

SweRV Core — первое RISC-V процессорное ядро Western Digital

В начале декабря 2018 г. компания Western Digital анонсировала инициативы по внедрению в свои решения процессоров на базе открытой архитектуры RISC-V, призванной ответить на вызовы по обработке «больших и быстрых данных».



Григорий Никонов — системный инженер компании Western Digital.

Проект RISC-V

RISC-V (RISC-пять) — открытая архитектура RISC-микропроцессоров, созданная в 2010 году исследователями из Computer Science Division, UC Berkeley (<https://ru.wikipedia.org/wiki/RISC-V>).

Цели разработки: доступная для свободного и бесплатного использования архитектура системы команд (ISA — Instruction Set Architecture), реконфигурируемость, модульность и расширяемость для широкого круга применений.

Основной вектор развития — создание утилитарных процессоров с низким потреблением энергии, быстрых и относительно простых. Однако есть разработки и более мощных 64-разрядных ядер.

Важность проекта состоит в том, что получившиеся процессоры могут быть предоставлены открытому сообществу под лицензией BSD, которая предусматривает создание производных процессоров, которые могут быть как открытыми, так и проприетарными. Основные игроки на рынке микропроцессоров, такие как ARM Holdings и MIPS Technologies, используют лицензионную модель для своих процессорных архитектур, взимая существенную плату за использование своих патентов. Кроме того, особенности их архитектуры защищены соглашениями о неразглашении, что не позволяет проводить независимый аудит безопасности получившихся продуктов.

Разработка CPU — это очень закрытый и сложный процесс, который требует огромной экспертизы в областях электронной логики, компиляторов и операционных систем. Перевод этого процесса на

открытую модель позволяет, подобно программному обеспечению с открытым кодом, использовать экспертизу и навыки сообщества для создания и доработки процессоров. По задумке создателей проекта, это должно привести к тому, что цикл разработки новых процессоров сократится с 12–18 месяцев до нескольких недель, количество разнообразных специализированных процессоров увеличится, их производство станет более доступным, а применение — более безопасным.

Относительно недавние истории с уязвимостями Meltdown и Spectre, которые коснулись процессоров x86 архитектуры, IBM Power и некоторых ядер ARM, показывают, что подход к безопасности процессоров должен быть пересмотрен, и открытость архитектуры может сыграть в этом важнейшую роль.

Список компаний, открыто поддерживающих проект, включает такие имена, как AMD, HPE, Huawei, IBM, Mellanox, Microsemi, Micron, Nvidia, Oracle, SiFive и Western Digital.

Инициативы Western Digital

Впервые об интересе к развитию архитектуры процессоров RISC-V компания Western Digital сказала в 2017 г., заявив о стратегических инвестициях в компанию Esperanto Technologies — разработчика высокопроизводительных вычислительных решений на архитектуре RISC-V. Тогда же компания заявила о планах по переводу всех используемых в ее продуктах процессорных ядер, а речь идет о более чем миллиарде ядер в год, на архитектуру RISC-V.

Отвечая на вопрос, почему Western Digital, компания, занимающаяся разработкой решений по хранению данных, анонсировала поддержку инициативы RISC-V и инвестирует в нее, СТО компании Мартин Финк (*Martin Fink*), приводит такие аргументы:

«Исторически сложилось так, что программное обеспечение развивалось, используя проприетарную бизнес-модель: кто-то написал код, продал его конечному пользователю и собрал плату за его использование или обновление. Модель с открытым исходным кодом перевернула это вверх дном, позволяя сотрудничеству между компаниями на общей базе кода, управляемой правилами. Сегодня модель с открытым исходным кодом, разработанная и оптимизированная Linux Foundation, помогла внедрить инновации в эко-

систему программного обеспечения. Мы полагаем, что эта открытая модель может быть применена к процессорам, что снижает стоимость входа для стартапов и существующих компаний.

Вторая часть ответа заключается в том, что почти каждый продукт Western Digital имеет какое-то процессорное ядро (в настоящее время мы используем один миллиард ядер каждый год в наших продуктах и публично привержены переходу наших процессорных ядер на RISC-V). Работая над внедрением RISC-V ядер в наши продукты, мы также работаем над созданием поддерживающей экосистемы, где данные являются ключевым активом для стимулирования инноваций» (*Martin Fink*, Chief Technology Officer Western Digital, <https://www.westerndigital.com/company/innovations#risc-v>).

Большинство процессоров, которые используются сегодня, являются процессорами общего назначения и достойно справляются с широким кругом разнообразных задач. Однако по мере того, как методы работы с данными меняются, меняется и характер потребностей в вычислительных ресурсах. Вместо того чтобы строить инфраструктуру вокруг возможностей процессора, Western Digital предлагает другой подход — отталкиваться от того, что лучше для данных. И тут становится понятным, что процессоры общего назначения оптимальны не для всех задач. Например, для анализа больших данных оптимально использовать процессоры с ядрами средней мощности, но с возможностью адресовать большое количество памяти. Для высокопроизводительных вычислений хорошо подойдут самые быстрые ядра с минимальными возможностями по вводу-выводу. Блокчейн лучше всего считать на специализированных ASIC-ах. Для анализа видеопотоков оптимально применять GPU и много памяти.

Поддерживая тенденцию использовать специализированные устройства там, где они дают преимущество, Western Digital планирует воспользоваться преимуществами открытой процессорной архитектуры, чтобы сделать свои устройства хранения умнее и функциональнее. Ведь почти половина всех данных в мире хранится на дисках и SSD Western Digital.

4 декабря 2018 г. на саммите RISC-V (RISC-V Summit) корпорация Western Digital объявила о трех инновациях по продвижению архитектуры RISC-V и разработке собственного нового Open Source ядра — RISC-V SweRV Core™.

В своем программном выступлении СТО Western Digital Мартин Финк обнаружил три инициативы:

- планы по выпуску нового ядра RISC-V с открытым исходным кодом;
- инициативу разработки открытого стандарта для когерентной кэш-памяти по сети;
- доступность симулятора наборов команд RISC-V с открытым исходным кодом.

Ожидается, что эти нововведения ускорят разработку новых открытий, специально разработанных вычислительных архитектур для сред больших данных и быстрых данных. Western Digital принимает активное участие в продвижении экосистемы RISC-V, включая многочисленные стратегические инвестиции и партнерства, и продемонстрировала прогресс в достижении заявленной цели перевода одного миллиарда процессорных ядер компании на архитектуру RISC-V.

«По мере того, как большие и быстрые данные продолжают распространяться, специализированные технологические решения необходимы для раскрытия истинной ценности данных в современных широкомасштабных приложениях, ориентированных на данные, — сказал Финк. — Наше ядро SweRV и новая инициатива по созданию когерентной структуры кэша демонстрируют значительные возможности, которые могут быть реализованы путем приближения данных к средствам их обработки».

RISC-V — это открытая, масштабируемая архитектура набора команд, которая обеспечивает разнообразие приложений и рабочих нагрузок больших данных и быстрых данных, которые используются от центров обработки данных до удаленных и мобильных систем на периферии. RISC-V предоставляет альтернативу современным стандартным вычислительным архитектурам общего назначения. С RISC-V можно использовать открытые стандартные интерфейсы для обеспечения: специализированной обработки данных; решений, ориентированных на память; уникальных систем хранения и гибкого интерконнекта приложений.

Western Digital планирует открыть исходный код своего нового ядра — RISC-V SweRV Core, который имеет двухсторонний суперскалярный дизайн. Ядро Western Digital RISC-V SweRV — это 32-рядное 9-ступенчатое конвейерное ядро, которое позволяет одновременно загружать и выполнять несколько инструкций, что сокращает время, необходимое для запуска программ. Это компактное ядро, работающее на скорости 4,9 CoreMarks/Mhz (на основе внутренних оценок). Его энергоэффективная конструкция обеспечивает тактовую частоту до 1,8 ГГц (на основе внутренних оценок) при 28-миллиметровой технологии CMOS. Компания планирует использовать ядро SweRV в различных встроенных конструкциях, включая флэш-контроллеры и твердотельные накопители. Ожидается, что открытый исходный код станет основой для разработки новых приложений, ориентированных на данные, таких, как Internet of

Things (IoT), безопасная обработка, промышленные системы управления и многое другое.

Western Digital OmniXtend™ — это новый открытый подход к обеспечению когерентной кэш-памяти по фабрике Ethernet. Эта архитектура системы, ориентированная на память, предоставляет открытые стандартные интерфейсы для доступа и обмена данными между процессорами, ускорителями машинного обучения, графическими процессорами, FPGA и другими компонентами. Это открытое решение для эффективного подключения постоянной (persistent) памяти к процессорам предлагает потенциальную поддержку будущих современных матриц, которые соединяют вычислительные компоненты, устройства хранения, память и компоненты ввода-вывода.

Western Digital также представила симулятор набора команд SweRV (Instruction Set Simulator, ISS)™ с открытым исходным кодом, который предлагает полную поддержку для тестирования приложений при их использовании с ядрами RISC-V. ISS — это компьютерная программа, которая имитирует выполнение инструкций процессора. Он позволяет моделировать внешние события, такие как прерывания и ошибки шины и обеспечивает правильную работу ядра RISC-V. Компания использовала SweRV ISS для строгого моделирования и проверки ядра SweRV с выполнением более 10 миллиардов инструкций. Western Digital ожидает, что и SweRV Core, и SweRV ISS помогут ускорить переход отрасли на архитектуру с открытым исходным кодом.

«Скорости, каналы и грубые вычисления больше не являются выигрышной формулой для вычислений на периферии и конечных точках. По мере того, как все больше данных перемещается на конечные устройства для обработки и анализа в реальном времени, конфигурируемые архитектуры будут лучше подходить для удовлетворения потребностей тяжелых и часто динамических прикладных рабочих нагрузок, особенно тех, которые ориентированы на искусственный интеллект и Интернет вещей, — сказал Марио Моралес (Mario Morales), вице-президент программы по технологиям и полупроводникам IDC. — Эффективность, конфигурируемость и низкое энергопотребление станут ключевыми показателями для архитектуры периферийных и оконечных (endpoint) компьютеров».

Western Digital SweRV ISS и OmniXtend архитектура доступны для загрузки в следующих локациях:

- OmniXtend: <https://github.com/westerndigitalcorporation/omnixtend>;
- SweRV ISS: <https://github.com/westerndigitalcorporation/swerv-ISS>.

Ожидается, что ядро Western Digital SweRV будет доступно в 1 кв. 2019 г. (<https://www.westerndigital.com/company/innovations#risc-v>).

*Григорий Никонов,
Western Digital*

Комплекс для раннего выявления сложных угроз

Ноябрь 2018 г. — Компания Positive Technologies анонсировала технологический комплекс для раннего выявления и предотвращения целевых атак. Решение предназначено для крупных компаний с высоким уровнем зрелости ИБ и позволяет выявлять сложные угрозы, в том числе специфичные для России.

Решение сочетает в себе технологии глубокого анализа трафика и передаваемых файлов, дополнено сервисом ретроспективного мониторинга от PT Expert Security Center. Оно выявляет присутствие атакующего не только на периметре, но и в инфраструктуре. Это существенно повышает эффективность выявления сложных атак на разных стадиях, а также снижает потенциальные финансовые потери.

«Число компаний, которые стали жертвами целевых атак в 2017 году, выросло в **два раза**: по нашим данным, **9 из 10** жертв даже не подозревают о взломе. Существующие решения выявляют целевые атаки на периметре, но не способны выявить угрозу, если злоумышленники уже проникли в инфраструктуру. Детектировать взлом удается не сразу: как показывает практика, до его обнаружения в среднем проходит до **197 дней**, — говорит *Алексей Данилин, руководитель направления по развитию бизнеса Positive Technologies.* — После преодоления периметра около 60% атак распространяются в инфраструктуре горизонтально, поэтому они долго остаются незамеченными. Чтобы эффективно и заблаговременно детектировать целевые атаки, необходимо следить за злонамеренной активностью и на периметре, и внутри сети, выявляя атаки в трафике. И, конечно, необходимо выполнять регулярный ретроспективный анализ. Именно этот подход мы постарались реализовать в новом решении».

Комплекс позволяет в режиме реального времени обнаруживать и локализовывать присутствие злоумышленника в сети, а также воссоздавать полную картину атаки для детального расследования. Решение анализирует файлы в различных потоках данных с помощью нескольких антивирусов, «песочницы» и собственных репутационных списков, а также выявляет атаки в трафике на основе большого количества признаков. Так, к примеру, автоматически выявляется применение всех популярных хакерских инструментов, эксплуатация уязвимостей ПО и нарушение политик безопасности — то, что обычно остается незамеченным другими средствами защиты. Благодаря ретроспективному анализу решение находит не обнаруженные ранее факты взлома инфраструктуры, что позволяет сократить до минимума длительность скрытого присутствия злоумышленника.

В основе комплекса — уникальная база знаний, которую эксперты Positive Technologies постоянно пополняют по итогам регулярных работ по анализу защищенности, расследований сложных инцидентов и анализа безопасности различных систем. Благодаря этому и глубокой экспертизе Positive Technologies в обеспечении безопасности сложных инфраструктур решение эффективно выявляет даже самые новые угрозы.