

Круглый стол

Низкий старт для высокого полета

В круглом столе принимают участие

Татьяна БАТАРОВА,
руководитель сектора ОПК ПАО «Ростелеком»

Антон СТРЕЛЬНИКОВ,
технический директор FERRUM IT Group

Александр ФИЛЬЧЕНКОВ,
директор департамента серверных и сетевых систем «Гравитон»

Импортозамещение аппаратного обеспечения в России – одна из наиболее актуальных задач, сопряженных с большими вызовами. Ряд трудностей, связанных с производственными мощностями, параллельным импортом, неразвитостью соответствующих экосистем, растущими требованиями к информационной безопасности, деградацией ИТ-инфраструктур, обусловлены объективными факторами. Мы попросили экспертов поделиться мнениями о способах преодоления дефицита аппаратных устройств, их востребованности и потенциале отечественного рынка.

Достаточны ли отечественные производственные мощности для удовлетворения спроса на серверное оборудование и решения для рабочих мест? В какой степени параллельный импорт сдерживает отечественное производство аппаратных решений или, наоборот, компенсирует дефицит?



Александр ФИЛЬЧЕНКОВ:

По нашим оценкам, в сегменте реестрового оборудования российских производители вполне способны закрыть потребности рынка. Ими не охвачены узкие ниши, например, многопроцессорных серверов.

В то же время спрос на серверы увеличивается. Например,

в этом году число заказов на серверное оборудование «Гравитон» выросло по разным категориям от 30 до 50%. Стабильно высокий спрос на серверы основного назначения, а по «железу» под ИИ мы наблюдаем более чем двукратный рост.

Для поддержания необходимого уровня выпуска оборудования мы опираемся на собственные и 18 контрактных производств. Такой подход помогает компании гибко управлять объемами выпуска продукции и быстро перенастраиваться на запуск новых моделей техники.

Наблюдаете ли вы постепенную деградацию ИТ-инфраструктур, созданных ранее на зарубежном оборудовании? Насколько быстро происходит этот процесс?



Антон СТРЕЛЬНИКОВ:

Деградация ИТ-инфраструктур происходит закономерно на уровне и «железа», и программного обеспечения. Цепочки поставок запчастей продолжают

меняться, и этот процесс еще не завершен.

Действительный срок поддержки в рабочем состоянии техники ушедших из России вендоров возможен для оборудования не старше семи-восьми лет. Причем эти цифры превышают заявленные производителем примерно вдвое. Такова типичная общемировая картина.

В ситуации, когда выходят из строя западные продукты, а комплектующих для них нет, некоторые компании идут на такие непопулярные меры, как покупка

целого решения, чтобы получить один искомый компонент. Понятно, что этот снежный ком будет только нарастать. Следует учитывать, что проблема комплектующих касается не только заказчиков, но и производителей. Компании, которые в перспективе трех-четырех лет не смогут снизить уровень использования зарубежных компонентов, столкнутся с проблемами.

Миграция на российский решение – тоже не безболезненный процесс. Но повысить его эффективность можно, если руководствоваться базовыми правилами: рассматривать широкий набор альтернатив, привлекать консультантов и проводить полноценные пилоты. Если все прошло хорошо на этом этапе, дальнейшее внедрение не составит труда.

Насколько остро стоит вопрос доверенных ПАКов? Как часто сегодня заказчик выдвигает требования доверенности при выборе оборудования?



Татьяна БАТАРОВА:

Вопрос доверенных программно-аппаратных комплексов действительно актуален и продолжает оставаться важным для многих заказчиков, особенно в корпоративном секторе и государственных структурах. Почему это важно?

Доверенные ПАКи обеспечивают более высокий уровень безопасности по сравнению с обычными решениями, так как проходят сертификацию и проверку на соответствие требованиям защиты информации. Это защита от несанкционированного доступа к данным; контроль

целостности программного обеспечения; гарантии отсутствия закладок и уязвимостей, которые могут быть использованы злоумышленниками.

Особенно актуально это на фоне роста киберугроз, когда организации стремятся защитить свои данные и инфраструктуру от потенциальных атак.

Все более высокие требования доверия продиктованы нормативными актами, обязывающими использовать сертифицированное оборудование для обработки конфиденциальной информации, персональных данных и других объектов КИИ, политикой безопасности (внутренними стандартами ИТ), сложностью современных угроз, повышением уровня осведомленности (руководители предприятий и ИТ-отделы понимают важность защиты данных и рисков, связанных с использованием ненадежного оборудования). Внимание к доверенным ПАКам усиливается по мере развития ИТ

и нарастания киберугроз. Организации все чаще обращают внимание на наличие сертификации и проверки оборудования перед его внедрением.

Антон СТРЕЛЬНИКОВ:

Заказчики действительно просят нас создать такие программно-аппаратные комплексы. Мы собираем ПАК из доверенных компонентов, включенных в реестр, тестируем их вместе с клиентами и затем интегрируем и обеспечиваем техническую поддержку. Такой подход востребован не только среди государственных структур и компаний с госучастием, но и у частных заказчиков.

Многие компании, которые формально не соответствуют требованиям регуляторов, хотят развернуть тестовые зоны на компонентах, устойчивых к санкциям, перенести туда свои существующие сервисы или запустить новые. Все это позволяет компаниям управлять рисками и уязвимостями, появившимися в их инфраструктуре из-за ухода глобальных поставщиков с российского рынка.

Насколько развиты экосистемы, построенные вокруг отечественных аппаратных платформ? Насколько востребованы ПАКи на практике?

Татьяна БАТАРОВА:

Экосистема активно развивается, но пока не может сравниться по масштабу и полноте с экосистемами, сформированными вокруг глобальных игроков, таких как Intel или AMD. Однако прогресс заметен. Ряд факторов указывают на рост и развитие этих экосистем. В частности, разработка процессоров (например, «Эльбрус», «Байкал» и «Комдив» используются в ряде спецприменений, таких как серверное оборудование, рабочие станции и встраиваемые системы); программная поддержка (для отечественных процессорных архитектур создаются операционные системы Astra Linux, Alt Linux и другие дистрибутивы Linux, адаптированные под эти архитектуры); поддержка периферийных устройств (производятся материнские платы, сетевые карты, контроллеры хранения данных и другие компоненты, совместимые с отечественными процессорами, однако их ассортимент и доступность ограничены). Среди других факторов – интеграция (отечественные аппаратные платформы интегрируются с системами управления базами данных, ERP-системами, средствами защиты информации и т. д.); господдержка в виде грантов и субсидий, стимулирующая разработку и внедрение отечественного оборудования.

Несмотря на позитивную динамику, у российских экосистем есть ряд ограничений: отечественные аппаратные платформы ориентированы преимущественно на внутренний рынок, российские платформы находятся на начальной стадии развития, недостаточная унификация стандартов и интерфейсов затрудняет интеграцию и создание комплексных решений. Наряду с этим развитие экосистемы требует большого количества специалистов, обладающих необходимыми навыками работы с отечественным оборудованием и ПО.

Тем не менее, перспективы развития отечественных экосистем

обнадеживающие. Господдержка, растущий спрос на импортозамещение и повышение интереса к вопросам ИБ создают благоприятные условия для роста. Не стоит забывать, что развитие экосистем – долгосрочный процесс, требующий значительных инвестиций и времени.

Востребованность программно-аппаратных комплексов зависит от отрасли, специфики задач, требований безопасности и уровня автоматизации процессов. ПАКи широко применяются там, где требуется автоматизировать сложные процессы и управлять большим количеством параметров одновременно, например, в энергетике (управление электростанциями, распределительными сетями, мониторинг оборудования), нефтегазовой промышленности (контроль за добычей, транспортировкой и переработкой), на транспорте и в машиностроении (автоматизированные системы управления движением поездов, самолетов, судов).

Одно из преимуществ ПАК – возможность интеграции средств защиты информации в аппаратную часть комплекса. Благодаря этому такие решения востребованы в сферах, где информация имеет высокую ценность и должна быть защищена от несанкционированного доступа (органы власти, ОПК, телекоммуникации и связь, медицина и биотехнологии). Таким образом, ПАКи востребованы во всех секторах экономики, где требуется высокая степень автоматизации, надежности и безопасности. Их практическая значимость возрастает по мере усложнения технологических процессов и повышения требований к защите информации.

Антон СТРЕЛЬНИКОВ:

Когда возникает вопрос о переносе крупной промышленной инфраструктуры, компании понимают, что трансформацию нужно проводить в комплексе. Если менять только по одному продукту за раз

в стеке технологий, то в перспективе пяти лет бизнес столкнется с тем, что продукты выбраны неудачные, совместимость ограничена либо отсутствует.

Поэтому нужна стратегия на внедрение изменений на всем ландшафте ИТ – шаг за шагом. В основе выбора решений должен лежать реальный опыт использования продукта, но не маркетинговые обещания вендора. И здесь самый простой способ – протестированное вертикально-интегрированное решение с несколькими вариантами исполнения на каждый слой. Разработчикам ПО стоит участвовать в программах тестирования взаимной совместимости со смежными вендорскими решениями.

Мы видим спрос со стороны заказчиков по самым разным направлениям: ПАКи с распределением нагрузки GPU в VDI, для команд работающих с большими объемами данных; ПАКи для бесшовного создания безопасных рабочих мест; медицинские комплексы.

Александр ФИЛЬЧЕНКОВ:

Классический подход к построению ИТ-инфраструктур на серверах преобладает. В то же время интерес к ПАК заметно вырос за последнее время. Например, наш комплекс внедряется сейчас на крупном предприятии транспорта и уже работает в организациях сферы науки. Как правило, ПАКи предпочитают заказчики, которые создают ИТ-инфраструктуру с нуля и хотят быстрее ее запустить. Зачастую внедрение ПАК экономически выгоднее. В одном из наших проектов, где комплекс заменил собой интеграцию шести программных и аппаратных элементов, экономия составила 2,3 раза.

Получить необходимую функциональность в формате ПАК заказчикам порой проще, чем путем классической интеграции, с привлечением интегратора. Мы со своей стороны тоже расширяем предложения. Например, совместно с ГК «Астра» разработали решение для малых и средних организаций от 50 рабочих мест, которым необходимо организовать инфраструктуру виртуализации с минимальными издержками.

Какие проблемы сегодня сдерживают российское производство СХД? Каковы сценарии развития этого сегмента, и какие факторы будут его определять?

Александр ФИЛЬЧЕНКОВ:

Отечественные производители закрывают потребности заказчиков в системах начального уровня, тогда как СХД среднего уровня и Hi-End в нашей стране еще не выпускаются. В то же время в России накапливается и развивается экспертиза по разработке и производству систем хранения данных. Например, предлагаются надежные отечественные решения, которые при определенной конфигурации удовлетворяют запросы заказчиков.

Самый заметный тренд в российском сегменте СХД – приобретение

практически всех ключевых разработчиков ПО компаниями, которые выпускают «железо». Таким образом, эти производители обеспечивают себя программными решениями из собственного контура, но для сторонних производителей доступ к ПО может быть ограничен. Конкурентное поле сжимается. В этом смысле высока ценность гибких предложений в сфере СХД, в частности, поставляемых с разным ПО (RADIX, BAUM или «Арго»). Заказчик может конфигурировать решение с учетом своих потребностей. У каждой программной платформы

свои особенности и преимущества, которые могут «сработать» в разных сценариях.

Драйвером рынка СХД служит потребность в разработке собственного ПО для интеграции с аппаратными платформами. Это новый для нашей страны пласт компетенций. Задача сложная, но ее решение может дать ощутимые конкурентные преимущества компании, которая сумеет предложить единое программно-аппаратное решение.

Кроме того, со стороны рынка мощный запрос на разработку – новых аппаратных решений, например, на all-flash NVMe-системы, многоконтроллерные СХД с распределенным хранением, решения с российской коммутацией. ■

Сетевые технологии на стыке науки и бизнеса

В последней декаде октября в МГУ имени М.В. Ломоносова состоялась 5-я Международная конференция «Современные сетевые технологии» (MoNeTec-2024). Мероприятие стало ключевым событием для специалистов в области сетевых технологий, искусственного интеллекта и цифровых инноваций. Конференция собрала более 300 участников со всего мира – ученых, представителей бизнеса и исследовательских центров. Гибридный формат MoNeTec-2024 позволил подключиться к обсуждению как очно, так и удаленно, что способствовало широкому обмену знаниями.

Программный комитет в составе ученых из России, Китая, США и Сингапура отобрал для устного представления 23 англоязычных доклада из 84 поданных. Для пленарных докладов были приглашены авторитетные исследователи из России и Китая.

Всего в рамках MoNeTec-2024 было представлено более полусотни докладов. На прошедших панельных дискуссиях обсуждались такие актуальные темы, как сети 5G и 6G, Интернет вещей, периферийные вычисления и безопасность ИИ.

Большой интерес вызвало, в частности, выступление профессора Евгения Тыртышника из ВМК МГУ, посвященное матричным декомпозициям для обработки больших данных. По словам ученого, даже самые мощные компьютеры не могут напрямую работать с астрономически большими данными, поступающими как массив всех элементов. Данные такого масштаба могут быть обработаны, если они имеют приемлемую структуру, отраженную соответствующей моделью представления. В докладе рассматривался простой и эффективный принцип отбора данных, на которых обучается модель.



Фото предоставлено ВМК МГУ имени М.В. Ломоносова

Директор Центра беспроводных технологий нового поколения и Интернета вещей Сколтеха Алексей Фролов предложил парадигму случайного доступа без источника решения для повышения эффективности беспроводных сетей. Такой подход предполагает, что устройства совместно используют общий кодер, тем самым упрощается процесс приема за счет исключения процедуры идентификации.

Конференция прошла при поддержке Научно-исследовательского центра ELVEES, который выступил основным спонсором мероприятия. Партнерами MoNeTec-2024 стали Объединенный институт ядерных исследований, ФИЦ «Информатика и управление» РАН, «Криптонит», BaseALT и МГУ.

MoNeTec-2024 закрепила значимость сетевых технологий, искусственного интеллекта для современной науки и бизнеса, участники мероприятия нацелены на дальнейшие исследования и сотрудничество.