- сеть ЭВМ

- суперкомпьютер

- по конечной цели;

- обнаружение слабости в алгоритме

- полный взлом алгоритма

- по доступу к шифрующим средствам;

- “внутренний” нарушитель

- “внешний” нарушитель

- по уровню подготовки;

- взаимодействие с компьютером на уровне пользователя

- математический аппарат

- программирование

- электротехника и физика

- социальная инженерия

- по первичной информации о средстве шифрования;

- пользователь

- криптограф

- “клептограф”

- по возможности кооперации.

- одиночка

- коллектив

Наиболее вероятные типы взломщиков:  
Взломщик 1:

* B1: Сеть ЭВМ
* B2: Полный взлом алгоритма
* B3: "Внешний" нарушитель
* B4: Программирование
* B5: Криптограф
* B6: Коллектив

Взломщик 2:

* B1: Персональный компьютер
* B2: Обнаружение слабости в алгоритме
* B3: "Внутренний" нарушитель
* B4: Математический аппарат
* B5: Пользователь
* B6: Одиночка

**Этап 3. Определения множества атак.**

- по доступу к открытому и зашифрованному тексту;

- только шифротекста

- открытого текста

- подобранного открытого текста

- адаптивно подобранного открытого текста

- информации из побочных каналов

- по контролю над процессом шифрования;

- пассивные

- активные

- имитация сообщения

- подмена сообщения

- по исходу атаки

- полный взлом

- глобальная дедукция

- частичная дедукция

- информационная дедукция

- по объему необходимых ресурсов;

- память

- время

- данные

- по степени применимости к различным шифрам;

- универсальные

- для определенной категории шифров

- для конкретного криптоалгоритма

- по используемым средствам;

- математические методы

- устройства-перехватчики физических параметров процесса шифрования

- эволюционное программирование

- квантовые компьютеры

- по последствиям атаки;

- нарушение конфиденциальности

- нарушение целостности

- нарушение доступности

- по возможности распараллеливания.

- распределенные

- не распределенные

Самые опасные атаки для ibpre

Атаки с выбором шифротекста (CCA):

* A1: выбор шифротекста
* A2: Активные, с имитацией и подменой сообщения
* A3: Память и время
* A4: универсальные A5: Математические методы
* A6: Нарушение конфиденциальности
* A7: Распределенные

Атаки с выбором открытого текста (CPA)

**Chosen Plaintext Attack (CPA)**:

* A1: Доступ к открытому тексту
* A2: Пассивные
* A3: Данные
* A4: Универсальные
* A5: Математические методы
* A6: Нарушение конфиденциальности
* А7: Не распределенные
* Атаки на побочные каналы
* A1: Информации из побочных каналов
* A2: Активные
* A3: Память, время и данные
* A4: Универсальные и для определенной категории шифров
* A5: Устройства-перехватчики физических параметров процесса шифрования
* A6: Нарушение конфиденциальности
  + A7: Распределенные.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A black background with white text

Description automatically generated