Введение

В настоящее время вопросы, связанные с достижением и поддержанием конфиденциальности, целостности, доступности информации и средств её обработки, объединяются понятием “информационная безопасность”.

Проблеме обеспечения информационной безопасности­ уделяется отдельное внимание как со стороны государств, так и в организациях различных масштабов, вне зависимости от сферы предоставления услуг и изготовления продукции. Для обеспечения информационной безопасности предприятия включают во множество сущестующих элементов и процессов систему защиты информации, которая, в свою очередь, также состоит из набора разнообразных компонентов. Такие системы охватывают организационный, правовой, программно-аппаратный и инженерно-технический аспекты деятельности организаций и в каждом из них поддерживают и улучшают работу сооответствующих механизмов.

**Правовой аспект** базируется на нормах информационного права и предполагает юридическое закрепление взаимоотношения между субъектами взаимоотношений в сфере информационной безопасности.

**Организационный аспект** включает в себя меры управленческого, ограничительного и технологического рода, определяющие политики и содержание системы защиты, регламентирующие соблюденеие персоналом правил защиты информации.

**Программно-аппаратный аспект,** в свою очередь, предназначен для защиты информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах.

**Инженерно-технический аспект** предназначен для активного и пассивного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью различных технических средств.

В рассмотрении вопросов, связанных с программно-аппаратными элементами системы зашиты, отдельную нишу занимает определение оптимальных и надежных средств крипотграфической защиты информации и каналов ее передачи. Защита данных при помощи криптографических инструментов – одно самых важных решений проблемы обеспечения их безопасности.

За многие годы в области криптографии было создано огромное количество механизмов для защиты информации: симметричные и асимметричные алгоритмы шифрования, протоколы элетронно-цифровой подписи, идентификации и аутентификации. Тем не менее, вслед за улучшением и созданием элементов защиты регулярно возникают все новые и новые методы атак на созданные технологии. Не смотря на негативную окраску данного явления, оно, безусловно, способствует дальнейшему развитию криптографических решений и продуктов, создаваемых на их основе.

Одним из классов атаков, направленным на [уязвимости](https://ru.wikipedia.org/wiki/Уязвимость_(компьютерная_безопасность)) в практической реализации [криптосистем](https://ru.wikipedia.org/wiki/Шифр) являются а**таки по сторонним** **каналам** (*Side channel attack*). Данные атаки используют информацию о физических процессах, протекающих в устройстве, на базе которого реалезуется криптографический алгоритм. Подобная побочная информация не рассматриваются в теоретических моделях алгоритмов. Не смотря на то, что подобные атаки были хорошо известны уже в [80-х годах](https://ru.wikipedia.org/wiki/1980-е), они получили широкое распространение только после публикации результатов, полученных [Полом Кохером](https://ru.wikipedia.org/w/index.php?title=Кохер,_Пол&action=edit&redlink=1) в [1996 году](https://ru.wikipedia.org/wiki/1996_год).

Атаки по сторонним каналам можно клпассифицировать несколькими способами. В зависимости от степени воздействия, атаки могут быть:

* Пассивные — атакующий получает необходимые данные без воздействия на криптосистему;
* Активные — атакующий реализует некоторое воздействие на криптосистему, в результате которого изменяется её поведение.

### Атака зондированием

Атака зондированием ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *probing attack*) — агрессивная пассивная простая атака. Для получения информации устройство вскрывается, с помощью [оптического микроскопа](https://ru.wikipedia.org/wiki/Оптический_микроскоп) исследуется [печатная плата](https://ru.wikipedia.org/wiki/Печатная_плата) и устанавливаются [щупы](https://ru.wikipedia.org/wiki/Щуп) на проводники, по которым идут сигналы, или же с помощью [микроскопа](https://ru.wikipedia.org/wiki/Микроскоп)[[9]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-9) исследуется состояние ячеек памяти.[[10]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Kommerling-10)[[11]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-11) Процесс упрощается при использовании зондирующей установки, включающей в себя микроскопы и [микроманипуляторы](https://ru.wikipedia.org/wiki/Манипулятор_(механизм)) для установки щупов на поверхности чипа. Такие установки используются в полупроводниковой промышленности для тестирования образцов продукции; цена на вторичном рынке составляет порядка 10000$.[[10]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Kommerling-10) Чтобы упростить наблюдение криптоаналитик обычно замедляет [тактовую частоту](https://ru.wikipedia.org/wiki/Тактовая_частота) работы устройства.[[12]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-12)

### Атаки по времени

Основная статья: [**Атака по времени**](https://ru.wikipedia.org/wiki/Атака_по_времени)

Атака по времени ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *timing attack*) — первая из широко известных атак по сторонним каналам, предложенная [Полом Кохером](https://ru.wikipedia.org/w/index.php?title=Пол_Кохер&action=edit&redlink=1) в [1996 году](https://ru.wikipedia.org/wiki/1996_год) [[13]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Kocher-13) и применённая на практике против алгоритма [RSA](https://ru.wikipedia.org/wiki/RSA) в [1998 году](https://ru.wikipedia.org/wiki/1998_год).[[14]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-14) Атака основана на предположении, что различные операции выполняются в устройстве за различное время, в зависимости от поданных входных данных. Таким образом, измеряя время вычислений и проводя статистический анализ данных, можно получить полную информацию о секретном [ключе](https://ru.wikipedia.org/wiki/Ключ_(криптография)).

Выделяют степени подверженности алгоритмов данному типу атак[[15]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-15):

* Атака невозможна на алгоритмы, операции которых выполняются за одинаковое число тактов на всех платформах: вращение, сдвиг и другие [битовые операции](https://ru.wikipedia.org/wiki/Битовые_операции) над фиксированным числом бит.
* Возможна атака на алгоритмы использующие сложение и вычитание.
* Особенно подвержены атакам по времени алгоритмы, использующие умножение, деление, возведение в степень и битовые операции над произвольным числом бит.

Одной из разновидностей атак по времени также являются атаки на [кэш](https://ru.wikipedia.org/wiki/Кэш) ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *cache-based attacks*). Данный тип атак основывается на измерениях времени и частоты промахов в [кэш процессора](https://ru.wikipedia.org/wiki/Кэш_процессора) и направлен на программные реализации шифров.[[16]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-16)

Атаки по времени также могут применяться удалённо. Так, например, известны атаки по [сети](https://ru.wikipedia.org/wiki/Компьютерная_сеть) на [сервера](https://ru.wikipedia.org/wiki/Сервер_(программное_обеспечение)) использующие [OpenSSL](https://ru.wikipedia.org/wiki/OpenSSL).[[17]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-17)

Из распространенных алгоритмов атаке по времени подвержены [DES](https://ru.wikipedia.org/wiki/DES), [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard),[[18]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Schindler-18) [IDEA](https://ru.wikipedia.org/wiki/IDEA), [RC5](https://ru.wikipedia.org/wiki/RC5).[[13]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Kocher-13)

### Атаки по ошибкам вычислений

Атака по ошибкам вычислений ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *fault–induction attack*) — активная атака. Основная идея — осуществление различных воздействий на шифратор с целью возникновения искажения информации на некоторых этапах шифрования. Управляя этими искажениями и сравнивая результаты на разных этапах работы устройства, криптоаналитик может восстановить секретный ключ. Изучение атак на основе ошибок вычислений обычно разделяется на две ветви: одна изучает теоретические возможности для осуществления различных ошибок в исполнении [алгоритма](https://ru.wikipedia.org/wiki/Алгоритм), другая исследует методы воздействия для реализации этих ошибок в конкретных устройствах.

#### Методы воздействия

Наиболее распространенные методы воздействия[[19]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Quisquater-19):

* Изменение напряжения [питания](https://ru.wikipedia.org/wiki/Источник_питания) криптосистемы. Отклонения в питании, сильно превышающие заданные производителем нормы, могут привести к ошибкам на определённых этапах работы, не мешая устройству в целом завершить процесс шифрования.[[20]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-20)
* Изменение конструкции шифратора (нарушение [электрических контактов](https://ru.wikipedia.org/wiki/Электрический_контакт)).
* Изменение тактовой частоты шифрующего устройства. При точном управлении отклонением [тактовой частоты](https://ru.wikipedia.org/wiki/Тактовая_частота) от заданной нормы можно добиться полного изменения выполнения [инструкций](https://ru.wikipedia.org/wiki/Машинный_код) в устройстве, вплоть до невыполнения выбранной инструкции.[[21]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Blomer-21) Такие атаки особенно применимы к [смарт-картам](https://ru.wikipedia.org/wiki/Смарт-карта), [тактовый сигнал](https://ru.wikipedia.org/wiki/Тактовый_сигнал) для которых задаётся внешним [генератором](https://ru.wikipedia.org/wiki/Генератор_тактовых_импульсов).
* Воздействие [лазерным лучом](https://ru.wikipedia.org/wiki/Лазер) или сфокусированным [световым пучком](https://ru.wikipedia.org/wiki/Световой_пучок). С помощью такого воздействия можно изменять состояние [ячеек памяти](https://ru.wikipedia.org/wiki/Ячейка_памяти) и влиять на [условные переходы](https://ru.wikipedia.org/wiki/Условный_переход) в исполнении кода.[[6]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Skorobogatov-6)
* Воздействие переменным [магнитным полем](https://ru.wikipedia.org/wiki/Магнитное_поле). Переменное магнитное поле вызывает в цепях устройства [вихревые токи](https://ru.wikipedia.org/wiki/Вихревые_токи), которые могут изменять состояние ячеек памяти.
* Помещение устройства в сильное [электромагнитное поле](https://ru.wikipedia.org/wiki/Электромагнитное_поле).
* Повышение [температуры](https://ru.wikipedia.org/wiki/Температура) некоторой части шифратора.

#### Типы ошибок

Атаки по ошибкам вычислений могут быть классифицированы по типу полученной ошибки[[19]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Quisquater-19):

* Постоянные или переменные ошибки. Постоянные ошибки влияют на всём времени исполнения алгоритма, например фиксирование значения в [памяти](https://ru.wikipedia.org/wiki/Компьютерная_память) или изменение пути прохождения [сигнала](https://ru.wikipedia.org/wiki/Сигнал). Переменные ошибки отражаются только на определённых этапах работы.
* Место возникновения ошибки: локальная ошибка, например изменения ячейки памяти, или ошибка в произвольном месте устройства, например атака с помощью электромагнитного поля.
* Время воздействия: некоторые атаки требуют применения воздействия в строго определённое время, как например изменения тактовой частоты, другие же позволяют осуществлять атаку в более широком диапазоне времени работы.
* Тип ошибки: смена значения [бита](https://ru.wikipedia.org/wiki/Бит), установка фиксированного значения, смена значения группы битов целиком, изменения потока исполнения команд и другие.

#### Примеры атак на ошибки вычислений

Атаки на основе ошибок вычислений изучаются с [1996 года](https://ru.wikipedia.org/wiki/1996_год)[[22]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Dohen-22) и с тех пор почти для всех алгоритмов была показана возможность взлома с помощью такого типа атак. Среди известных алгоритмов можно выделить:

* Атаки на [RSA](https://ru.wikipedia.org/wiki/RSA), использующие [китайскую теорему об остатках](https://ru.wikipedia.org/wiki/Китайская_теорема_об_остатках)[[22]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Dohen-22)[[23]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-23)
* [Дифференциальный криптоанализ](https://ru.wikipedia.org/wiki/Дифференциальный_криптоанализ) по ошибкам вычислений [DES](https://ru.wikipedia.org/wiki/DES)[[24]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-24)
* Криптоанализ [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard)[[21]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-Blomer-21)
* Дифференциальный криптоанализ систем, основанных на [эллиптических кривых](https://ru.wikipedia.org/wiki/Эллиптическая_кривая)[[25]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-25)

### Атаки по энергопотреблению

Атака по энергопотреблению ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *power analysis attack*) — пассивная атака, предложенная Полом Кохером в [1999 году](https://ru.wikipedia.org/wiki/1999_год).[[26]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-DPA-26) Суть данной атаки состоит в том, что в процессе работы шифратора криптоаналитик с высокой точностью измеряет [энергопотребление](https://ru.wikipedia.org/wiki/Электрическая_мощность) устройства и таким образом получает информацию о выполняемых в устройстве операциях и их параметрах. Так как питание устройства обычно предоставляется внешними [источниками](https://ru.wikipedia.org/wiki/Источник_питания), такая атака очень легко осуществима: достаточно поставить последовательно в цепь питания [резистор](https://ru.wikipedia.org/wiki/Резистор) и точно измерять [ток](https://ru.wikipedia.org/wiki/Сила_тока), проходящий через него. Другой способ — измерять изменения напряжения на выходах устройства в процессе шифрования.[[27]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-27)

Атаки по мощности отличаются высокой эффективностью с точки зрения затрат на криптоанализ. Так например простая атака по мощности ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *simple power analysis*) на [смарт-карту](https://ru.wikipedia.org/wiki/Смарт-карта) осуществима за несколько секунд, а некоторые варианты разностных атак по мощности ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *differential power analysis*) позволяют получить секретный ключ всего за 15 измерений.[[26]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-DPA-26)

### Атаки по электромагнитному излучению

Атака по электромагнитному излучению ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *electromagnetic analysis attacks*) — пассивная атака. Электронные шифрующие устройства излучают [электромагнитное излучение](https://ru.wikipedia.org/wiki/Электромагнитное_излучение) во время своей работы. Связывая определённые [спектральные компоненты](https://ru.wikipedia.org/wiki/Спектральная_линия) этого излучения с операциями выполняемыми в устройстве, можно получить достаточно информации для определения секретного ключа или самой обрабатываемой информации.

Примером этого вида атак является [перехват ван Эйка](https://ru.wikipedia.org/wiki/Перехват_ван_Эйка) осуществлённый в [1986 году](https://ru.wikipedia.org/wiki/1986_год). В дальнейшем атаки по электромагнитному излучению применялись к различным шифрам, таким как:

* [DES](https://ru.wikipedia.org/wiki/DES) и [RSA](https://ru.wikipedia.org/wiki/RSA)[[28]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-28)[[29]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-29)
* Реализации [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard)[[30]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-30) и криптосистем на [эллиптических кривых](https://ru.wikipedia.org/wiki/Эллиптическая_кривая)[[31]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-31) на [FPGA](https://ru.wikipedia.org/wiki/FPGA)
* Использования [криптографических хэш-функций](https://ru.wikipedia.org/wiki/Криптографическая_хеш-функция) [HMAC](https://ru.wikipedia.org/wiki/HMAC)[[32]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-32)

### Акустические атаки

Основная статья: [**Акустический криптоанализ**](https://ru.wikipedia.org/wiki/Акустический_криптоанализ)

Акустическая атака ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *acoustic attack*) — пассивная атака, направленная на получение информации из звуков производимых устройством. Исторически данный тип атак связывается с прослушкой работы [принтеров](https://ru.wikipedia.org/wiki/Принтер) и [клавиатур](https://ru.wikipedia.org/wiki/Клавиатура),[[33]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-33) но в последние годы были найдены уязвимости позволяющие использовать акустические атаки направленные на внутренние компоненты электронных шифраторов.[[34]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-34)

### Атаки по видимому излучению

Атака по видимому излучению ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *visible light attack*) — пассивная атака, предложенная Маркусом Куном в [2002 году](https://ru.wikipedia.org/wiki/2002_год).[[35]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-35) В своей работе он показал, что используя высокоточный датчик [интенсивности](https://ru.wikipedia.org/wiki/Интенсивность_(физика)) света можно измерить изменения в интенсивности рассеянного от [монитора](https://ru.wikipedia.org/wiki/Монитор_(устройство)) света, и таким образом восстановить изображение на экране.[[36]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-36) Данный тип атак также можно применить к шифраторам использующим [светодиодные индикаторы](https://ru.wikipedia.org/wiki/Светодиод), анализируя данные от которых можно получить информацию об операциях в устройстве.[[37]](https://ru.wikipedia.org/wiki/Атака_по_сторонним_каналам" \l "cite_note-37)