Концепция доверенного ПАК для КИИ ОПК:

правовое обеспечение, технологический стек и требования к реализации

Елена АНТИПИНА,
генеральный директор Института государственно-частного планирования

Евгений КАНДЗЮБА,
руководитель проектов Научно-исследовательского центра цифровых технологий

В современном мире на фоне стремительного развития информационных технологий и усиления геополитической напряженности обеспечение безопасности критической информационной инфраструктуры (КИИ) оборонно-промышленного комплекса (ОПК) – одна из приоритетных задач национальной безопасности. КИИ ОПК представляет собой совокупность информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в сфере оборонной промышленности и обеспечивающих выполнение критически важных функций государства. Защита этой инфраструктуры от кибератак, несанкционированного доступа и других угроз – ключевой фактор поддержания обороноспособности страны.

Концепция доверенного программно-аппаратного комплекса (ПАК) выступает в качестве фундаментального инструмента в решении задачи обеспечения безопасности КИИ ОПК. Доверенный ПАК представляет собой интегрированную систему аппаратных и программных средств, разработанную и произведенную с учетом строгих требований к безопасности, надежности и технологической независимости. Эта концепция позволяет создавать защищенные, отказоустойчивые и полностью контролируемые системы, способные противостоять современным киберугрозам и обеспечивать непрерывность функционирования критически важных объектов ОПК в Российской Федерации.

Основные характеристики доверенного ПАК должны включать:

- Полный контроль над жизненным циклом компонентов, что обеспечивает прозрачность всех процессов разработки и производства.
- Отсутствие недокументированных возможностей, что исключает возможность скрытого управления системой или несанкционированного доступа к данным.
- Высокий уровень защиты от несанкционированного доступа, реализуемый аппаратном и программном уровне.
- Возможность проверки и аудита исходного кода всех программных компонентов, что обеспечивает дополнительный уровень доверия к системе.
- Использование отечественных технологий и компонентов, что снижает зависимость от иностранных поставщиков и минимизирует риски, связанные с санкциями или прекращением поставок.

Особенности применения в КИИ ОПК

Применение доверенных ПАК в КИИ ОПК характеризуется рядом специфических требований и особенностей, которые отражают уникальную природу задач, решаемых в рамках ОПК:

Многоуровневая система защиты государственной тайны:

- Реализация комплексных систем криптографической защиты с использованием квантово-устойчивых алгоритмов шифрования отечественной разработки.
- Внедрение многофакторных механизмов аутентификации и авторизации пользователей с учетом специфики режимных объектов и требований к разграничению доступа.
- Создание изолированных сегментов сети с динамической архитектурой для обработки информации различных уровней секретности, включая системы автоматического переключения между режимами секретности.
- Разработка и внедрение систем активного противодействия утечкам информации, включая методы квантовой криптографии для защиты каналов связи.

Обеспечение непрерывности функционирования в экстремальных условиях:

- Разработка отказоустойчивой архитектуры с многократным резервированием критически важных компонентов и возможностью «горячей» замены.
- Внедрение интеллектуальных систем прогнозирования и предотвращения сбоев на основе анализа больших данных и машинного обучения.
- Создание распределенных систем управления с возможностью автономной работы отдельных сегментов в условиях нарушения связности сети.
- Разработка механизмов быстрого восстановления работоспособности после кибератак или физического воздействия, включая системы автоматической реконфигурации и перераспределения ресурсов.

Адаптивная высокопроизводительность для специализированных задач ОПК:

- Оптимизация аппаратной части для эффективного решения специфических задач, таких как многомерное моделирование физических процессов, анализ больших объемов разнородных данных, обработка сигналов в реальном времени.
- Разработка специализированных вычислительных ускорителей на базе ПЛИС и заказных СБИС для решения узкоспециализированных задач в области криптографии, цифровой обработки сигналов и искусственного интеллекта.
- Создание программных средств динамического распределения вычислительных ресурсов с учетом приоритетности задач и текущей оперативной обстановки.
- Внедрение технологий квантовых вычислений для решения задач оптимизации и моделирования сложных систем.

Гарантированная технологическая независимость на всех уровнях:

- Использование отечественных процессоров с открытой архитектурой, систем хранения данных на базе российских накопителей и коммутационного оборудования собственной разработки.
- Разработка и применение полностью отечественного стека системного и прикладного ПО, включая операционные системы, СУБД, средства виртуализации и контейнеризации.
- Создание полного цикла разработки и производства ключевых компонентов на территории России, включая проектирование и производство микроэлектроники по технологическим нормам 28 нм и ниже.
- Внедрение системы сквозного контроля качества и безопасности на всех этапах жизненного цикла компонентов ПАК, от проектирования до утилизации.

Проактивная адаптация к эволюционирующим угрозам:

- Реализация механизмов непрерывного обновления ПО и микрокодов устройств с использованием технологий ИИ для анализа и прогнозирования потенциальных уязвимостей.
- Внедрение систем активного киберпротивоборства, способных не только обнаруживать и предотвращать атаки, но и проводить контрмеры в автоматическом режиме.
- Создание распределенной инфраструктуры для оперативного реагирования на новые типы угроз, включая системы автоматического обмена информацией об инцидентах между различными объектами КИИ ОПК.
- Разработка и внедрение технологий цифрового двойника для моделирования и тестирования систем защиты в условиях, максимально приближенных к реальным сценариям кибератак.

> Комплексный подход к применению доверенных ПАК в КИИ ОПК позволяет обеспечить высокий уровень защиты стратегически важных объектов.

Комплексный и многоуровневый подход к разработке и применению доверенных ПАК в КИИ ОПК позволяет обеспечить беспрецедентно высокий уровень защиты стратегически важных объектов и систем, а также создать надежный фундамент для долгосрочного технологического развития отечественной промышленности в области информационной безопасности,

высокопроизводительных вычислений и передовых цифровых технологий. Это, в свою очередь, способствует укреплению цифрового суверенитета России и повышению ее конкурентоспособности на глобальной арене.

Нормативно-правовая база, регулирующая разработку, производство и применение доверенных ПАК для КИИ ОПК, представляет собой сложную систему законодательных и подзаконных актов. Эта многоуровневая структура позволяет обеспечить комплексное регулирование всех аспектов создания и применения доверенных ПАК.

Постоянное развитие нормативно-правовой базы в этой области обусловлено необходимостью оперативного реагирования на появление новых технологий и изменение характера угроз ИБ. Такая динамика требует от разработчиков и производителей доверенных ПАК постоянного мониторинга изменений законодательства и оперативной адаптации своих продуктов к новым требованиям. С одной стороны, это дополнительный вызов, а с другой – стимул инновационного развития отрасли.

Московский научно-промышленный кластер двойного назначения «Российские аппаратно-программные комплексы»

Концепция научно-промышленного кластера двойного назначения разработана Институтом государственно-частного планирования по поручению коллегии Военно-промышленной комиссии РФ с целью интеграции военных и гражданских секторов экономики. Научно-промышленный кластер двойного назначения – это региональный консорциум организаций ОПК, научно-образовательных организаций, средних и малых инновационных компаний с целью выпуска высокотехнологичной продукции гражданского и двойного назначения, сохранения и развития научно-промышленной инфраструктуры и кадрового потенциала организаций ОПК для оперативного переключения между режимами диверсификации и мобилизации.

С целью получения доверенных российских ПАК для КИИ органов государственной исполнительной власти (программно-аппаратные комплексы для региональных центров управления) и организаций ОПК было решено приступить к диверсификации АО «МЦСТ» и созданию таких ПАК на базе микропроцессорной архитектуры «Эльбрус».

К настоящему времени созданы и успешно функционируют несколько подобных структур в Сибири и на Урале: Томский научно-промышленный кластер двойного назначения «Комплексные автоматизированные системы», объединяющий более 30 организаций, Свердловские научно-промышленные кластеры двойного назначения металлургии и металлообработки и транспортного машиностроения, объединяющие около 40 организаций.

В 2023 г. по решению Межведомственной рабочей группы коллегии ВПК РФ по диверсификации и развитию рыночных механизмов в организациях ОПК в целях импортозамещения и реализации национальных проектов было принято решение о создании Московского научно-промышленного кластера двойного назначения «Российские программно-аппаратные комплексы» с целью диверсификации АО «МЦСТ» и создания ПАК для КИИ. В первую очередь это должны были быть ПАК для региональных центров управления, но скоро стало понятно, что для информационной инфраструктуры ОПК решения, созданные на микропроцессорах «Эльбрус» также должны стать наиболее доверенными и защитить от несанкционированного доступа. Большое внимание этому было уделено на форуме «Информационные технологии на службе оборонно-промышленного комплекса России», который ежегодно проходит под патронажем коллегии ВПК на территории субъектов РФ с развитым ОПК.

Важной темой обсуждения на форуме в этом году в Архангельске было то, что сегодня известен немалый список уязвимостей зарубежных процессоров, вполне возможны и другие недокументированные функции, вплоть до враждебных. Таким образом, очевидна необходимость поэтапного перевода ИТ-отрасли России и дружественных ей стран на процессоры с доверенной архитектурой. На первом этапе необходимо перевести на доверенные решения на базе российских процессоров «Эльбрус» КИИ, от которой зависит безопасность важнейших внутригосударственных взаимосвязей, общая безопасность государства и граждан.

На форуме отмечалось значение государственно-частного планирования для формирования российских ИТ-решений, направленных на повышение эффективности и производительности предприятий ОПК, играющих особую роль в обеспечении технологической независимости и безопасности страны. Эксперты рекомендуют:

- При построении доверенного контура КИИ организации ОПК ориентироваться на использование российских процессоров и отечественных программных решений. При создании ПАК ядром должны быть процессоры «Эльбрус» и «Комдив», использующие российскую архитектуру, а также защищенные российские системы серверной виртуализации.
- Развивать проект по созданию гибридных кластеров, модульных ПАК и резервно-контрольных контуров для различных применений в ОПК на микропроцессоре «Эльбрус», что позволит обеспечить мягкий переход на полностью российские ПАК, а также универсальность и масштабируемость решений, отвечающих современным вызовам нацбезопасности и потребностям отрасли.
- Сформировать консолидированный заказ со стороны организаций ОПК для обеспечения рынка отечественными процессорами.

Данный подход резко понизит себестоимость продукции и повысит доступность для разработчиков и производителей.

- Поддержать инициативу Московского научно-промышленного кластера двойного назначения «Российские программно-аппаратные комплексы» по формированию комплексной научно-технической программы полного инновационного цикла «Российские программно-аппаратные комплексы с реализацией функции безопасных вычислений на базе процессора «Эльбрус» для КИИ и заранее обеспечить сбыт такой продукции для нужд КИИ ОПК.

Для реализации этих масштабных задач ранее первый заместитель Председателя Правительства РФ Д.В. Мантуров поручил Институту государственно-частного планирования отработать механизм взаимного трансфера технологий военного и гражданского применения, принадлежащих государству, на базе научно-промышленных кластеров двойного назначения, а также проработать дополнительные формы поддержки проектов таких кластеров по созданию отечественных доверенных ПАК для использования в КИИ.

Позднее данное поручение было дополнено поручением от 25 августа 2023 г.: «проработать вопрос создания комплексной научно-технической программы полного инновационного цикла (КНТП) «Российские программно-аппаратные комплексы с реализацией функции безопасных вычислений на базе процессора «Эльбрус» для критической информационной инфраструктуры».

Для выполнения поручений было решено сформировать Московский научно-промышленный кластер двойного назначения «Российские программно-аппаратные комплексы» (рис. 1), первыми участниками которого стали ведущие промышленные и научные предприятия, технические вузы, профильные институты Российской академии наук, обладающие уникальными компетенциями по созданию решений на основе микропроцессоров «Эльбрус»:

Рис. 1. *Московский научно-промышленный кластер двойного назначения «Российские программно-аппаратные комплексы»*

- АО «МЦСТ» – разработчик микропроцессоров «Эльбрус»;
- ПАО «ИНЭУМ им. И.С. Брука» – разработчик промышленных решений на архитектуре «Эльбрус», адаптирует передовые технологии для производственных задач;
- ООО «НИЦ ЦТ» – разработчик операционных систем и ПО, создатель рабочего стенда с гибридным кластером на основе системы «1С: Предприятие 8.3»;
- ООО «Институт государственно-частного планирования» – координатор процессов диверсификации организаций ОПК и разработчик концепции региональных центров управления;
- ООО «Эльбрус. Доверенные решения» – интегратор решений на базе микропроцессора «Эльбрус»;
- ФГБУН «ИСП РАН» проводит исследования в области системного программирования;
- ФГБУН «ЦЭМИ РАН» обеспечивает экономико-математическое моделирование;
- АО «НИИВК им. М.А. Карцева» – разработчик высокопроизводительных вычислительных систем и инфраструктурных решений на основе систем виртуализации для платформ «Эльбрус»;
- ФГАОУ ВО «МФТИ» обеспечивает подготовку кадров и научные исследования;
- МГТУ им. Н.Э. Баумана обеспечивает инженерные разработки и подготовку кадров;
- РТУ МИРЭА проводит исследования в области радиоэлектроники;
- МТУСИ – обладатель крупнейшей в стране учебной площадки, оснащенной системами на основе платформы «Эльбрус»;
- АО «НПО "Техномаш" им. С.А. Афанасьева» – разработчик ПАК для машиностроительной отрасли;
- ФАУ «ГосНИИАС» – разработчик систем управления авиатехникой и решений в сфере ИИ.

ПАК на базе «Эльбруса» – фундамент КИИ

Архитектура «Эльбрус» – ключевое решение для обеспечения технологической независимости и безопасности предприятий КИИ благодаря нескольким аспектам. Процессоры «Эльбрус» созданы российскими специалистами без использования зарубежных лицензий или IP-блоков, что исключает наличие «закладок» и недокументированных возможностей. Уникальная архитектура безопасности, реализованная на аппаратном уровне, обеспечивает защиту от различных типов

атак и недоступна в зарубежных процессорах. Платформа «Эльбрус» совместима с российским ПО, что поддерживает оптимальную производительность и безопасность. Возможность сертификации благодаря полному контролю над архитектурой и производством позволяет применять «Эльбрус» в самых критичных системах, соответствующих требованиям ФСТЭК, ФСБ и Министерства обороны РФ.

Наряду с этим «Эльбрус» обеспечивает независимость от геополитических факторов, гарантируя работоспособность критической инфраструктуры в условиях санкций или других ограничений. Масштабируемая и гибкая архитектура «Эльбрус» позволяет создать решения с различной производительностью (от встраиваемых систем до суперкомпьютеров) и поддерживает специфические требования КИИ к безопасности и надежности. Также разработаны средства эмуляции и виртуализации для постепенной миграции на платформу «Эльбрус». Платформа обладает четкой дорожной картой развития, обеспечивая долгосрочную поддержку и улучшение технологии. По совокупности этих факторов «Эльбрус» – оптимальный, а зачастую единственно возможный выбор для организаций, стремящихся защитить свои информационные системы.

Лидер Московского научно-промышленного кластера двойного назначения «Российские программно-аппаратные комплексы» – Научно-исследовательский центр цифровых технологий (НИЦ ЦТ), который совместно с компанией МЦСТ разрабатывает оптимизированную ОС, раскрывающую потенциал процессоров «Эльбрус», включая уникальную технологию безопасных вычислений.

Технология безопасных вычислений — щит от цифровых угроз

Технология безопасных вычислений, реализованная в процессорах «Эльбрус» и поддерживаемая ОС от НИЦ ЦТ, представляет собой комплексный подход к обеспечению кибербезопасности на аппаратном и программном уровнях. Ключевые аспекты этой технологии:

- Защита от ошибок программиста: автоматическое обнаружение неинициализированных данных, строгий контроль границ объектов в памяти, предотвращение использования освобожденной памяти (use-after-free).
- Противодействие эксплуатации уязвимостей: защита от переполнения буфера (buffer overflow), предотвращение атак типа «возврат в библиотеку» (return-to-libc), блокирование выполнения кода из стека и кучи.
- Изоляция недоверенных модулей: строгое разграничение доступа между различными компонентами системы, предотвращение утечек информации через сторонние библиотеки.
- Аппаратная поддержка шифрования: встроенные криптографические ускорители, защищенное хранение ключей шифрования.
- Контроль целостности программного обеспечения: проверка цифровых подписей при загрузке системы и приложений, непрерывный мониторинг целостности исполняемого кода.

Операционная система от НИЦ ЦТ интегрирована с этими механизмами безопасности, обеспечивает оптимальное использование аппаратных средств защиты, дополнительные уровни программной защиты, централизованное управление политиками безопасности, подробное логирование и аудит событий безопасности.

Благодаря этой технологии, системы на базе «Эльбрус» способны противостоять большинству известных типов кибератак, обеспечивая беспрецедентный уровень защиты КИИ.

Гибридные кластеры: новый уровень производительности и гибкости

ПАК может строиться на базе гибридных кластеров. Это инновационное решение, объединяющее мощь процессоров «Эльбрус» с другими вычислительными архитектурами для достижения максимальной эффективности в различных задачах.

Гибридные кластеры предлагают следующие преимущества:

- Гибкость и адаптивность: возможность комбинировать различные типы процессоров позволяет создавать системы, оптимально подходящие для конкретных задач РЦУ и других объектов критической инфраструктуры.
- Плавный переход: гибридные кластеры позволяют постепенно переходить на отечественные решения, сохраняя совместимость с существующими системами.

Расширенные возможности для искусственного интеллекта и машинного обучения: комбинация «Эльбрусов» со специализированными ускорителями открывает новые горизонты для развития ИИ-технологий в управлении городской инфраструктурой.

Структура типового ПАК на базе гибридного кластера может включать:

- Вычислительные узлы на базе процессоров «Эльбрус» для основных задач и обеспечения безопасности, а на базе прочих процессоров для решения задач совместимости с имеющимся программным обеспечением.
- Специализированные ускорители (GPU, FPGA) для задач машинного обучения и обработки больших данных.
- Высокоскоростную сеть для эффективного взаимодействия между узлами.
- Распределенную систему хранения данных.
- Систему управления кластером и оркестрации задач.
- Средства защиты информации и мониторинга безопасности.

Такая архитектура позволяет создать мощную, гибкую и безопасную вычислительную платформу для решения широкого спектра задач в рамках РЦУ и управления критической информационной инфраструктурой.

Примером реализации гибридного подхода служит решение компании НИЦ ЦТ, объединяющее

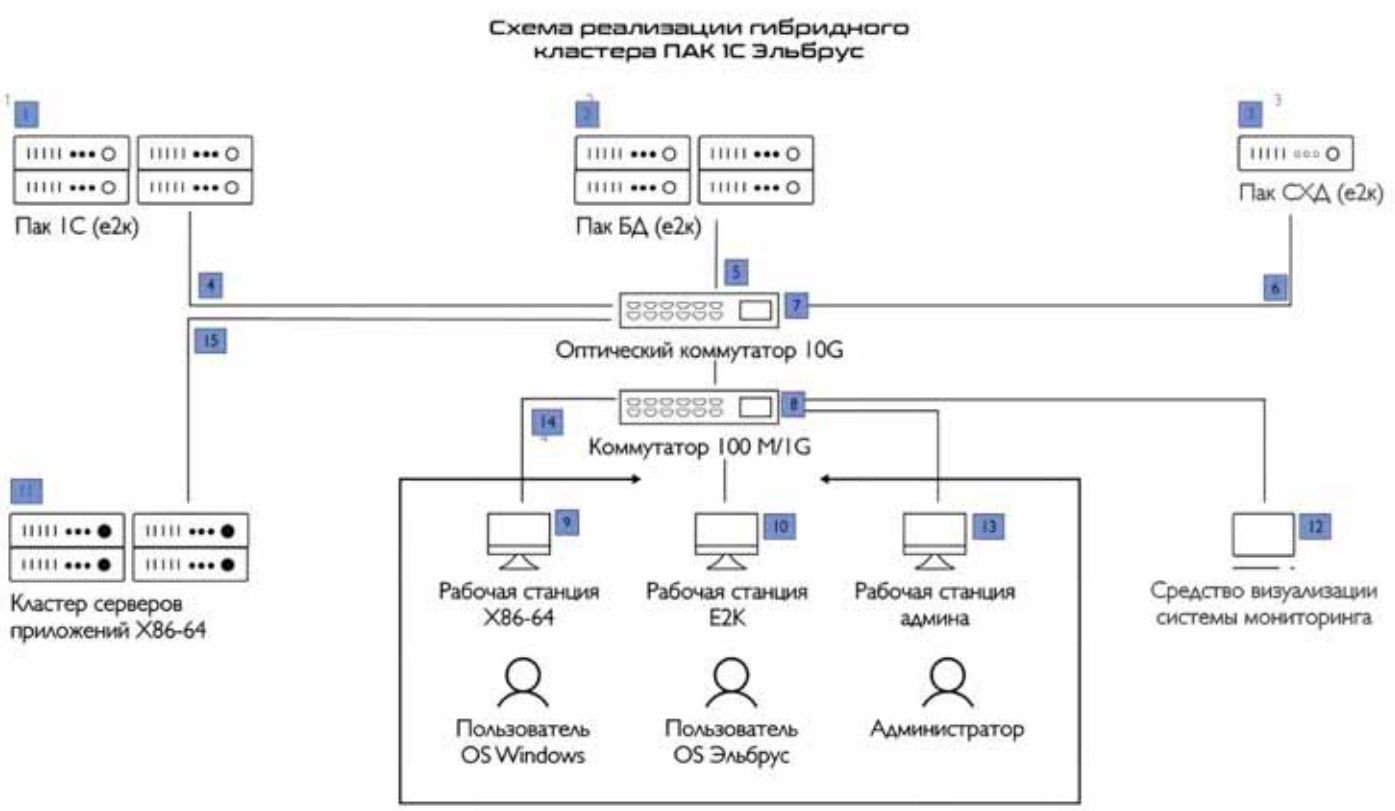

Рис. 2. *Схема реализации гибридного кластера ПАК 1С «Эльбрус»*

аппаратные архитектуры x86 и E2K (ПАК 1С «Эльбрус») (рис. 2). Этот программно-аппаратный комплекс включает в себя несколько взаимосвязанных компонентов, обеспечивающих хранение и обработку данных, а также выполнение прикладных задач. Система построена таким образом, что позволяет эффективно использовать преимущества обеих архитектур, обеспечивая при этом высокую производительность и надежность. Пользователи получают доступ к сервисам и приложениям, работающим как на платформе x86, так и на «Эльбрус», что обеспечивает гибкость в использовании и возможность постепенного перехода на отечественные технологии.

ПАК 1С «Эльбрус» представляет собой интеграцию кластерных технологий для создания высокопроизводительных систем автоматизации бизнеса. Гибридный кластер (рис. 3) представляет собой инновационное решение, объединяющее преимущества архитектур x86 и E2K для создания высокопроизводительных систем автоматизации бизнеса. Ключевая функциональность этого решения включает:

- Повышенную отказоустойчивость за счет комбинации серверов на базе x86 и E2K архитектур, обеспечивающую бесперебойную работу критически важных бизнес-приложений.
- Оптимальное распределение нагрузки между компонентами x86 и E2K, что позволяет достичь максимальной производительности системы в целом.
- Надежное хранение и эффективную обработку больших объемов данных с использованием современных технологий баз данных, адаптированных для работы на обеих архитектурах.
- Гибкую масштабируемость, позволяющую наращивать мощности системы путем добавления серверов как x86, так и E2K архитектуры в зависимости от потребностей бизнеса.
- Поддержку широкого спектра пользовательских устройств и операционных систем для удобного доступа к ресурсам кластера, независимо от используемой архитектуры.
- Интеграцию отечественных (E2K) и зарубежных (x86) технологий, обеспечивающую оптимальный баланс между импортозамещением и совместимостью с существующей IT-инфраструктурой предприятия.

Такая гибридная архитектура позволяет предприятиям создавать надежные, производительные и адаптивные системы автоматизации, способные эффективно решать широкий спектр бизнес-задач, одновременно обеспечивая плавный переход к отечественным технологиям.

Данная интеграция позволяет не только плавно заменить зарубежные системы, но и значительно повысить эффективность внутренних процессов, улучшая производительность и обеспечивая бесперебойную работу, распределяя нагрузку между узлами.

Практическая реализация гибридных кластеров, таких как ПАК 1С «Эльбрус», наглядно демонстрирует эффективность концепции «мягкого импортозамещения», разработанной компанией НИЦ ЦТ. Этот инновационный подход предполагает постепенный и плавный переход от зарубежных решений

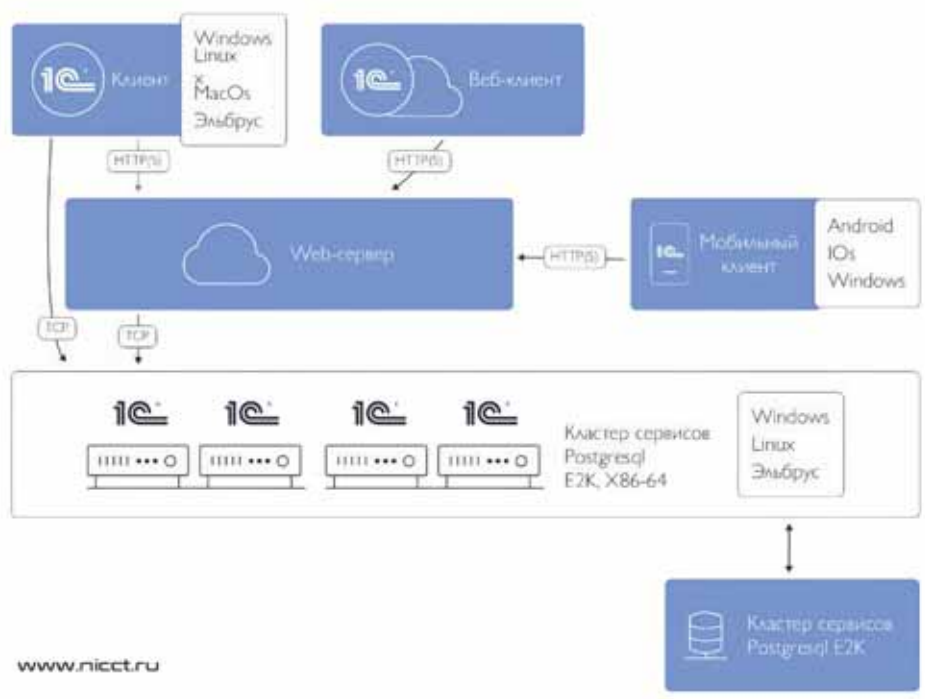

Рис. 3. *Гибридный кластер 1С «Эльбрус»*

к отечественным аналогам, минимизируя риски и сохраняя эффективность работы предприятий в процессе трансформации IT-инфраструктуры.

Ключевым элементом «мягкого импортозамещения» в контексте гибридных кластеров является использование комбинации архитектур x86 и E2K («Эльбрус»). Такой подход позволяет организациям сохранить совместимость с существующими системами и приложениями, одновременно внедряя отечественные разработки. Это особенно важно для предприятий, которые не могут позволить себе резкую смену ИТ-инфраструктуры из-за критичности бизнес-процессов или ограниченности ресурсов.

Реализация «мягкого импортозамещения» на примере ПАК 1С «Эльбрус» демонстрирует, как можно интегрировать отечественные компоненты в существующую инфраструктуру, обеспечивая постепенный переход к полностью российским решениям. При этом сохраняется высокая производительность и надежность работы IT-систем, что критически важно для бизнеса.

Однако для успешного внедрения концепции «мягкого импортозамещения» необходимо развитие целой экосистемы отечественного программного обеспечения, совместимого с различными аппаратными платформами. Именно поэтому следующим логичным шагом в развитии платформы «Эльбрус» станет формирование вокруг нее полноценной экосистемы, выходящей за рамки чисто аппаратных решений.

Московский научно-промышленный кластер двойного назначения «Российские программно-аппаратные комплексы» — ядро экосистемы «Эльбрус»

На сегодняшний день благодаря работе участников Московского кластера, вокруг процессоров «Эльбрус» формируется полноценная экосистема, включающая:

- Оптимизированную операционную систему.
- Средства разработки и отладки программного обеспечения.
- Пакет офисных и специализированных приложений.
- Инструменты для работы с большими данными и искусственным интеллектом.
- Системы управления базами данных.
- Средства виртуализации и контейнеризации.

Эта экосистема позволяет создавать комплексные решения для различных отраслей, от управления городской инфраструктурой до промышленной автоматизации, полностью на отечественной технологической базе.

Московский научно-промышленный кластер двойного назначения «Российские программно-аппаратные комплексы» и его участники, включая НИЦ ЦТ, создают не просто технологии, а фундамент доверенной цифровой инфраструктуры России. Концепция «мягкого импортозамещения», разработанная НИЦ ЦТ, в сочетании с инновационными решениями на базе процессоров «Эльбрус», формирует экосистему, которая является не только инструментом эффективного импортозамещения, но и гарантом информационной безопасности страны.

Разработка доверенных ПАК для КИИ на базе технологий «Эльбрус» обеспечивает высокий уровень защиты стратегически важных объектов и систем. Это ключевой элемент в создании устойчивой и безопасной цифровой среды, способной противостоять современным киберугрозам.

Развитие умных регионов на основе доверенных отечественных технологий «Эльбрус» становится стратегическим императивом для России. Это путь к формированию по-настоящему защищенной, эффективной и независимой цифровой инфраструктуры, способной обеспечить технологическое лидерство страны в условиях глобальных вызовов и угроз.

Таким образом, выбор в пользу развития экосистемы «Эльбрус» и реализации стратегии «мягкого импортозамещения» – это выбор в пользу безопасного и суверенного цифрового будущего России. Это комплексный подход, обеспечивающий технологическую независимость и создающий основу для инновационного развития и укрепления национальной безопасности в цифровую эпоху. ■