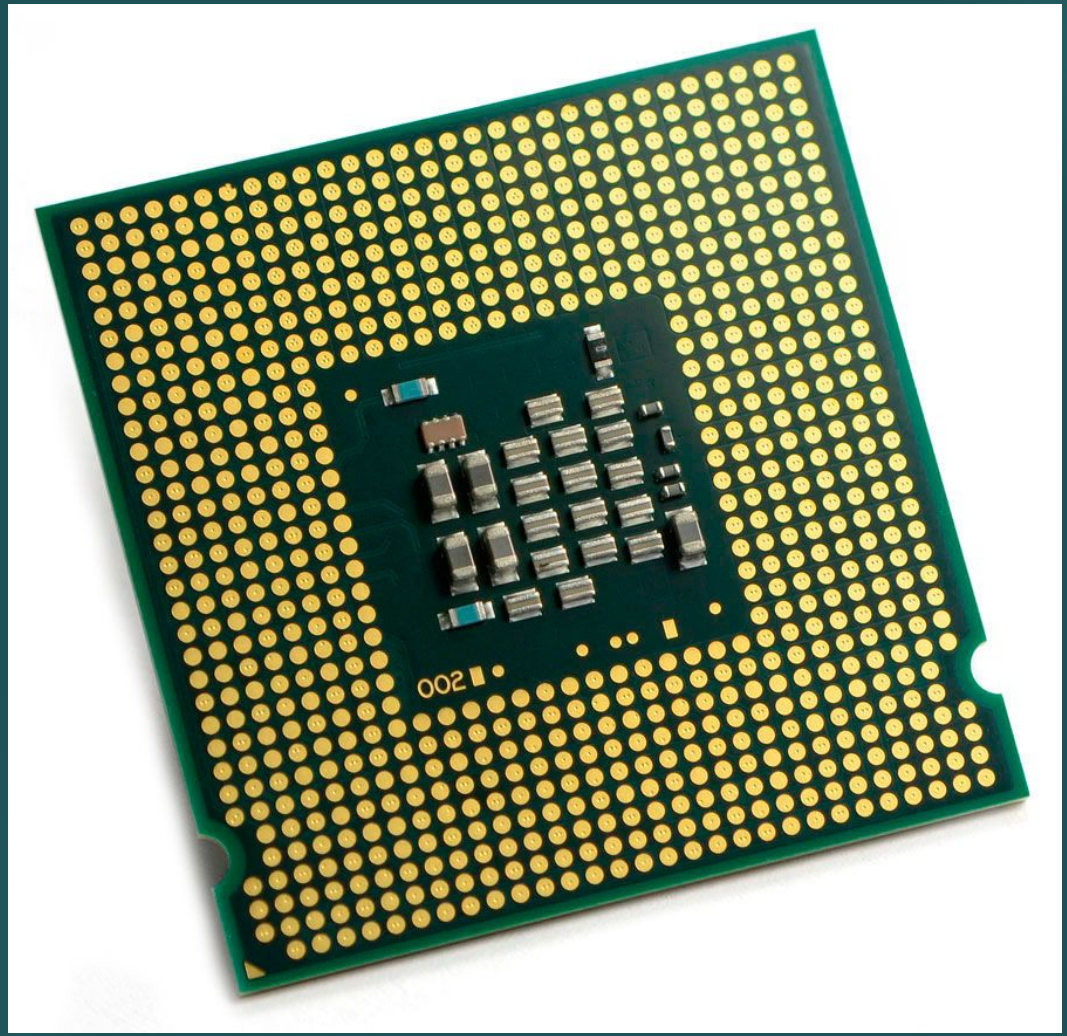
Темная сторона цифрового мира
О массовой уязвимости процессоров Intel

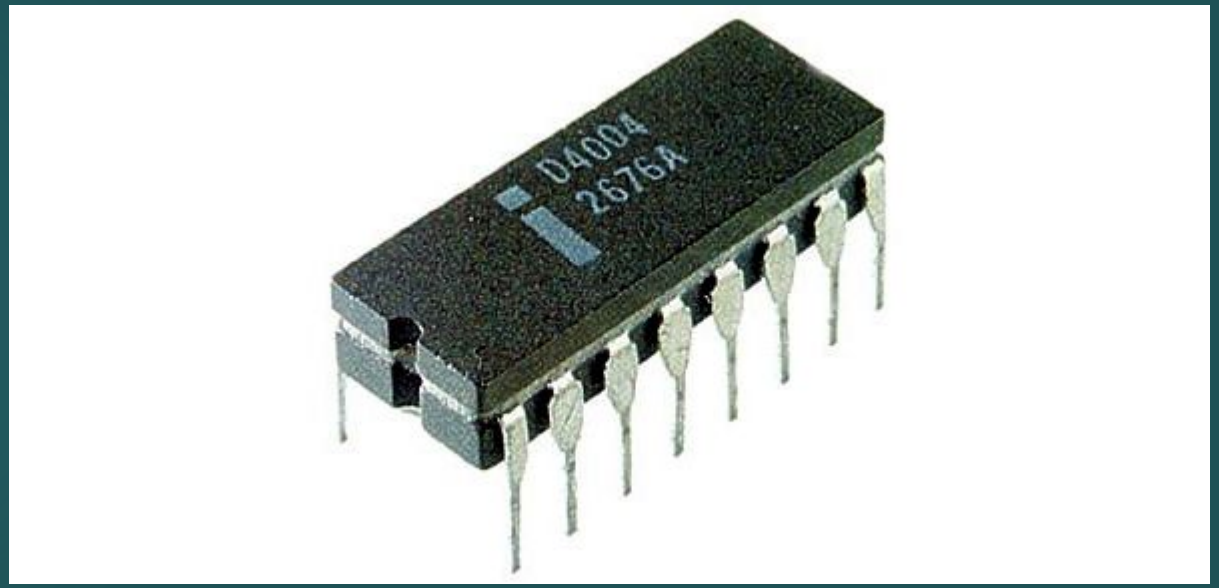
9-3

РАХМАНКУЛОВ Э.
МОЛОДЦОВ Г.
ФЕДОТОВА Е.
ГАВРИЛОВ И.

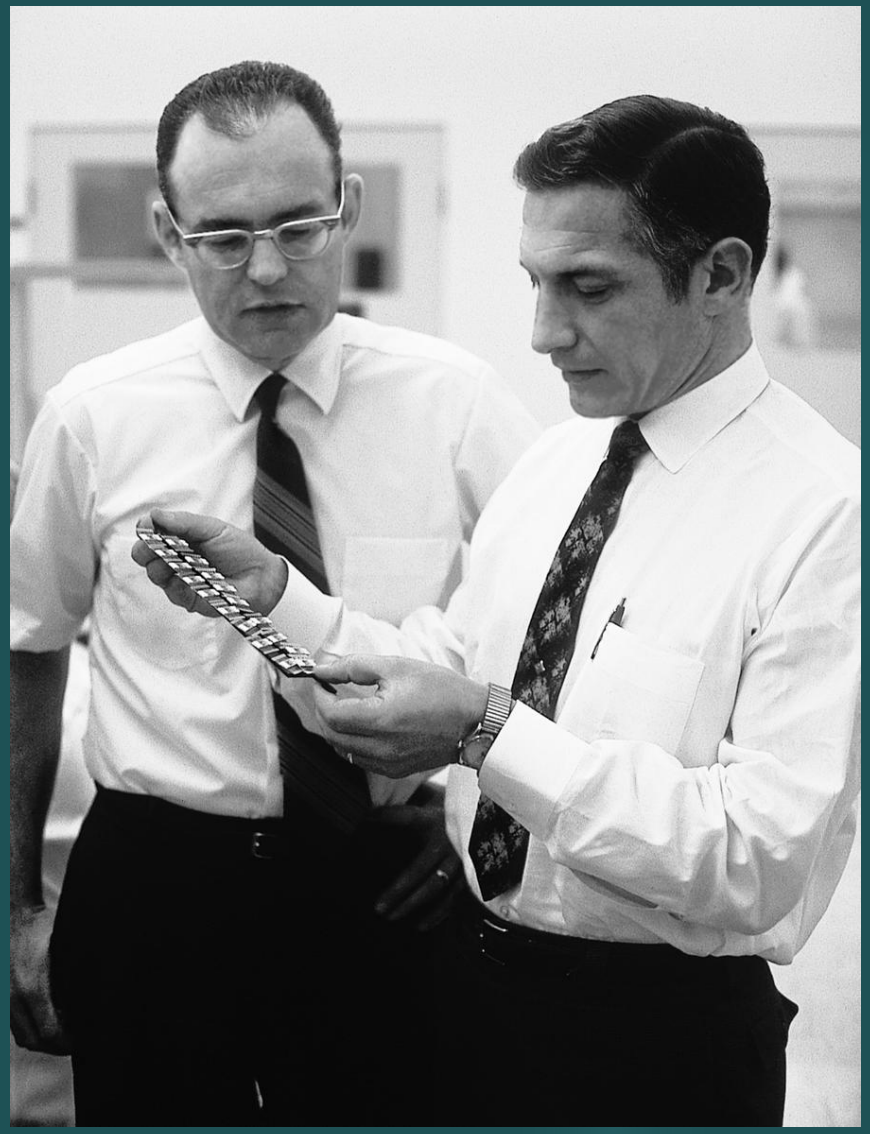


Центральный процессор – это часть компьютера, выполняющая заданные программой преобразования информации и осуществляющая управление всем вычислительным процессом.

- Переход к микропроцессорам позволил создать персональные компьютеры
- Первым общедоступным микропроцессором был 4-разрядный Intel 4004
- По данным компании IDC, по итогам 2009 года на рынке микропроцессоров для настольных ПК, ноутбуков и серверов доля корпорации Intel составила 79,7 %



Роберт Нойс совместно с Гордоном Муром-основатели корпорации Intel (1968).

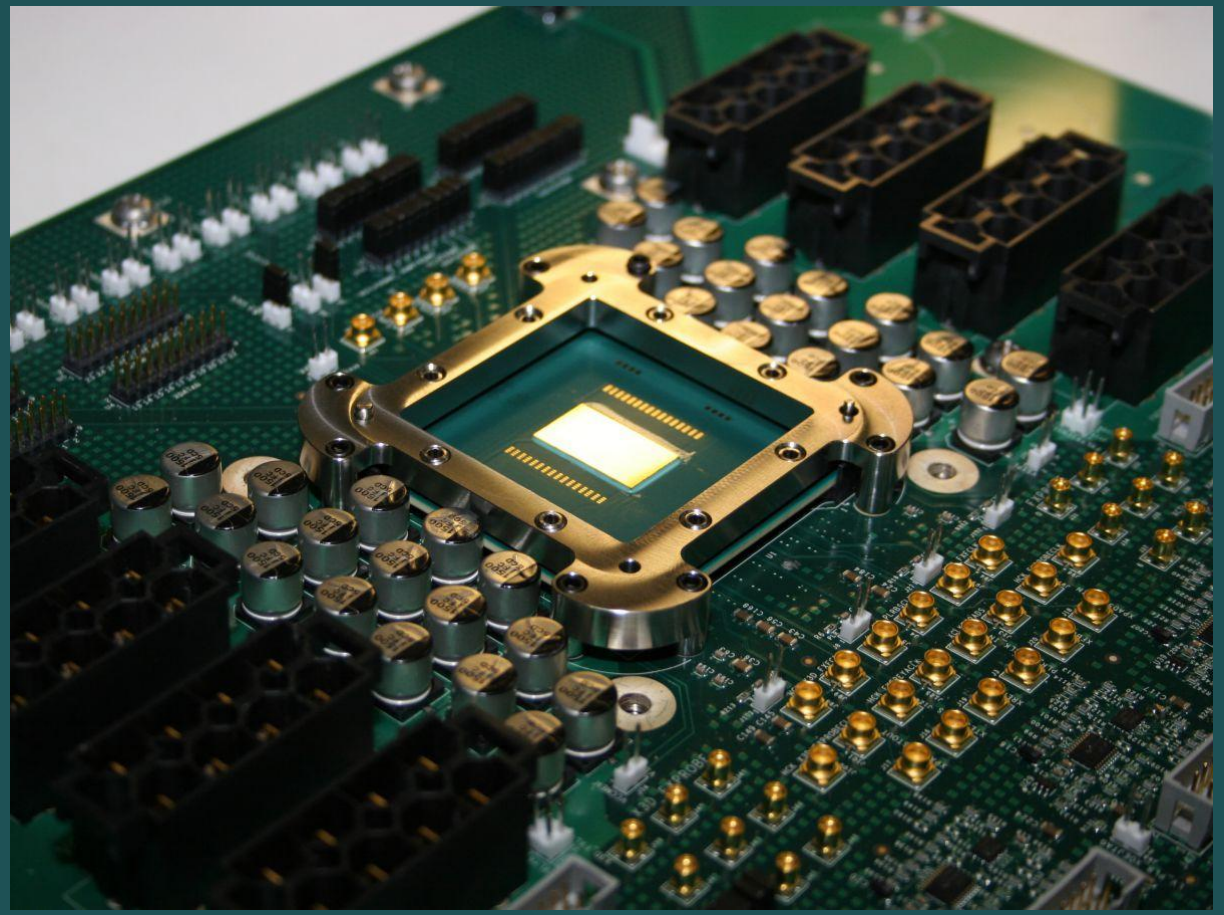


Однако, в 21 веке, под угрозой взлома находится, пожалуй, всё, что связано с технологиями. К сожалению, процессоры не являются исключением, и могут быть атакованы

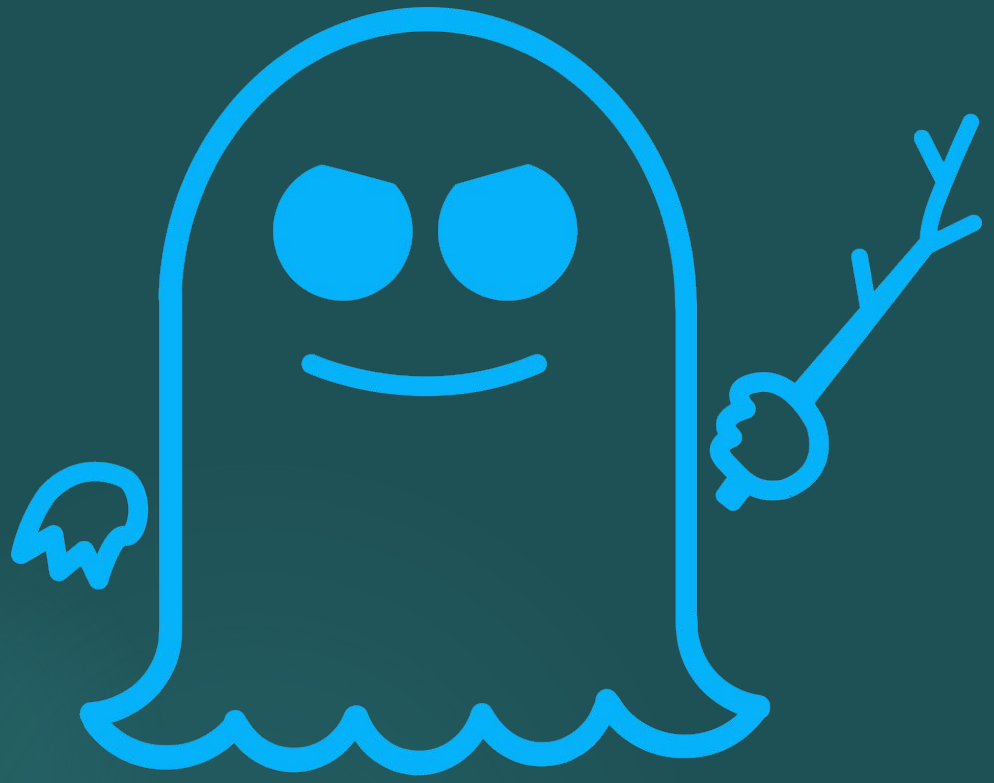
Возможность атаки порождается тремя механизмами, позволяющими ускорить работу процессора:

- Спекулятивное выполнение операций, в том числе чтение из оперативной памяти без проверки прав доступа процесса к читаемым областям.
- Отсутствия очистки кэша от результатов ошибочного спекулятивного исполнения (подобная очистка, вероятно, снизила бы скорость работы процессора).

- Ядро операционной системы держит свои данные в адресном пространстве процесса, защищая их от доступа уровнем привилегий. Данная технология позволяет быстрее исполнять системные вызовы. При таких вызовах повышается уровень привилегий, а при возврате обратно уровень привилегий снова понижается, при этом не требуется перезагружать таблицу страничных дескрипторов.



В случае Meltdown речь идёт о краже данных у самого ядра операционной системы, самого защищённого программного компонента, куда никто вторгаться не имеет права. Но так как уязвимости аппаратные, сделать это возможно.



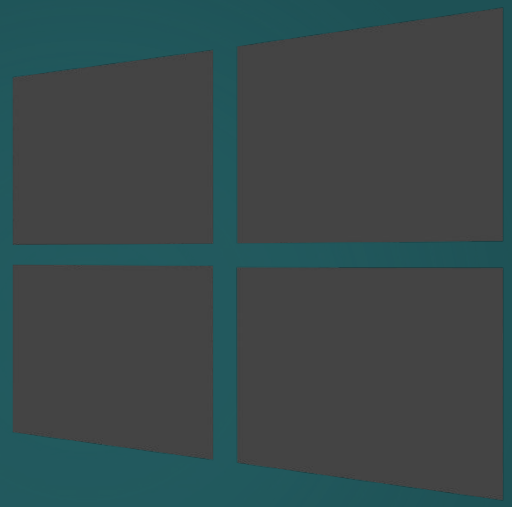
В случае Spectre всё на первый взгляд проще, так как дело касается только общения программ между собой, а не с ядром ОС. Но на практике именно Spectre сейчас наиболее опасны, потому что противодействовать им намного сложнее, чем Meltdown.

Чем опасны

Могут быть украдены ваши важные данные: пароли, банковская информация, личные данные и так далее. В последнее время компании, занимающиеся информационной безопасностью, отметили резкий рост числа образцов вредоносных приложений, которые пытаются использовать Meltdown и Spectre.

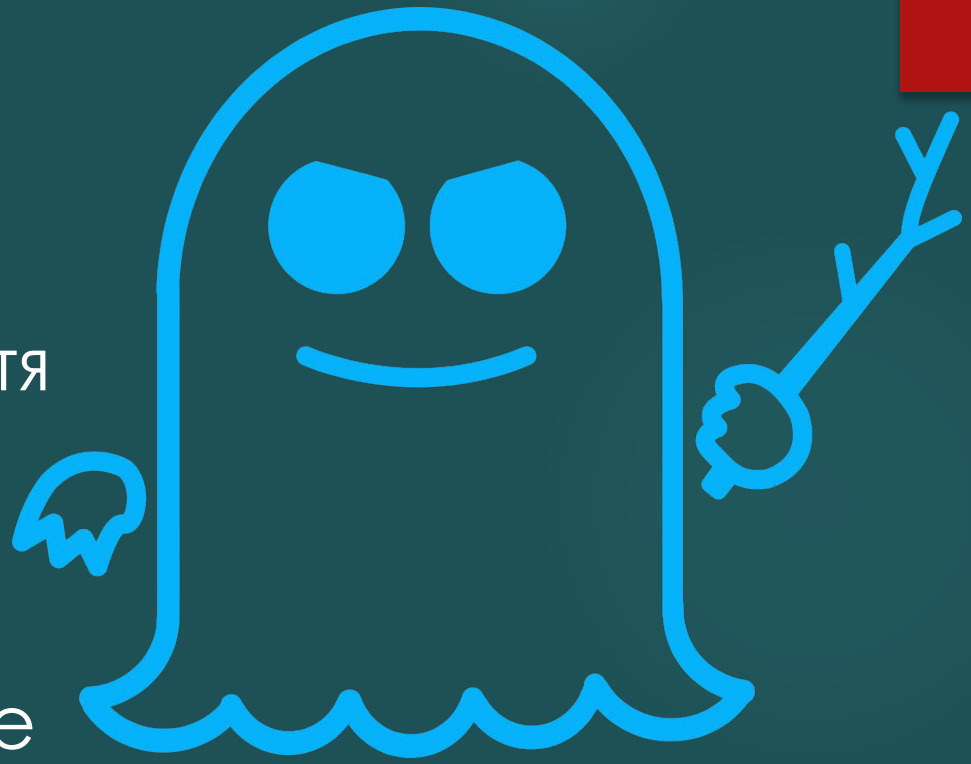
Более того, пользователю даже необязательно что-то скачивать и/или устанавливать — есть варианты атак, которые работают прямо в браузере, то есть достаточно зайти на веб-сайт. Даже на знакомых сайтах могут оказаться вредоносные блоки (рекламные, например). К тому сейчас есть много приложений, которые мимикрируют под настоящие программы, но на самом деле тоже работают в специально созданном браузер

Баг не обошел стороной ни Windows, ни Linux, ни macOS-совместимые ноутбуки и ПК. Исправить уязвимость возможно на уровне операционной системы.



Для исправления ошибки разработчикам операционных систем необходимо изолировать ядро процессора от пользовательской среды на программном уровне. Специалисты отмечают, что исправление ошибки может привести к снижению производительности Windows и Linux-совместимых машин на 5 — 30%. Некоторые сообщают о 63% падении производительности

В настоящее время не существует готовых программных технологий защиты от атаки Spectre, хотя ведется определённая работа. По данным веб-сайта, посвященному продвижению атаки, «Это не так легко исправить, и она (ошибка) будет преследовать нас в течение длительного времени».



SPECTRE

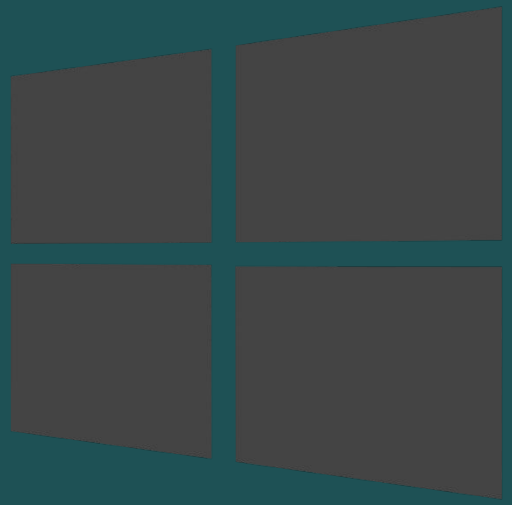
Уязвимость затрагивает все компьютеры, оснащенные чипами Intel и выпущенные за последние 10 лет (по другим данным, 20 лет).

Пользователям продукции Apple повезло больше всего — для обеспечения безопасности им надо обновить операционную систему на всех устройствах до macOS 10.13.2, iOS 11.2 и tvOS 11.2 (или старше), а также обновить Safari как минимум до версии 11.0.2. Увы, старые устройства, которые не получили обновления своих ОС до этих версий, так и останутся уязвимыми.

С Android ситуация сложнее. Исправления для операционной системы выпускают производители устройств. Обновления нерегулярны, а патчи для устройств старше пары лет появляются совсем редко. Так что они тоже останутся уязвимыми.

Пользователям Linux необходимо обновить ядро до версии 4.14.11 и старше, а заодно обновить и все остальные программы с драйверами.

Обновления выпущены только для Windows 7 SP1, Windows 8.1 и Windows 10, а также для браузеров Internet Explorer и Edge.



Кроме того, вне зависимости от устройства и ОС крайне желательно установить и/или обновить антивирус. Все остальные программы, а в особенности браузеры, так же стоит обновить до самой последней версии. Из прочих простых мер защиты можно, как обычно, порекомендовать не посещать незнакомые сайты, установить блокировщик рекламы, а также не скачивать и не запускать файлы от неизвестных людей или из подозрительных источников.