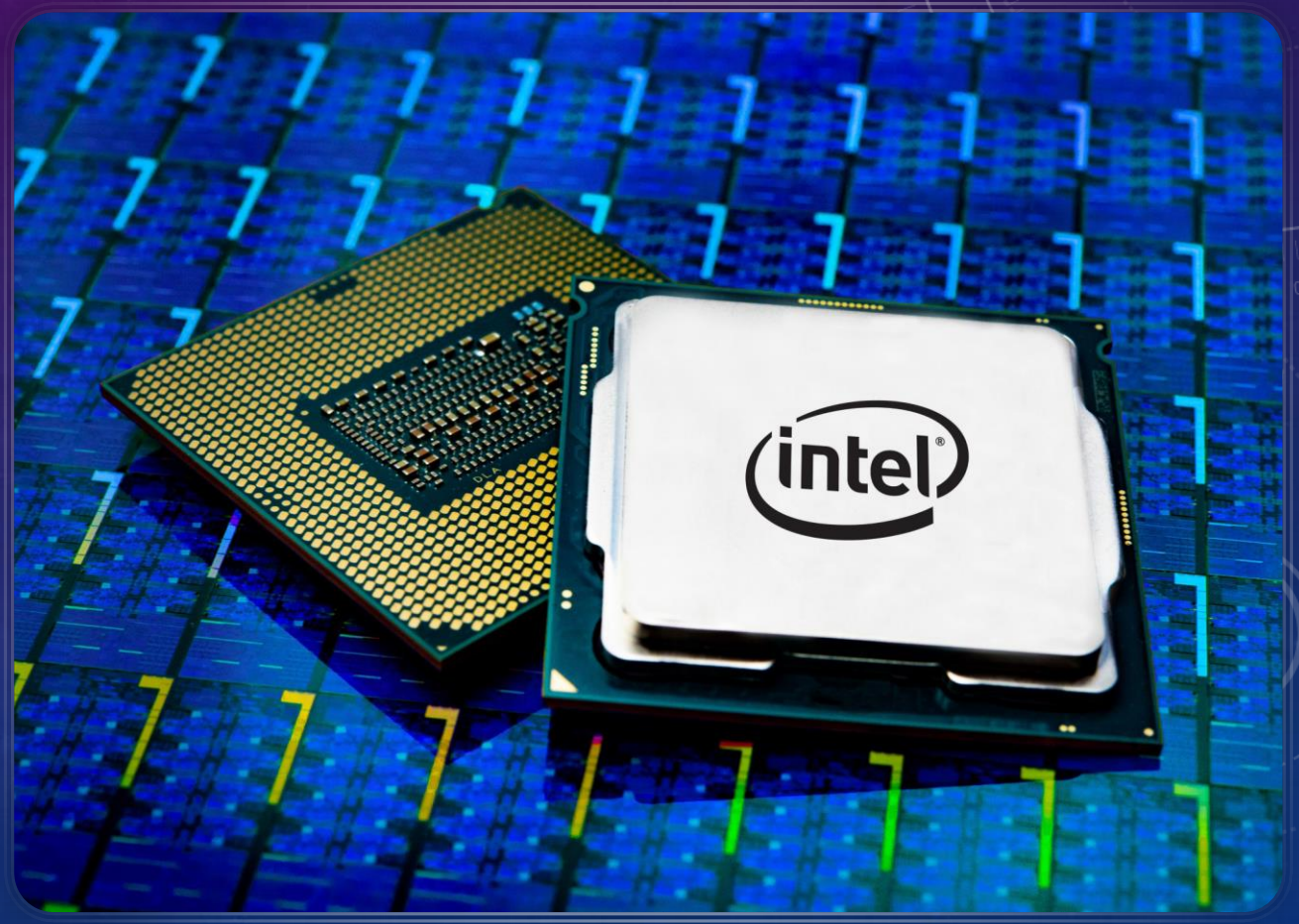
ДОКЛАД НА ТЕМУ «АППАРАТНЫЕ УЯЗВИМОСТИ ПРОЦЕССОРОВ»

ВЫПОЛНИЛ: СТУДЕНТ ГРУППЫ ИБ-2102
ВАСИЛЬЕВ МАКСИМ ДМИТРИЕВИЧ

ВВЕДЕНИЕ

Аппаратные уязвимости процессоров

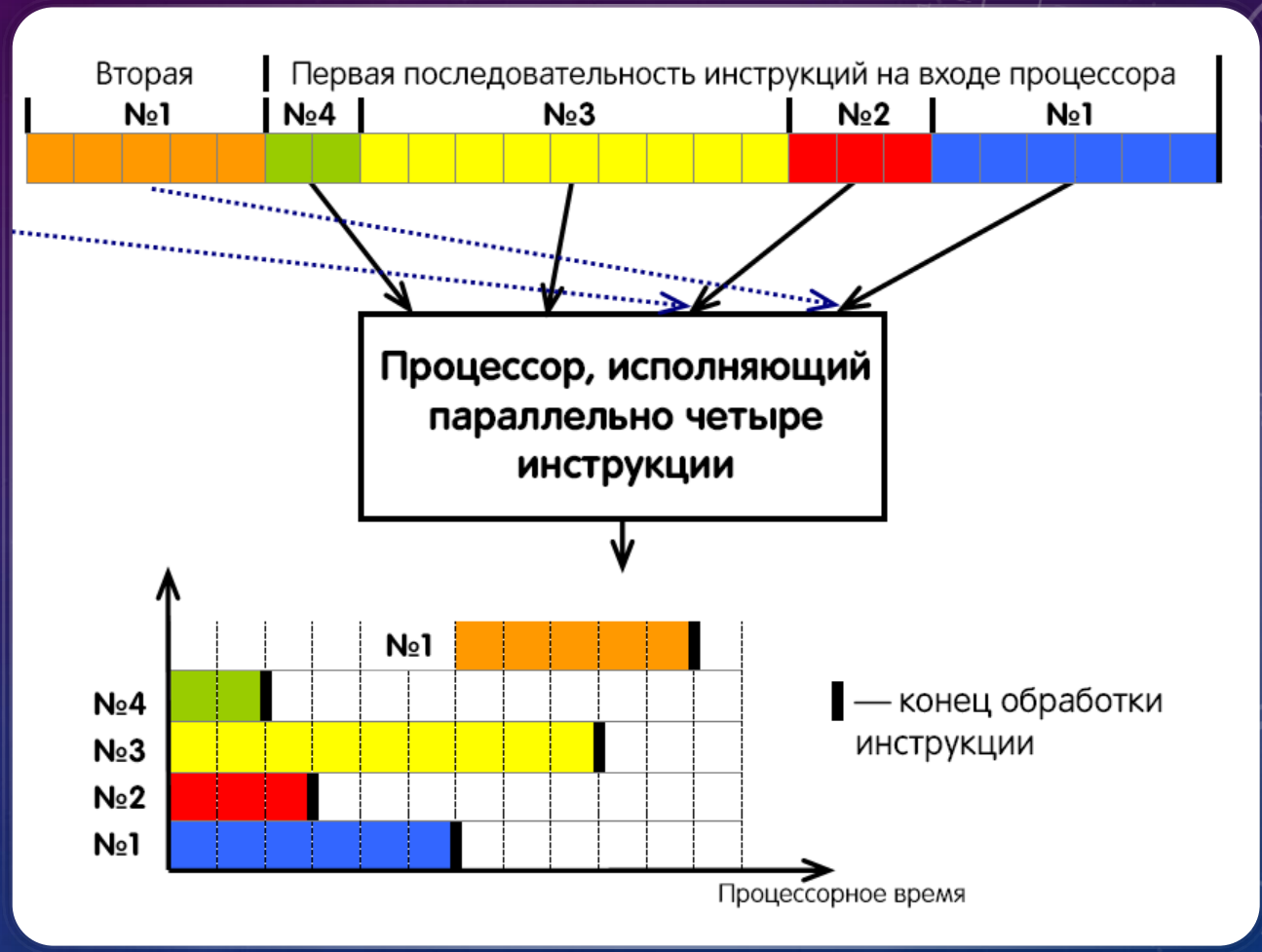


МЕХАНИКА РАБОТЫ УЯЗВИМОСТЕЙ

Уязвимость — это ошибка в процессорах, имеющих технологию внеочередного исполнения машинных инструкций, предсказания ветвлений, гиперпоточности, и других.

УЯЗВИМОСТЬ MELTDOWN

Уязвимость Meltdown основывается на технологии внеочередного исполнения машинных инструкций процессора.

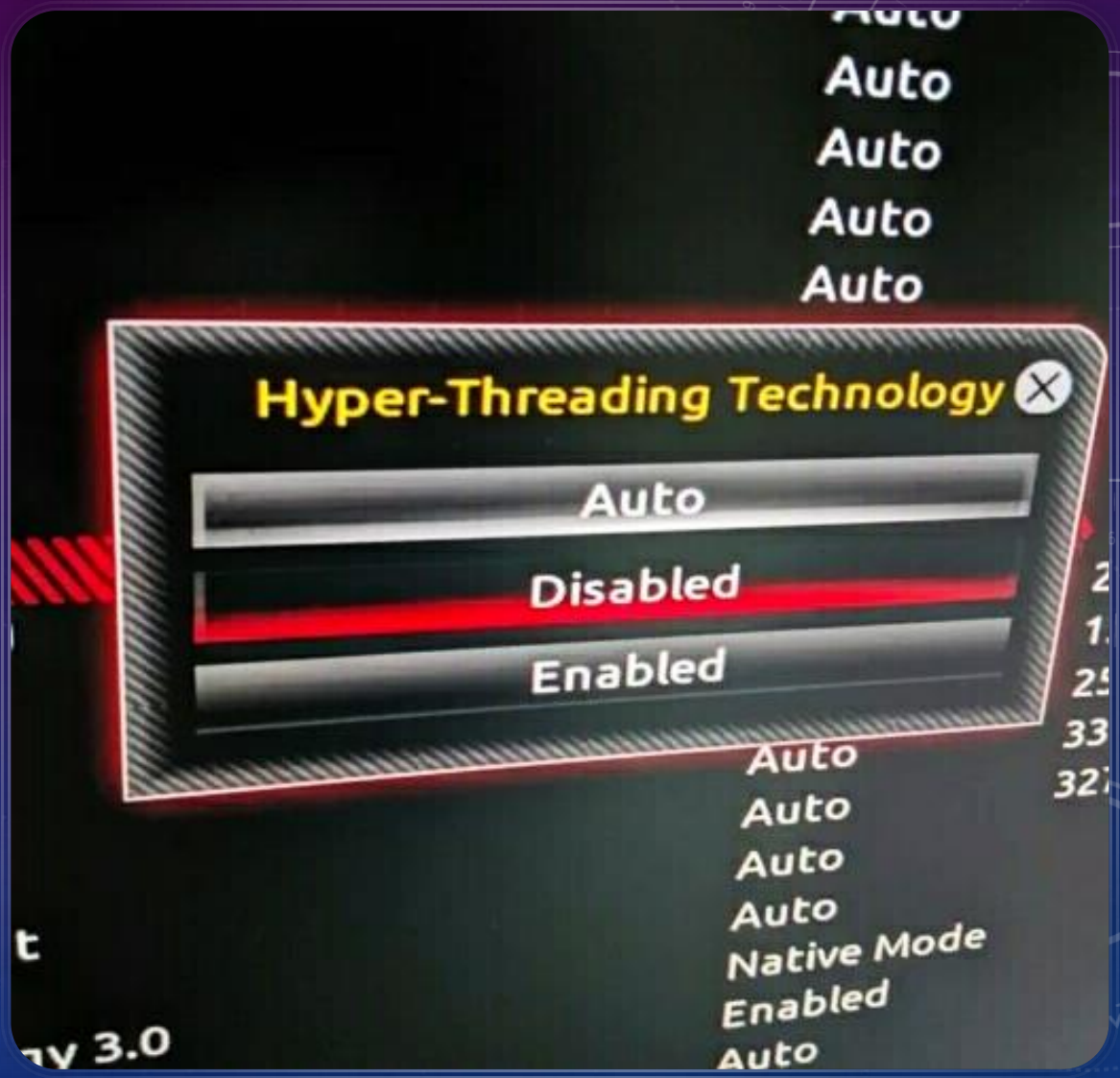


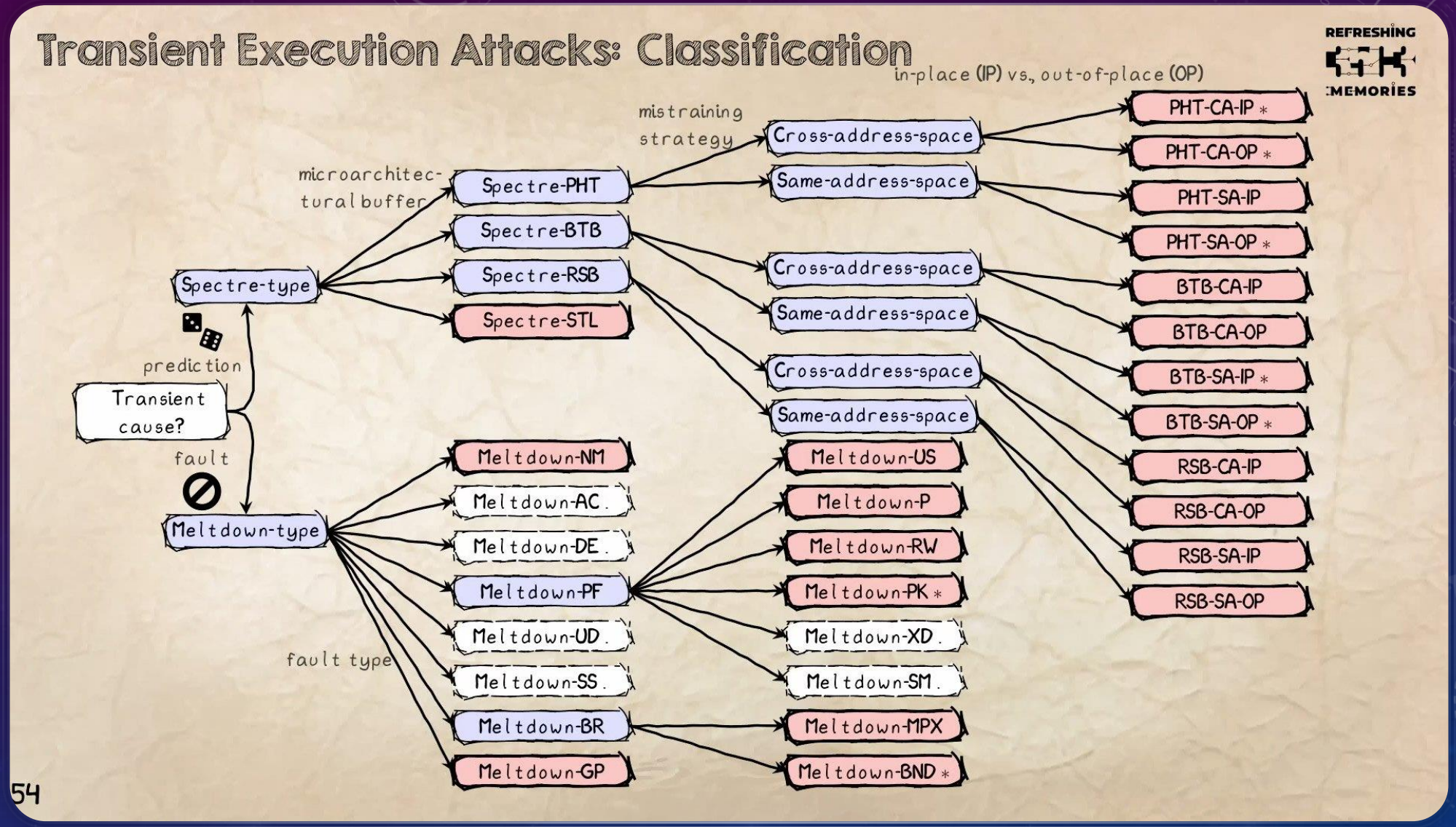
УЯЗВИМОСТЬ SPECTRE

Уязвимость Spectre похожа на Meltdown, но имеет другую причину, впрочем, тоже относящуюся к способам ускорения вычислений в процессоре — она возникла из-за наличия в современных процессорах предсказания ветвлений.

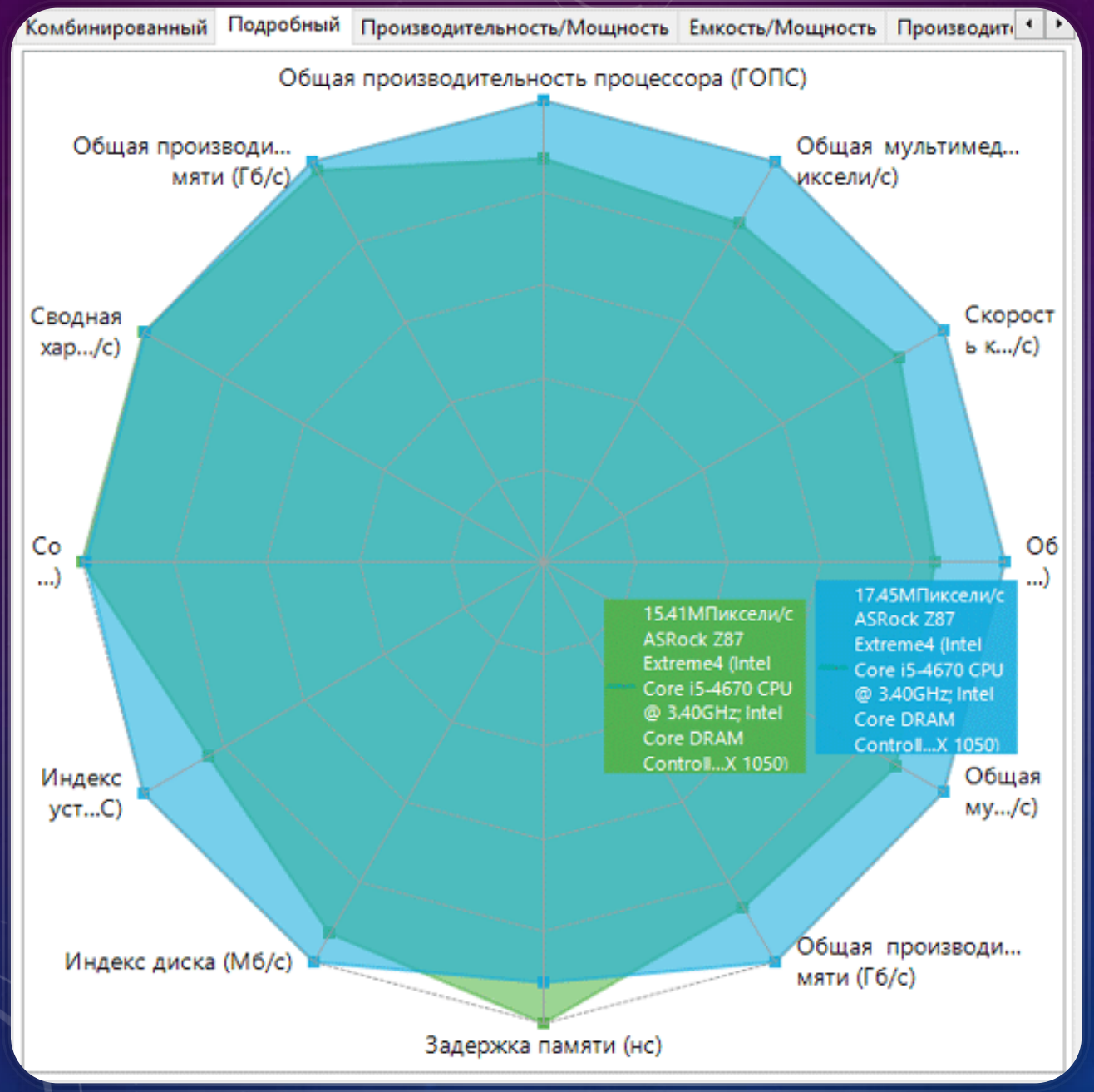
УЯЗВИМОСТЬ ZOMBIELLOAD

Уязвимость ZombielLoad основывается на технологии гиперпоточности (Hyper-Threading), которая также призвана увеличивать быстродействие процессора за счет исполнения физическим ядром процессора двух потоков вычислений.





Классификация найденных за год вариаций Meltdown и Spectre



Тесты производительности Intel core i5-4670 с включенной (зеленая диаграмма) и выключенной (голубая диаграмма) защитой от уязвимостей.

Производительность снижается почти на 10 %

ВЫВОД

Мы познакомились с некоторыми примерами уязвимостей современных процессоров, которые являются следствием многочисленных оптимизационных надстроек в процессорах. Стоит заметить, что причина этих проблем – не сами алгоритмы оптимизации, а скорее их реализация. Действительно, механизмы предсказания ветвлений и внеочередного исполнения не представляли бы опасности, если бы не оставляли никакого, даже микроархитектурного, следа после отката результатов.

Внедрение механизмов оптимизации без учета рисков безопасности привело к серьезным последствиям, пошатнувшим репутацию компаний и повлекших большие убытки. Но есть и хорошая новость: исследователи безопасности процессоров обратили внимание на эту проблему и продолжают в упреждающем режиме искать новые пути кражи данных, чтобы их закрыть.

СПАСИБО ЗА ВНИМАНИЕ!