Почему компьютер может выдать секрет без взлома: как работают атаки по побочным каналам

Дата публикации: 03.08.2026

Когда речь заходит о кибератаках, большинство людей представляют себе взлом паролей, вирусы, программы-вымогатели или проникновение хакеров в компьютерные сети. Однако существует совершенно иной класс атак, при котором злоумышленнику не нужно взламывать систему или обходить защиту. Иногда достаточно внимательно наблюдать за тем, как работает сам компьютер.

Такие методы получили название атак по побочным каналам (Side Channel Attacks). Они считаются одними из самых необычных направлений современной кибербезопасности, поскольку используют не ошибки в программах, а физические особенности работы электронных устройств.

Представьте себе запертый сейф. Даже если преступник не знает код и не может открыть замок, он может попытаться внимательно прислушаться к едва заметным щелчкам механизма при вращении диска. Иногда подобные звуки позволяют понять, что происходит внутри замка. Компьютеры ведут себя

похожим образом: во время работы они постоянно оставляют множество косвенных "следов", которые в определенных условиях способны раскрыть конфиденциальную информацию.

Такими следами могут быть время выполнения вычислений, изменение энергопотребления, электромагнитное излучение, микроскопические задержки доступа к памяти, изменение частоты процессора или даже едва различимый шум электронных компонентов.

Сам компьютер не пытается передать эти сведения наружу. Они возникают как побочный эффект его нормальной работы. Но если злоумышленник умеет правильно анализировать такие сигналы, он может постепенно восстановить защищенные данные, например криптографические ключи, содержимое памяти или информацию о действиях пользователя.

Идея подобных атак появилась задолго до появления современных облачных сервисов. Еще в середине 1980-х годов голландский исследователь Вим ван Эк показал, что изображение с компьютерного монитора можно восстановить, принимая его слабое электромагнитное излучение специальной аппаратурой. Экран ничего не передавал намеренно, но физические процессы внутри устройства создавали своеобразную "утечку".

Настоящий прорыв произошел в конце 1990-х годов, когда специалисты по криптографии обнаружили, что даже математически надежные алгоритмы шифрования могут быть уязвимы из-за особенностей работы оборудования.

Исследователь Пол Кохер продемонстрировал, что продолжительность выполнения криптографических операций может зависеть от используемого секретного ключа. Если очень точно измерять время работы устройства, постепенно становится возможным восстановить конфиденциальную информацию.

Позже было доказано, что аналогичным образом можно анализировать и энергопотребление электронных устройств. Даже небольшие колебания электрического тока способны рассказать опытному исследователю о том, какие вычисления выполняет процессор в данный момент.

Эти открытия полностью изменили представление специалистов о компьютерной безопасности. Оказалось, что мало разработать надежный алгоритм шифрования — необходимо еще обеспечить, чтобы его работа не оставляла физических следов, пригодных для анализа.

Сегодня существует несколько основных разновидностей подобных атак. Наиболее известны анализ времени выполнения операций, измерение

энергопотребления, исследование электромагнитного излучения, анализ акустических сигналов и изучение особенностей работы памяти, процессоров и накопителей.

Особенно интересными оказались акустические атаки. В одном из экспериментов исследователи смогли восстановить 4096-битный криптографический ключ, анализируя едва слышимый высокочастотный шум, который издавал ноутбук во время выполнения операций шифрования. Для человека эти звуки практически незаметны, однако чувствительная аппаратура способна различать мельчайшие изменения.

Широкую известность атаки по побочным каналам получили в 2018 году после публикации двух крупнейших аппаратных уязвимостей — Spectre и Meltdown.

Обе проблемы были связаны со спекулятивным выполнением инструкций — технологией, благодаря которой современные процессоры заранее пытаются предугадать дальнейшие действия программы и начинают выполнять вычисления еще до получения окончательных команд. Именно этот механизм позволяет современным компьютерам работать значительно быстрее.

Однако исследователи обнаружили, что подобные предварительные вычисления оставляют небольшие изменения в состоянии процессора и кэш-памяти. Анализируя эти изменения, вредоносная программа могла получить доступ к данным, которые должны были оставаться полностью изолированными.

Эти открытия заставили производителей процессоров пересмотреть многие архитектурные решения, существовавшие десятилетиями.

На этом развитие атак не остановилось. В 2022 году специалисты обнаружили уязвимость Hertzbleed, показавшую, что даже автоматическое изменение тактовой частоты процессора способно стать источником утечки информации. В некоторых условиях этого оказалось достаточно, чтобы дистанционно получать сведения о криптографических операциях удаленного сервера.

В 2023 году внимание специалистов привлекли уязвимости Downfall и Zenbleed. Первая затронула некоторые процессоры Intel, вторая — процессоры AMD поколения Zen 2. В обоих случаях речь шла о возможности случайного появления данных одного процесса в памяти другого, что потенциально позволяло нарушить изоляцию программ.

Современные исследования уже давно вышли за пределы центральных процессоров. Сегодня специалисты изучают графические ускорители,

твердотельные накопители, оперативную память, сетевые адаптеры и даже браузеры.

Одним из наиболее необычных примеров последних лет стала атака GPU.zip. Она показала, что особенности обработки изображений графическим процессором способны в определенных ситуациях раскрывать отдельные элементы содержимого других веб-страниц.

Еще более неожиданным оказалось исследование GoFetch, опубликованное в 2024 году. Оно продемонстрировало, что некоторые процессоры Apple могут непреднамеренно раскрывать криптографические секреты из-за интеллектуального механизма прогнозирования обращения к памяти.

Последней заметной разработкой стала атака FROST. Она использует особенности работы современных SSD-накопителей и механизма хранения данных внутри браузера. Если несколько программ одновременно обращаются к одному накопителю, возникают едва заметные задержки, напоминающие автомобильную пробку на дороге. Анализируя подобные микрозадержки, исследователи показали возможность получения косвенной информации о действиях пользователя, например о посещаемых сайтах или работающих приложениях.

К счастью, большинству обычных пользователей не стоит опасаться подобных атак в повседневной жизни. Они чрезвычайно сложны, требуют высокой квалификации, дорогостоящего оборудования или специфических условий эксплуатации системы. Гораздо чаще злоумышленники используют значительно более простые методы: фишинговые письма, вредоносные программы, кражу паролей, эксплуатацию программных ошибок и программы-вымогатели.

Тем не менее значение атак по побочным каналам трудно переоценить. Они помогают исследователям обнаруживать фундаментальные недостатки архитектуры современных вычислительных систем задолго до того, как ими воспользуются преступники. Именно благодаря таким исследованиям производители процессоров, операционных систем, браузеров и криптографических библиотек постоянно совершенствуют механизмы защиты.

Для обычного пользователя главный вывод достаточно прост. Современный компьютер способен раскрывать информацию не только из-за ошибок программного обеспечения, но и благодаря особенностям собственной работы. Поэтому безопасность сегодня зависит не только от надежных паролей или антивируса, но и от того, насколько тщательно инженеры учитывают мельчайшие физические процессы, происходящие внутри электронных устройств. Именно такие исследования позволяют создавать компьютеры нового

поколения, которые будут не только быстрее, но и значительно безопаснее.