



КОНСОРЦИУМ
ТЕХНОЛОГИЧЕСКИХ
КОМПАНИЙ РОССИИ

ИССЛЕДОВАТЕЛЬСКИЙ ЦИКЛ КТКР
МЕТОДОЛОГИЯ ПРЕДИКТИВНОГО
АНАЛИЗА РИСКОВ

БУДУЩИЕ ОГРАНИЧЕНИЯ ЦИФРОВОГО РАЗВИТИЯ РОССИИ

Вопросы, которые государству
важно задавать заранее

Как крупные цифровые
решения создают новые
зависимости, узкие места
и ограничения будущего
манёвра



МОСКВА 2026

БУДУЩИЕ ОГРАНИЧЕНИЯ ЦИФРОВОГО РАЗВИТИЯ РОССИИ

ГЛАВНАЯ СЛЕПАЯ ЗОНА ГОСУДАРСТВА

Цифровая повестка выходит на новый уровень

Главная задача цифрового развития России постепенно меняется.

Ещё недавно основное внимание было сосредоточено на создании собственных решений, замене иностранных продуктов, развитии государственных платформ, переводе услуг в электронный вид и работе с большими данными.

Эта повестка сохраняет значение. Но за ней уже проступает следующий уровень.

Крупные технологические решения не только открывают новые возможности, но и формируют будущие ограничения. Самые чувствительные из них редко возникают в момент сбой, внешнего давления или очевидной управленческой ошибки. Чаще они складываются раньше, когда проект выглядит успешным и воспринимается как движение вперёд.

Запускается государственная информационная система, внедряется промышленное программное обеспечение, строится дата-центр, развивается телекоммуникационная инфраструктура, появляется отечественный продукт, усиливается кибербезопасность или создаётся новый цифровой сервис для граждан и бизнеса.

Снаружи это выглядит как развитие. Но каждое крупное решение меняет среду вокруг себя. Оно требует энергии, специалистов, оборудования, совместимых систем, устойчивых поставщиков, понятных стандартов, качественных данных, регламентов и долгосрочной поддержки. На старте эти условия воспринимаются как рабочая часть проекта. Позднее именно они могут превратиться в узкие места.

Так успешное решение со временем способно создать новую зависимость.

Главная слепая зона заключается не в отсутствии информации

Главная сложность состоит в том, что зависимость редко выглядит как зависимость в момент появления. Сначала она воспринимается как удобство, ускорение и рациональный выбор.

Принято считать, что большие ошибки возникают из-за нехватки информации. Не хватило данных, не увидели угрозу, не получили предупреждение, не было аналитики. Иногда это действительно так. Но самые болезненные ограничения крупных систем часто возникают иначе.

Многие зависимости, с которыми столкнулась Россия в последние годы, не являлись тайной. Было известно, что критически важное программное обеспечение создаётся зарубежными компаниями. Было известно, что многие производственные цепочки опираются на иностранное оборудование и компоненты. Было известно, что микроэлектроника, вычислительная инфраструктура и отдельные технологические стандарты зависят от внешней среды.

Информация существовала, проблема заключалась в другом. Государство, компании и эксперты могли видеть зависимость, обсуждать её и даже признавать её существование, но не считать настолько значимой, чтобы заранее менять решения и закладывать альтернативы.

По сути, слепая зона возникает не там, где нет информации. Она возникает там, где система ещё не готова признать значение того, что уже видит.

Именно поэтому крупнейшие управленческие ошибки почти всегда выглядят очевидными после того, как произошли.

Импортозамещение оказалось больше, чем технологической задачей

Импортозамещение стало своеобразным стресс-тестом государственного управления. Оно показало, что система способна десятилетиями жить рядом с критической зависимостью и не воспринимать её как ограничение будущего развития.

Этот вывод выходит далеко за пределы темы иностранных технологий. Он заставляет иначе посмотреть и на сегодняшние решения.

Какие зависимости, которые сейчас кажутся удобными и рациональными, через несколько лет могут стать стратегическим ограничением?

Какие процессы работают настолько хорошо, что мы перестали воспринимать их как источник риска?

Какие решения сегодняшнего дня постепенно сокращают пространство будущего манёвра?

Именно эти вопросы становятся новой управленческой компетенцией.

Цифровой суверенитет является вопросом будущей свободы действий

Мировая повестка уже показывает этот сдвиг. Искусственный интеллект всё чаще рассматривается не только как технологический рынок, но и как промышленная и инфраструктурная база будущей экономики.

За моделями стоят дата-центры, энергия, чипы, охлаждение, инженерные команды, программные платформы и массивы данных. Вокруг одной технологии быстро возникает целая система условий, без которых она теряет возможность развиваться.

Но искусственный интеллект является только самым заметным примером. Та же логика проявляется в государственных информационных системах, микроэлектронике, промышленном программном обеспечении, телекоммуникациях, кибербезопасности, облачной инфраструктуре, квантовых технологиях, стандартах обмена данными и подготовке инженерных кадров.

Разные по содержанию направления объединяет одна закономерность. За каждым из них стоит набор условий, без которых развитие начинает замедляться. В одном случае узким местом становятся вычислительные мощности, в другом — совместимость, кадры, данные, доверенная инфраструктура, технологические стандарты или концентрация компетенций у узкого круга участников.

Именно поэтому цифровая политика постепенно перестаёт быть только политикой сервисов, платформ и программного обеспечения. Она превращается в политику условий, без которых эти решения не смогут развиваться.

Важный сигнал для России

Если мировая конкуренция смещается от отдельных цифровых продуктов к контролю над условиями их развития, значит, цифровой суверенитет необходимо оценивать не только по факту наличия отечественного решения.

Вопрос «Есть ли у нас своё?» постепенно перестаёт быть достаточным.

Гораздо важнее становится другой вопрос: какие ограничения могут возникнуть вокруг этого решения через несколько лет?

Цифровой суверенитет нельзя измерять только количеством заменённых иностранных продуктов. Настоящий вопрос глубже. Исчезает ли зависимость после замены или просто меняет форму? Отечественное решение может укреплять устойчивость страны, но одновременно создавать новую уязвимость, если вокруг него постепенно возникает зависимость от ограниченного числа специалистов, вычислительных ресурсов, поставщиков, технологий или критических компетенций.

Наиболее опасные зависимости возникают под видом успеха

Особенно показателен пример искусственного интеллекта. Его развитие связано не только с мощностями и моделями, но и с качеством данных, на которых обучаются системы. Если будущие решения будут опираться на чужие датасеты, синтетические данные сомнительного происхождения или внешние алгоритмические шаблоны, страна может получить внешне самостоятельный искусственный интеллект, который воспроизводит чужую картину мира, чужие категории и чужие способы интерпретации. *Такая зависимость сложнее зависимости от оборудования, потому что она проявляется не в поставках, а в смыслах.*

Есть и другой слой, который часто остаётся в тени - кадровый след технологического решения. Когда для проекта выбирается редкий стек, закрытая платформа или узкая инженерная специализация, государство фактически связывает дальнейшее развитие с доступностью небольшой группы людей. Через несколько лет именно команда, архитектурная школа или накопленные знания могут стать ограничением сильнее, чем бюджет или оборудование.

Подобные проблемы почти никогда не появляются внезапно. Сначала растёт стоимость изменений. Затем становится труднее заменить подрядчика, расширить систему, перенести данные или подключить альтернативное решение. Постепенно выясняется, что ключевые знания сосредоточены у ограниченного числа специалистов, а любая корректировка требует всё большего числа согласований.

В какой-то момент проект уже нельзя быстро перестроить. Формально он продолжает работать, а управленческое пространство для изменений уже начинает сужаться.

Будущие ограничения требуют новой управленческой компетенции

Поэтому крупное цифровое решение необходимо рассматривать не только как ИТ-проект, но и как инвестиционное решение с долгим следом. Оно фиксирует выбор архитектуры, поставщиков, стандартов, кадровой школы, модели данных и будущих расходов на сопровождение. *На старте этот выбор может выглядеть техническим, но позднее он начинает определять свободу действий государства.*

Именно здесь возникает скрытая цена цифровизации. Чем крупнее система, тем дороже ошибка в исходной архитектуре. Исправлять приходится уже не отдельный модуль, а всю цепочку решений, которые успели на него опереться.

Поэтому новым объектом стратегического наблюдения должна стать не только сама технология, но и след, который она оставляет в экономике, управлении и инфраструктуре.

Для государства это означает необходимость смотреть не только на факт внедрения, но и на траекторию последствий.

Какие решения сегодняшнего дня через пять лет станут критически важными для страны?

Где под видом суверенного продукта может возникнуть новая зависимость?

Какие государственные системы становятся слишком связанными между собой?

В каких участках растёт сложность, которую пока принимают за нормальную цену цифровизации?

Какие компетенции необходимо развивать уже сейчас, чтобы не покупать время слишком дорого потом?

Именно эти вопросы добавляют к текущей цифровой повестке новый уровень.

Предиктивный анализ становится частью цифрового суверенитета

Для ответа на такие вопросы недостаточно обычного мониторинга проектов. Отчётность показывает сроки, бюджеты и статус исполнения. Контроль фиксирует отклонения, аудит выявляет нарушения. Но будущие ограничения часто формируются раньше, чем появляется формальный сбой.

Они видны в слабых признаках: усложнении интеграций, накоплении временных решений, зависимости от ограниченного числа специалистов, снижении доступности вычислительных ресурсов, отсутствии реальных альтернатив поставщику или технологическому стеку.

По отдельности каждый такой признак может выглядеть обычной рабочей сложностью. Значение появляется тогда, когда несколько признаков начинают усиливать друг друга. Поэтому государству нужен ранний анализ условий, при которых сегодняшнее решение может со временем стать ограничением развития. Такой подход развивается в рамках [Методологии предиктивного анализа рисков](#), подготовленной Консорциумом технологических компаний России (КТКР).

Смысл методологии заключается в рассмотрении крупных решений через возможные последствия, скрытые взаимосвязи и будущую стоимость изменений. Такой анализ помогает заранее видеть, где рабочая сложность способна со временем превратиться в ограничение развития.

Главная ценность подобного подхода заключается в сохранении пространства для манёвра. Если проблема замечена поздно, выбор обычно сужается до дорогой перестройки, срочной замены или вынужденного сохранения неудачной конфигурации. Если она видна заранее, остаётся время на альтернативы, резервные компетенции, стандарты совместимости и более устойчивую архитектуру развития.

В сложной технологической среде выигрывает тот, кто раньше других понимает, что обычное рабочее решение уже начинает менять будущий коридор возможностей. Именно здесь сегодня проходит новая граница цифрового суверенитета.

Михаил Крихели,
Глава Консорциума Технологических Компаний России

Другие статьи автора - www.itconsortium.ru/krikheli-blog

БУДУЩЕЕ ОГРАНИЧЕНИЯ ЦИФРОВОГО РАЗВИТИЯ РОССИИ

Самые опасные ограничения часто возникают тогда, когда проект выглядит успешным.

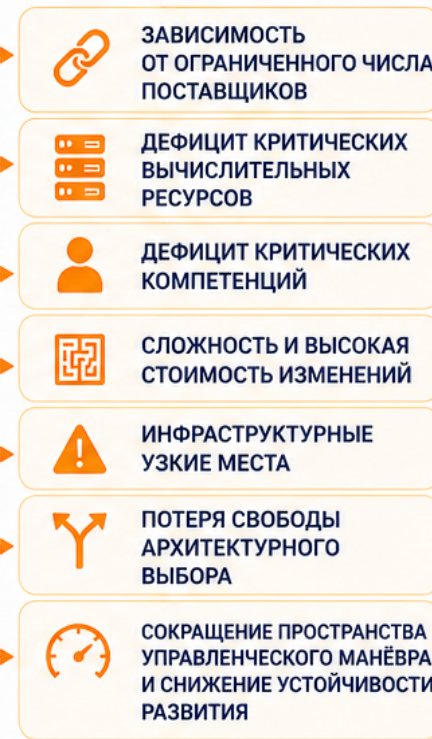


Главная слепая зона: государство может видеть зависимость, но не считать её достаточно значимой, чтобы действовать заранее.

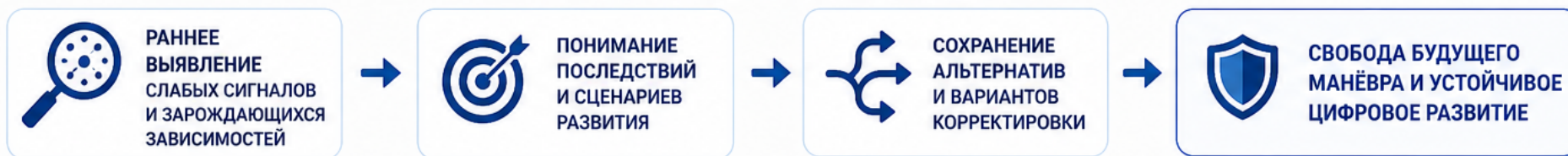
СЕГОДНЯШНИЕ РЕШЕНИЯ



БУДУЩЕЕ ОГРАНИЧЕНИЯ



КАК РАБОТАЕТ ПРЕДИКТИВНЫЙ ПОДХОД



СТРАТЕГИЧЕСКОЕ НАБЛЮДЕНИЕ СЕГОДНЯ — СВОБОДА ВЫБОРА И УСТОЙЧИВОСТЬ РАЗВИТИЯ ЗАВТРА