Цифровая экономика

Август 2026
Тематическое приложение
к газете «Коммерсантъ» **№31**

Коммерсантъ
ONLINE

Guide



КСЕНИЯ АХМЕТЖАНОВА,
РЕДАКТОР GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

НА ЗЕМЛЕ ТОЛЬКО И ГОВОРЯТ, ЧТО ОБ ИИ

Этим летом одной из популярных тем для обсуждения стал доклад AI 2040 от Дэниела Кокотайло и AI Futures Project. Кокотайло — этот тот человек, который еще за год до релиза ChatGPT предсказал, что в течение пяти лет нейросети научатся создавать реалистичные фото и видео, смогут ставить диагнозы лучше врачей и пр. В 2025 году, после ухода из OpenAI, исследователь ИИ основал проект AI Futures Project и весной того же года представил прогноз AI 2027. Тогда он обратил внимание на то, что после ИИ-агенты станут более автономными, в 2027 году появится ИИ-агент на новой архитектуре, которая позволит ему непрерывно совершенствоваться. Как итог прогноза: к концу 2027 года Кокотайло предсказал, что ИИ-системы превзойдут человека во всем.

Что мы видим в его обновленной версии прогноза на ближайшие годы: есть оптимистичный план развития, но для этого странам надо замедлить гонку за сверхмощным ИИ, сделать исследования прозрачными и выстроить систему совместного контроля над вычислительными ресурсами. И сделать это надо прежде, чем появятся по-настоящему сверхчеловеческие системы.

По сути, в «Plan A» в этом докладе — сценарий международной «сделки» вокруг ИИ. Авторы говорят, что уже к началу 2030-х годов стихийная гонка за суперинтеллектом станет слишком рискованной. И если не будет специальных договоренностей, это может закончиться потерей контроля над системами и предельной концентрацией власти у узкой группы игроков. Они предлагают временно остановить обучение самых мощных моделей, сделать исследования открытыми для международного анализа и перенастроить инфраструктуру так, чтобы ключевые дата-центры и фабрики чипов можно было быстро вывести из игры в случае нарушения договоренностей. Но готовы ли страны это регулировать и обсуждать — большой вопрос.

↑ КОЛОНКА РЕДАКТОРА

НЕЙРОСЕТИ УЛАВЛИВАЮТ СЛЕД

СЕГОДНЯ ОКОЛО 42% ПОЛЬЗОВАТЕЛЕЙ НАЧИНАЮТ ПОИСК НОВОЙ ИНФОРМАЦИИ В НЕЙРОСЕТЯХ, 51% — ДОВЕРЯЮТ ИХ ОТВЕТУ, 59% — ИСПОЛЬЗУЮТ ИИ ПРИ ВЫБОРЕ ТОВАРОВ И УСЛУГ, ГОВОРИТСЯ В ИССЛЕДОВАНИИ АГЕНТСТВА «ИМПУЛЬС.ГУРУ». НА ЭТОМ ФОНЕ КОМПАНИИ ВСЕ БОЛЬШЕ ОБРАЩАЮТ ВНИМАНИЕ НА ПРОДВИЖЕНИЕ В НЕЙРОСЕТЯХ, ИЛИ GEO. КАК БИЗНЕСУ ЗАКРЕПИТЬСЯ В ОТВЕТАХ ИИ И СКОЛЬКО ЭТО БУДЕТ СТОИТЬ, РАЗБИРАЛСЯ GUIDE. ВЕРОНИКА ПЕТРОВА

ЦЕННИК С ДВУМЯ НУЛЯМИ Продвижением в нейросетях, по словам основателя агентства NeuroReach Василия Жаркова, сейчас интересуется практически каждая компания, которая серьезно занимается маркетингом. По данным Аналитического центра РИР, 32% специалистов по рекламе уже оптимизируют контент для попадания в такие выборки нейросетей (GEO) и ИИ-помощников поисковиков (AEO). Еще 42% намерены начать работу в этом направлении до конца года.

GEO бренды занимаются либо самостоятельно, либо обращаются в агентства по продвижению. «Обычно бизнес приходит в GEO „попробовать“ и стартует от 100–200 тыс. рублей в месяц. Те, кто видит отдачу, увеличивают бюджеты либо начинают работы по формированию или перестройке собственного отдела»,— говорит совладелец и руководитель отдела продвижения агентства SLT Святослав Волков. По оценке Василия Жаркова, стоимость услуг на рынке начинается от 150 тыс. рублей в месяц, эксклюзивное продвижение с гарантией — от 300 тыс.

Спрос на такие услуги довольно высок, однако, по словам Святослава Волкова, ажиотаж постепенно спадает. «За GEO сейчас в основном приходят как за дополнительным каналом продвижения, когда уже есть SEO, контент-маркетинг, контекстная реклама. Доля обращений велика, у нас примерно треть всех клиентов приходят на GEO»,— объясняет эксперт.

Интерес к нейросетям остается на высоком уровне, считает господин Жарков: «У нас одни из самых высоких цен на рынке. Стоимость начинается от 300 тыс. рублей в месяц, средний чек — около 425 тыс. Поэтому мы ориентируемся на крупнейшие компании России. И заявки приходят именно от них. В среднем около 50 квалифицированных заявок в месяц от крупного и среднего бизнеса».

Более активному продвижению GEO, как считают эксперты, мешает отсутствие четких метрик, которые бы разделяли трафик из поисковых систем и трафик из блоков с нейроответами в этих же поисковиках, и небольшая доля переходов из нейросетей (ChatGPT, Claude, DeepSeek и т. д.) на сайты компаний.

«Рынок GEO пока перегрет обещаниями и страдает от отсутствия прозрачных систем сквозной аналитики. Многие компании не понимают, как именно измерять ROI (показывает окупаемость от вложенных инвестиций) от GEO-активностей, и боятся потратить деньги впустую»,— отмечает председатель digital-комитета «АКАР Северо-Запад» и генеральный директор агентства Grand Media Service Андрей Волков.

Святослав Волков замечает еще одну проблему: «Сейчас любой лид, пришедший из блока нейроответов, будет записан в лид с SEO-канала, а не с GEO. В то же самое время количество блоков с нейроответами очень высоко. По нашему исследованию, в промышленной отрасли около 50% всех запросов в „Яндексе“ содержат ответ ИИ, в Google — 80–90%».



ЕВГЕНИЙ ПАВЛЕНКО

РЫНОК ПОСТЕПЕННО АДАПТИРУЕТ СВОЙ КОНТЕНТ ПОД ВНИМАНИЕ НЕЙРОСЕТЕЙ

КРУПНЫЕ КОМПАНИИ VS. МАЛЫЕ БРЕНДЫ По словам экспертов, обратить внимание на GEO в первую очередь стоит известным компаниям, у которых уже развиты другие методы продвижения: SEO, PR, контент-маркетинг. При этом, как считает господин Жарков, именно крупным брендам необходимо решать вопрос с GEO. «О крупных брендах нейросети регулярно дают недостоверные ответы, собранные из некачественных данных веб-поиска. Такой ответ как минимум обнуляет усилия PR и бренд-маркетинга, как максимум — создает прямые репутационные риски. Вторая причина — масштаб. У крупного бизнеса массовый рынок сбыта. Например, проблемы с сотовой связью сейчас обсуждает вся страна, и пользователи массово спрашивают решение у нейросетей. Какого оператора порекомендует ИИ — такую сим-карту и такой тариф человек и выберет»,— говорит Василий Жарков.

В Biocad, которая уже учитывает принципы GEO при работе с цифровым контентом, также отмечают, что известным компаниям важно, чтобы ИИ-помощники и нейросети использовали корректную информацию о бренде и его продукции. «Для крупной компании это в том числе вопрос управления достоверностью информации о себе: важно, чтобы ИИ опирался на актуальные, понятные и непротиворечивые данные»,— комментирует директор департамента по стратегическим коммуникациям Biocad Ирина Кенюхова.

Известность бренда не гарантирует автоматическое попадание в ИИ-ответы, отмечает Андрей Волков. «Если бренд не управляет своим присутствием в ИИ-ответах, нейросеть может сформировать ответ на основе неполных, устаревших или негативных источников. При этом пользователи все чаще обращаются к ИИ как к первичному источнику информации, и если бренда нет в этих ответах, его как бы „не существует“ для нового поколения потребителей»,— подчеркивает эксперт.

ИНТЕРНЕТ ВСЕ ПОМНИТ Попасть в рекомендации ИИ можно только при условии сформированного «цифрового следа». Андрей Волков отмечает: «Нейросети при формировании ответов ищут не самые популярные бренды, а те, которые наиболее полно и авторитетно раскрывают конкретный аспект запроса. Это означает, что узкоспециализированный, но хорошо задокументированный в публичном поле бренд может получить рекомендацию ИИ, обойдя гигантов, которые не уделяют внимания детальной проработке своего цифрового следа. Но GEO не работает в отрыве от базового SEO. 70% сайтов в генеративной выдаче „Яндекса“ — это сайты из топ-10 органической выдачи. Сначала нужно обеспечить техническое присутствие, а затем через PR и контент-дистрибуцию формировать цифровой след, который заметят ИИ-алгоритмы».

«Цифровой след» бренда формируется на основе всех данных о компании в сети: информация на собственном сайте компании и в социальных сетях, отзывы пользователей на специальных сервисах и личных страницах, публикации в СМИ, рейтинги. «Нейросеть собирает из этого портрет компании, и качество портрета определяется качеством и согласованностью данных: если источники противоречат друг другу, противоречивым будет и ответ»,— объясняет Василий Жарков.

Помимо этого, ИИ оценивают плотность сущностей (четкие факты, цифры, имена) и индекс цитирования в топик-кластерах (авторитетность в конкретной нише), замечает Андрей Волков. «Именно поэтому классический PR становится главным двигателем GEO. Он создает тот самый качественный пассивный след, который ИИ воспринимает как сигнал доверия»,— заключает он.

Развитие нейросетей и появление ИИ-ответов меняют подход компаний к продвижению, уверена Ирина Кенюхова. По ее словам, сейчас компания все больше ориентируется на вопросы, которые пользователи задают поисковикам. «Люди ожидают получить сразу готовый и понятный ответ. Поэтому меняется и структура контента. Мы стараемся уже в первом абзаце давать основную информацию и прямой ответ на потенциальный вопрос пользователя, а затем раскрывать детали. Это повышает вероятность того, что информация будет корректно считана и использована как классическими поисковыми системами, так и генеративными сервисами»,— делится госпожа Кенюхова. ■

ПЕТЕРБУРГ И ЛЕНОБЛАСТЬ НАРАЩИВАЮТ ЦИФРОВЫЕ МОЩНОСТИ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В САНКТ-ПЕТЕРБУРГЕ И ЛЕНИНГРАДСКОЙ ОБЛАСТИ ВЫХОДИТ НА НОВЫЙ УРОВЕНЬ: РЕГИОНЫ УКРЕПЛЯЮТ ПОЗИЦИИ В ФЕДЕРАЛЬНЫХ РЕЙТИНГАХ, А РАСТУЩАЯ НАГРУЗКА НА IT-СИСТЕМЫ И КУРС НА ИМПОРТОЗАМЕЩЕНИЕ ЗАДАЮТ ЖЕСТКИЕ ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ. НА ФОНЕ УСИЛЕНИЯ РЕГУЛЯТОРНЫХ НОРМ И НЕОБХОДИМОСТИ БЕСПЕРЕБОЙНОЙ РАБОТЫ ГОСОРГАНОВ И СУБЪЕКТОВ КИИ ОСОБУЮ ЦЕННОСТЬ ПРИОБРЕТАЮТ НАДЕЖНЫЕ И ЭКОНОМИЧЕСКИ ЭФФЕКТИВНЫЕ РЕШЕНИЯ. О ТРЕНДАХ И КЛЮЧЕВЫХ ТЕХНОЛОГИЧЕСКИХ ПОДХОДАХ К ПОСТРОЕНИЮ ДОВЕРЕННОГО ВЫСОКОНАГРУЖЕННОГО IT-ЛАНДШАФТА РАССКАЗАЛ ДИРЕКТОР ПО РАЗВИТИЮ БИЗНЕСА СКАЛА^Р (ГРУППА RUBYTECH) МИХАИЛ ГИЛЯЗОВ. АЛЕКСАНДР КРЫЛОВ

КЛЮЧЕВЫЕ КРИТЕРИИ Санкт Петербург и Ленинградская область — лидеры цифровой трансформации. По индексу «IQ городов» за 2024 год Петербург занял второе место среди крупнейших городов России (после Москвы), а Ленинградская область поднялась на шесть позиций и вошла в топ-10 федерального рейтинга, заняв девятое место. Регион несколько лет подряд лидирует в СЗФО по внедрению технологий в экономике, социальной сфере и госуправлении. За счет масштабной цифровизации — от электронных госуслуг до платформ «умного города» — госорганы стали ключевыми заказчиками высоконагруженных IT-систем, отмечает директор по развитию бизнеса Скала^р (группа Rubytech) Михаил Гилязов.

Для IT-инфраструктуры госорганов ключевыми критериями стали надежность, сохранность данных, отказоустойчивость и непрерывность сервисов — для этого применяют резервирование, синхронизацию между ЦОД разных регионов и механизмы аварийного переключения. Важны также масштабируемость и производительность: системы должны справляться с ростом нагрузки, например, при массовом обращении граждан. В части безопасности обязательны защита от кибератак и соответствие требованиям ФСТЭК и ФСБ: сертифицированные средства криптозащиты, контроль доступа, доверенная загрузка. Критична совместимость новых решений с действующими системами и возможности платформенного подхода — объединения разрозненных систем в единое информационное пространство с общими сервисами.

Очевидно, что и государственные, и корпоративные процессы постепенно увеличивают требования к IT-инфраструктуре. Новые системы должны работать с большими объемами данных, поддерживать высокие нагрузки и интегрироваться с существующим IT-контуром. Для этого используется инфраструктура высоконагруженных систем (ИВНС). Один из способов ее построения — программно-аппаратные комплексы, которые объединяют аппаратные и программные компоненты в готовое единое решение и применяются для высоконагруженных информационных систем, в том числе для виртуализации, работы с транзакционными базами данных, обработки и хранения больших объемов данных.

«На российском рынке есть программно-аппаратные комплексы (ПАК), ориентированные именно под задачи импортозамещения и построения доверенной IT-инфраструктуры. Наша линейка изначально проектировалась как интегрированный стек, где аппаратная платформа, виртуализация и средства управления согласованы между собой на уровне архитектуры. Это позволяет минимизировать риски несовместимости компонентов и ускорить ввод в эксплуатацию, что критически важно для крупных заказчиков с высокими требованиями к отказоустойчивости и информационной безопасности»,— говорит Михаил Гилязов.

На практике важно не просто подобрать компоненты, а создать целостную, предсказуемо работающую под нагрузкой связку, соответствующую регуляторным требованиям и способную адаптироваться к меняющимся задачам. Поэтому заказчики все чаще оценивают не только технические характеристики, но и опыт поставщика, наличие референсных проектов и готовность сопровождать решение на всем жизненном цикле, добавляет он.



ПРЕСС-СЛУЖБА ГРУППЫ RUBYTECH

СТРЕМИТЕЛЬНАЯ ЦИФРОВИЗАЦИЯ УСИЛИВАЕТ НАГРУЗКУ НА IT-ИНФРАСТРУКТУРУ МЕГАПОЛИСОВ

ПАК: ЭКОНОМИЯ В ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВЕ Объем российского рынка IT-инфраструктуры для высоконагруженных систем, включая и продажи ПАК, по данным консалтинговой компании «Б1», в 2025 году вырос на 15% и достиг 658 млрд рублей. Большая часть спроса на ИВНС пришлась на госсектор — 29%.

Сегодня российские разработчики способны уверенно конкурировать с зарубежными вендорами в сфере высоконагруженных инфраструктур, это стало возможно по нескольким причинам. Госструктуры стали пионерами импортозамещения: программа стартовала в 2014 году, а к 2022-му госсектор уже опережал другие отрасли по его уровню. Цифровизация и развитие ИИ резко увеличили нагрузку на IT-системы, а усиление требований к защите КИИ стимулировало спрос на решения, соответствующие российским стандартам. Отечественные команды адаптируют технологии под локальные особенности — от законодательства до специфики технологической платформы. Важную роль играет также и накопленная инженерная экспертиза, подчеркивают в Rubytech. В России сложилась сильная школа разработки, а крупные компании десятилетиями строили собственные высоконагруженные IT-ландшафты, накапливая глубокие знания в архитектуре распределенных систем, также активно развивается экосистемный подход — вендоры стремятся предлагать не разрозненные инструменты, а целостные технологические стеки: ОС, СУБД, виртуализацию, мониторинг, где все компоненты хорошо совместимы между собой.

Стоит отдельно отметить экономический аспект: в дискуссиях о конкуренции с зарубежными вендорами ему уделяют меньше внимания, чем технологиям, хотя именно он зачастую становится решающим фактором для заказчика, считает Михаил Гилязов. «Корректно сравнивать совокупную стоимость владения на горизонте трех-пяти лет, и на этой дистанции ПАК выигрывает. В цену комплекса уже включены техническая поддержка, обновления и гарантийное обслуживание, а существенная часть экономии возникает там, где ее обычно не считают: заказчик не оплачивает работы по стыковке компонентов между собой и не несет издержек от простоев из-за несовместимости. Работает и эффект разделения затрат: покупая ПАК, компания оплачивает лишь долю вендорских расходов на R&D — она распределяется между множеством комплексов. При самостоятельной сборке заказчик несет все расходы: на исследования, операции и поддержку жизненного цикла. Сегодня отечественные ПАК все чаще выбирают как экономически более выгодный вариант»,— объясняет эксперт.

Отечественные решения для высоких нагрузок охватывают широкий спектр задач: проектирование устойчивых к пиковым нагрузкам архитектур, автоматическое масштабирование ресурсов, прогнозирование нагрузок с помощью ИИ-алгоритмов. Для отказоустойчивости применяют кластеры с репликацией, механизмами быстрого переключения и непрерывным мониторингом. Фундаментом инфраструктуры служат программно-аппаратные комплексы, где «железо» и ПО интегрированы как единое целое — это обеспечивает производительность и надежность. Кибербезопасность реализуется за счет защиты на уровне ядра, противодействия DDoS-атакам, шифрования и контроля доступа.

МИГРАЦИЯ БЕЗ ПРОСТОЕВ: СТРАТЕГИЯ ПЕРЕХОДА Кроме подведомственных учреждений комитета по информатизации и связи Санкт-Петербурга, которые реализуют основные диджитал-проекты в масштабах всего города, нуждаются в отказоустойчивой и масштабируемой инфраструктуре также и субъекты КИИ, предприятия энергетики, ТЭК и промышленности. ПАО «Россети Ленэнерго» — один из ключевых потребителей высоконагруженных решений в регионе. Ранее «Ъ Северо-Запад» поговорил с генеральным директором компании Игорем Кузьминым о том, как компания ведет системную работу по замене импортного оборудования на российские аналоги и переходит на отечественное программное обеспечение. Доля таких закупок по итогам 2025 года составила почти 98%.

Для компаний такого уровня важно провести миграцию в сжатые сроки, одновременно сокращая затраты на инфраструктуру, и сохранить высокую скорость масштабирования, подчеркивает господин Гилязов, добавляя, что главная задача — не просто заменить «железо» и софт, а сделать это так, чтобы бизнес не остановился, а после переезда система стала гибче.

«Имеет смысл брать только готовые доверенные ПАК. Это ключевой момент: когда вы покупаете не разрозненные компоненты, а комплекс, где аппаратная и программная части уже сбалансированы и прошли проверку на совместимость, вы сразу закрываете вопрос с комплаенсом и сильно сокращаете время на интеграцию. Вендор берет на себя часть рисков, и заказчику не нужно тратить ресурсы на то, чтобы „подружить" разные элементы. Это напрямую ускоряет миграцию и снижает скрытые издержки»,— рекомендует эксперт.

Он также советует строить архитектуру с запасом гибкости, делая упор на модульность: поскольку система состоит из независимых блоков, их можно мигрировать поэтапно, параллельно запуская уже перенесенные части. По его мнению, такой подход минимизирует простои и позволяет масштабировать отдельные компоненты под растущую нагрузку без полной перестройки системы, кроме того, модульная архитектура проще в управлении и лучше поддается автоматизации.

Эксперт предостерегает, что сжатые сроки миграции не стоит считать платой за производительность, а скорее наоборот. Преимущество ПАК в том, что вендор заранее оптимизирует весь стек: прошивки, BIOS, драйверы, гипервизор, СУБД под конкретные нагрузки. В самосборной инфраструктуре часть мощности теряется из-за неоптимальных настроек и несовместимости компонентов. Единый стек решает задачу меньшим числом узлов, это экономит бюджет на стойках, лицензиях, питании, охлаждении, что особенно важно для проектов КИИ.

«Если собрать все это вместе — готовые сертифицированные блоки, гибкую архитектуру и автоматизацию,— получится сбалансированный маршрут, который позволяет уложиться в регуляторные сроки, обеспечивает предсказуемую экономику эксплуатации и оставляет задел для дальнейшего роста»,— резюмирует Михаил Гилязов. ■

ЗАДВОЕНИЕ В ПРОМЫШЛЕННЫХ МАСШТАБАХ

ЦИФРОВЫЕ ДВОЙНИКИ ПОСТЕПЕННО ПЕРЕХОДЯТ ИЗ КАТЕГОРИИ ПИЛОТА В ДЕЙСТВУЮЩИЙ ИНСТРУМЕНТ ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ. НАИБОЛЬШИЙ СПРОС ФОРМИРУЮТ НЕФТЕГАЗОВЫЕ, ЭНЕРГЕТИЧЕСКИЕ, МЕТАЛЛУРГИЧЕСКИЕ, ХИМИЧЕСКИЕ И МАШИНОСТРОИТЕЛЬНЫЕ КОМПАНИИ, ДЛЯ КОТОРЫХ АВАРИИ И ПРОСТОИ СВЯЗАНЫ СО ЗНАЧИТЕЛЬНЫМИ ПОТЕРЯМИ. ОДНАКО РАСПРОСТРАНЕНИЕ ТЕХНОЛОГИИ СДЕРЖИВАЮТ НИЗКОЕ КАЧЕСТВО ДАННЫХ, ИЗНОШЕННОСТЬ ОБОРУДОВАНИЯ, ДЕФИЦИТ СПЕЦИАЛИСТОВ И ОТСУТСТВИЕ ЕДИНЫХ ПРАВИЛ ИНТЕГРАЦИИ, ОТМЕЧАЮТ ЭКСПЕРТЫ. ВИКТОР ИРИСОВ

Цифровой двойник представляет собой динамическую виртуальную модель физического объекта или процесса, которая регулярно получает информацию о его фактическом состоянии. В отличие от статической трехмерной модели, такая система позволяет анализировать отклонения, прогнозировать отказы и рассчитывать сценарии.

Чем дороже актив и чем выше цена отклонения от запланированного режима эксплуатации, тем очевиднее выгода от виртуальной модели, говорит руководитель проектов центра промышленной автоматизации «Айсорс» Игорь Ломухин, добавляя, что технология позволяет оптимизировать работу оборудования либо заблаговременно выявить риск отказа отдельного элемента или технологического процесса.

Аналитик ФГ «Финам» Леонид Делицын отмечает, что раньше вычислительные модели использовались преимущественно там, где натурный эксперимент был дорогим, длительным или опасным. По данным, которые приводит директор департамента решений АСТУ «Сигмы» Константин Сипачев, к 2025 году около половины нефтегазовых компаний уже управляют активами благодаря цифровым двойникам, а доля предприятий ТЭК с ИИ выросла с 29% (2021) до 58% (2024).



ЕВГЕНИЙ ПАВЛЕНКО

ПО ДАННЫМ ЭКСПЕРТОВ, ОКОЛО ПОЛОВИНЫ НЕФТЕГАЗОВЫХ КОМПАНИЙ В РОССИИ УЖЕ УПРАВЛЯЮТ АКТИВАМИ С ПОМОЩЬЮ ЦИФРОВЫХ ДВОЙНИКОВ

СТАДИЯ ВНЕДРЕНИЯ Управляющий партнер консалтинговой компании «1702» Артем Дмитренко относит российский рынок к стадии перехода от пилотов к более широкому внедрению. Среди примеров он называет использование цифровых моделей «Русалом» на глиноземных и алюминиевых производствах и применение двойников «Газпром нефтью» при бурении сложных скважин.

В промышленности формируется последовательная архитектура внедрения. «Показателен пример „СИБУР-Кстово“,— рассказывает господин Дмитренко.— Компания связывает комплекс цифровых технологий: автоматизацию, цифровые двойники и предиктивную аналитику. За последние пять лет энергопотребление предприятия снизилось на 15%, а коэффициент использования мощностей достиг 97%. Такая связка — датчики, цифровой двойник, аналитика, алгоритм оптимизации — становится типичной архитектурой современного промышленного проекта».

Однако наличие отдельных цифровых моделей еще не означает появления полноценного двойника предприятия. Директор по работе с ключевыми заказчиками ГК «СиСофт» Вадим Антонов указывает, что на российском рынке есть отечественные платформы для информационного моделирования промышленных активов и изделий, мониторинга оборудования и объективного контроля, но практически отсутствуют комплексные решения, способные отразить текущее состояние всего предприятия и моделировать его деятельность в реальном времени.

Такая система должна быть интегрирована с оперативно-диспетчерским управлением, средствами объективного контроля и другими источниками производственных данных. Ее задача не просто показывать состояние объекта, но и прогнозировать изменения, рассчитывать варианты действий и искать оптимальный режим управления. Поэтому проекты подобного масштаба остаются единичными, а сравнимой статистики по их эффективности в России недостаточно.

ЦИФРОВАЯ НЕЗРЕЛОСТЬ Главным ограничением использования двойников становится не отсутствие интереса, а цифровая зрелость предприятий. По оценке НИУ ВШЭ, которую приводит коммерческий директор ROXIT Антон Колосов, к полноценному внедрению цифровых двойников готовы не более 1% российских предприятий. Остальным требуется предварительно упорядочить ИТ-ландшафт и работу с данными.

Если системы управления производством, ресурсами, жизненным циклом изделий и технологическими процессами работают изолированно, справочники не синхронизированы, а значительная часть информации хранится в электронных таблицах или зависит от знаний отдельных технологов, построить достоверную модель затруднительно. В ряде случаев значительная часть бюджета расходуется не на разработку алгоритмов, а на сбор, очистку и сопоставление сведений.

Еще одним барьером остается изношенный парк оборудования. Старые станки и агрегаты часто не имеют штатных датчиков и интерфейсов передачи информации. Их дооснащение увеличивает стоимость проекта, а иногда оказывается технически или экономически невыгодным. Одновременно сохраняется проблема совместимости устаревших систем с современными аналитическими платформами.

Готовность персонала также влияет на результат. Предприятию необходимы специалисты, способные проверить математическую модель, интерпретировать прогноз и включить его в производственные регламенты. Руководители небольших предприятий, ориентированные на краткосрочные показатели, в свою очередь, не всегда готовы финансировать проект с эффектом через несколько лет.

Меньше интереса к технологии, по оценке господина Колосова, проявляют легкая промышленность и строительный сектор. В первом случае ограничениями выступают невысокая маржинальность и частая смена ассортимента. В строительстве цифровой двойник нередко отождествляют с BIM-моделью, хотя последняя преимущественно описывает объект, тогда как двойник должен постоянно получать эксплуатационные данные и моделировать его поведение.

Для небольшого производства с простыми и предсказуемыми операциями необходимость в сложной модели также ограничена. Общая закономерность, по словам господина Делицына, заключается в том, что потребность в двойнике возрастает вместе со сложностью системы и величиной потенциальных потерь.

ЭКОНОМИКА ВХОДА Единой оценки стоимости и срока возврата инвестиций для цифровых двойников нет. Наиболее предсказуемую экономику имеют локальные решения, привязанные к конкретной дорогостоящей проблеме. По оценкам экспертов, модель отдельного узла или процесса в успешном проекте может окупиться примерно за полтора-два года. Источником возврата инвестиций становятся, например, снижение расхода топлива на энергетическом объекте или повышение качества сплава в металлургии.

Двойник цеха или предприятия требует более продолжительного горизонта. Антон Колосов оценивает его в три года и более, отмечая повышенный риск недостижения планового эффекта. Игорь Ломухин говорит о диапазоне от трех до пяти лет для крупных объектов. По его оценке, создание полноценной модели может стоить от десятков до сотен миллионов рублей в зависимости от детализации и числа интегрируемых подсистем.

При этом расходы не ограничиваются лицензиями и разработкой модели. Предприятию требуются датчики, сети промышленного интернета вещей, вычислительные мощности, интеграция с ERP, MES, PLM, CAD, SCADA и АСУ ТП, очистка исторических данных, верификация результатов и защита инфраструктуры. После запуска возникают постоянные затраты на обновление, калибровку, информационную безопасность и содержание команды сопровождения.

Константин Сипачев приводит пример системы удаленного мониторинга с предиктивной аналитикой в одном из крупных энергетических холдингов. «Это позволяет избежать ущерба на 264 млн рублей за 24 месяца. Однако внедрению мешают нехватка данных, потребность в больших вычислительных мощностях и строгие требования к кибербезопасности на всех этапах жизненного цикла ИИ»,— резюмирует эксперт.

ПРОБЛЕМАТИКА ПОДДЕРЖКИ Участники рынка считают меры государственной поддержки необходимыми, однако предлагают связывать их с достижением производственного эффекта. Среди возможных инструментов эксперты предлагают софинансирование первых внедрений и последующего тиражирования, создание испытательных полигонов, льготный доступ к вычислительной инфраструктуре, подготовку инженеров и поддержку совместимости российских решений.

Государственная политика также должна снижать зависимость от зарубежных платформ, полагает Леонид Делицын: «Без поддержки отечественных платформ все станет пронизано решениями от Open AI, DeepSeek и т. д., без которых не смогут работать. А такая зависимость создает долгосрочные риски».

Антон Колосов ссылается на «дорожную карту» Минцифры, разработанную НИУ ВШЭ. Она предусматривает введение в 2026–2027 годах правил обращения с промышленными данными и поддержку двойников уровня цеха. На более длительном горизонте, к 2034 году, рассматривается возможность обязательного применения технологии крупными высокотехнологичными промышленными компаниями. Конкретные параметры таких требований и поддержки еще предстоит определить.

Отдельной задачей остается правовой режим промышленных данных. Сейчас они могут подпадать под нормы о коммерческой тайне, персональных данных или защите критической информационной инфраструктуры, однако самостоятельная и единообразно регулируемая категория отсутствует. Это осложняет обмен сведениями между заказчиками, производителями оборудования, разработчиками программного обеспечения и интеграторами.

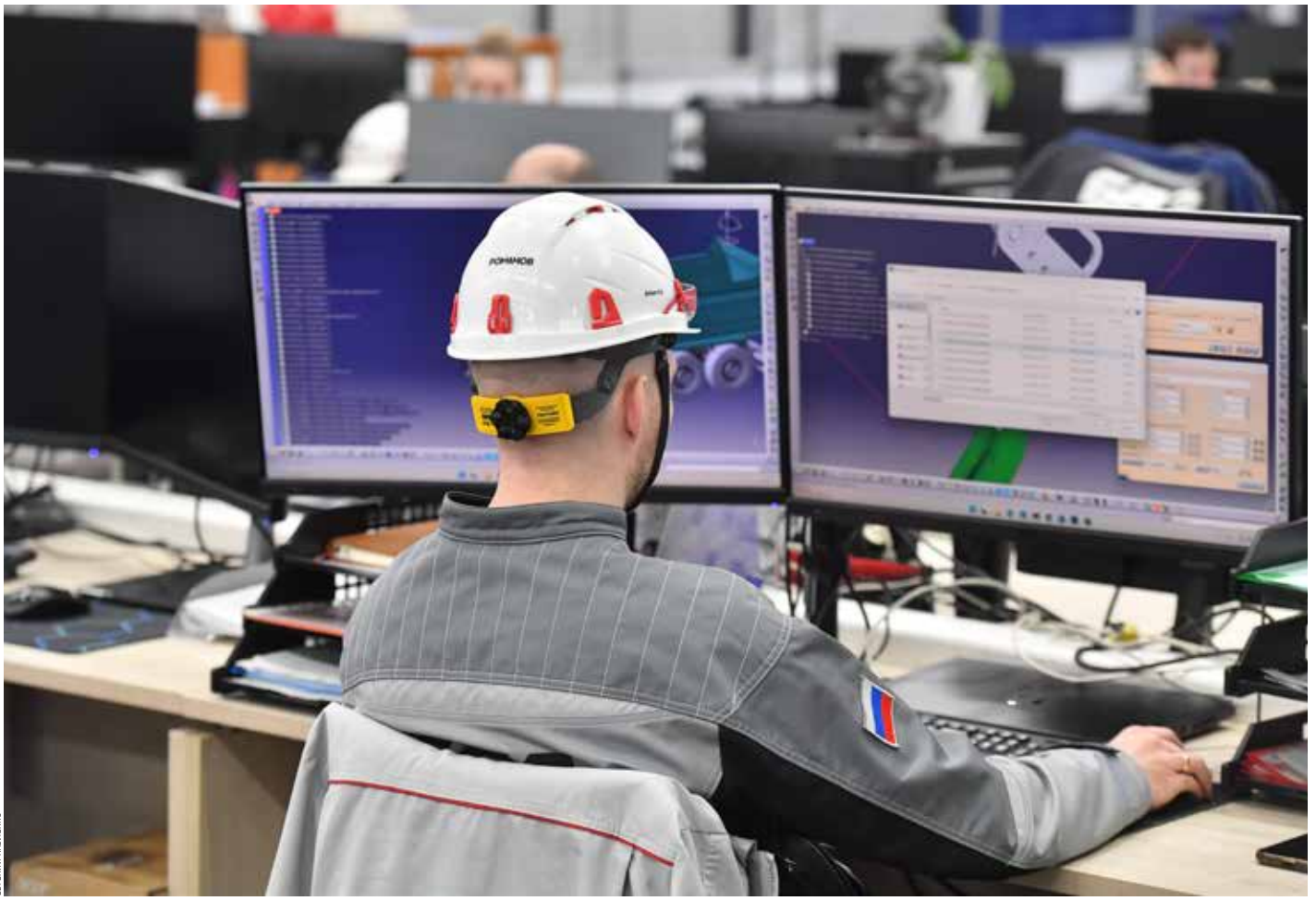
Базовые определения закреплены в ГОСТ Р 57700.37. Участники рынка полагают, что следующий этап стандартизации должен касаться прежде всего «стыков» между системами. Необходимы единые подходы к идентификации объектов и параметров, передаче временных рядов, описанию версий моделей, фиксации происхождения и качества данных, верификации расчетов и обеспечению кибербезопасности.

Стандартизация интерфейсов должна также дать предприятиям возможность менять поставщиков без полного пересоздания модели. В противном случае каждый цифровой двойник превращается в закрытую индивидуальную разработку, а стоимость масштабирования возрастает. ■

НОЛЬ ДОВЕРИЯ

РОСТ ЧИСЛА КИБЕРАТАК И ВРЕДОНОСНЫХ ВНЕДРЕНИЙ ЧЕРЕЗ ПОДРЯДЧИКОВ ЗАСТАВЛЯЕТ ПРОМЫШЛЕННИКОВ ПЕРЕСМАТРИВАТЬ ПЕРИМЕТРОВУЮ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. АРХИТЕКТУРА ZERO TRUST ПРЕДПОЛАГАЕТ ПРОВЕРКУ КАЖДОГО ПОЛЬЗОВАТЕЛЯ, УСТРОЙСТВА И ПРИЛОЖЕНИЯ, А ТАКЖЕ РАЗДЕЛЕНИЕ ИНФРАСТРУКТУРЫ НА ИЗОЛИРОВАННЫЕ СЕГМЕНТЫ. ТАКОЙ ПОДХОД ОГРАНИЧИВАЕТ РАСПРОСТРАНЕНИЕ АТАКИ, ОДНАКО ЕГО ВНЕДРЕНИЕ НА ПРОИЗВОДСТВЕ ТРЕБУЕТ УЧЕТА НЕПРЕРЫВНОСТИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И ОБХОДИТСЯ НЕДЕШЕВО. ВИКТОР ИРИСОВ

По данным ИБ-компании «Бастион», около 94% проведенных ею внутренних тестов на проникновение завершилось полным захватом корпоративной сети. Аналитики изучили защищенность более 300 компаний из разных отраслей. Годом ранее доля успешных проникновений составляла 85,7%. Общее количество кибератак за год выросло на 25%, утверждают в «Бастионе». На партнеров и подрядчиков с менее защищенной инфраструктурой пришлось 26% успешных атак. По оценке RED Security, с атаками через подрядчиков была связана треть расследованных инцидентов компрометации инфраструктуры российских компаний, тогда как годом ранее их доля не превышала 10%.



ЕВГЕНИЙ ПАВЛЕНКО

ЭКСПЕРТЫ ОТМЕЧАЮТ, ЧТО ПРИ НЕДОСТАТОЧНОЙ ЗРЕЛОСТИ ПРОЦЕССОВ ОШИБОЧНАЯ РЕАЛИЗАЦИЯ ZERO TRUST МОЖЕТ ПОВЫСИТЬ УЯЗВИМОСТЬ ИНФРАСТРУКТУРЫ

ПОТЕНЦИАЛЬНАЯ КОМПРОМЕТАЦИЯ

Zero Trust, или модель нулевого доверия, исходит из того, что любые пользователи, устройства или приложения по умолчанию считаются потенциально скомпрометированными. Доверие не предоставляется на основании нахождения внутри корпоративного периметра: каждый запрос требует идентификации и проверки, а доступ ограничивается минимально необходимым набором ресурсов.

На место классического сетевого периметра приходит микросегментация, а в основе подхода находится идентификация: каждый запрос автоматически проверяется, а пользователю предоставляются минимально необходимые права доступа только к отдельным разрешенным ресурсам, объясняет руководитель направления продуктовой безопасности Selectel Антон Ведерников. По его словам, эта модель особенно актуальна для облачной и распределенной инфраструктуры, с которой одновременно работают сотрудники и внешние подрядчики.

Микросегментация предполагает разделение сети на отдельные зоны с собственными политиками доступа. Если злоумышленник получает контроль над одним устройством или сервисом, его возможности ограничиваются настройками этого компонента. Это препятствует горизонтальному перемещению внутри сети, повышению привилегий и последующей компрометации критически важных систем.

Ведущий специалист отдела продвижения продуктов «Кода Безопасности» Дмитрий Лебедев сравнивает микросегменты с отсеками океанского судна, где при пробоине в одном из отсеков, то есть при компрометации одного сегмента, закрывается переборка, соединяющая его с другими отсеками-сегментами. Таким образом, злоумышленники получают доступ к ограниченному количеству данных и не могут серьезным образом повлиять на всю инфраструктуру.

Для промышленных предприятий Zero Trust имеет дополнительное значение из-за соседства корпоративной ИТ-инфраструктуры и технологических сетей, управляющих оборудованием. Компрометация офисного сегмента сама по себе не должна давать злоумышленнику возможность перейти к системам промышленной автоматизации.

Вместе с тем механическое применение корпоративных политик безопасности в технологической среде может создавать операционные риски. При внедрении Zero Trust необходимо учитывать требования к непрерывной работе оборудования, недопустимость незапланированных простоев, ограниченные возможности обновления устаревших систем и необходимость удаленного доступа производителей и сервисных подрядчиков.

Если злоумышленнику удается получить доступ к одному из компонентов системы, его возможности ограничены правами и сетевыми настройками этого компонента, говорит господин Ведерников. При этом компании должны заранее определить, каким специалистам и на какой срок необходим доступ к конкретным производственным системам, а также предусмотреть порядок действий при отказе средств идентификации.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Эффективность Zero Trust зависит не только от набора технических решений. До начала проекта необходимо инвентаризировать инфраструктуру, описать бизнес-процессы и потоков данных, распределение зон ответственности и разработка политик доступа. После внедрить постоянный мониторинг, пересмотр прав, поиск уязвимостей и проведение киберучений.

По оценке господина Лебедева, при недостаточной зрелости процессов ошибочная реализация модели может, напротив, повысить уязвимость инфраструктуры. Например, концентрация расширенных прав у одного-двух сотрудников формирует новую критическую точку отказа.

Техническая сегментация не устраняет риски, связанные с действиями сотрудников. По данным «Бастиона», только 1% работников сообщает службе безопасности о подозрительных письмах, тогда как 16% переходят по вредоносным ссылкам.

Одновременно снижается стоимость первоначального доступа к корпоративным сетям. Как утверждают в «Бастионе», на теневом рынке такой доступ может стоить $10–50. Криминальная инфраструктура эволюционирует от отдельных сервисных моделей, включая программы-вымогатели и фишинг как услугу, к Crime-as-a-Service — комплексному предложению инструментов для проведения атак.

На этом фоне проверка только при входе в сеть оказывается недостаточной. Zero Trust предусматривает повторную оценку пользователя и устройства на разных этапах работы. Во внимание могут приниматься география подключения, характеристики устройства и нетипичное поведение учетной записи. При обнаружении аномалий доступ блокируется либо требует дополнительного подтверждения.

ИИ В КОНТУР

Распространение корпоративных систем генеративного искусственного интеллекта расширяет область применения Zero Trust. Языковые модели и ИИ-агенты получают доступ к документам, базам данных и внутренним сервисам, фактически превращаясь в самостоятельный тип учетной записи.

К ним принципы Zero Trust применимы буквально, отмечает технический директор направления GenAI Just AI Антон Сипачев. При использовании внешних облачных моделей между сотрудником и сервисом, по его словам, необходим шлюз, способный выявлять и маскировать персональные и конфиденциальные данные.

Для моделей, развернутых внутри корпоративного контура, возникает другая задача. Система, подключенная к внутренней базе знаний, должна наследовать права конкретного пользователя: сотрудник не должен получать через чат-бот документы, недоступные ему напрямую.

Дополнительным риском становится prompt injection — внедрение скрытой вредоносной инструкции в документ, письмо или другой источник, который обрабатывает ИИ. Получив такую команду, агент с избыточными полномочиями может обратиться к закрытым данным или выполнить нежелательное действие. Поэтому его права необходимо ограничивать, а запросы, ответы и обращения к сервисам нужно регистрировать и проверять, полагает господин Сипачев.

К преимуществам Zero Trust участники рынка относят сокращение поверхности атаки, ограничение последствий компрометации и повышение прозрачности инфраструктуры для ИТ- и ИБ-подразделений.

Основными препятствиями остаются стоимость и сложность внедрения. Компаниям приходится пересматривать сетевую архитектуру, модели управления доступом, порядок взаимодействия с подрядчиками и процедуры эксплуатации производственного оборудования. ■

ГОРОД НАШЕЙ СЛАВЫ ЦИФРОВОЙ

САНКТ-ПЕТЕРБУРГ И ЛЕНИНГРАДСКАЯ ОБЛАСТЬ СЕГОДНЯ ЗАНИМАЮТ ЛИДИРУЮЩИЕ ПОЗИЦИИ В РЕЙТИНГЕ РЕГИОНОВ СЕВЕРО-ЗАПАДНОГО ФЕДЕРАЛЬНОГО ОКРУГА ПО УРОВНЮ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ. В ОБОИХ СУБЪЕКТАХ ВОТ УЖЕ НА ПРОТЯЖЕНИИ НЕСКОЛЬКИХ ЛЕТ ПРОДОЛЖАЕТСЯ МАСШТАБНАЯ КАМПАНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ, ПРЕДПОЛАГАЮЩАЯ ОБШИРНОЕ ВНЕДРЕНИЕ ИИ, ПЕРЕХОД НА ОТЕЧЕСТВЕННОЕ ПО ВЗАМЕН ИНОСТРАННОГО, ПЕРЕВОД В ЦИФРУ БОЛЬШИНСТВА ГОСУДАРСТВЕННЫХ СОЦИАЛЬНЫХ ИНСТРУМЕНТОВ И УСЛУГ, А ТАКЖЕ МНОГИЕ ДРУГИЕ ВАЖНЫЕ СОСТАВЛЯЮЩИЕ. В ТОМ, КАК ПРОДВИГАЕТСЯ ЭТОТ ПРОЦЕСС, В КАКИХ АСПЕКТАХ УДАЛОСЬ ДОСТИЧЬ ЗАМЕТНОГО УСПЕХА, А НА КАКИЕ СТОИТ ОБРАТИТЬ ОСОБОЕ ВНИМАНИЕ В БЛИЖАЙШЕЙ ПЕРСПЕКТИВЕ, РАЗБИРАЛСЯ НИКОЛАЙ КОЗИН.

ОТ «ЛОСКУТНОЙ АВТОМАТИЗАЦИИ» К ЕДИНОЙ СИСТЕМЕ Впервые Стратегию цифровой трансформации Санкт-Петербурга приняли в 2021 году. Как сообщала городская администрация, она включала список из 78 конкретных проектов — от организации быстрой медицинской диагностики для борьбы с особо опасными заболеваниями до разработки передовых электронных сервисов для внутреннего туризма.

За минувшие годы стратегия неоднократно дополнялась и редактировалась. Так, в 2022 году в нее включили две новые отрасли: «Безопасность» и «Экологию и природопользование». Также был запущен масштабный проект по переводу органов власти на отечественное ПО. А в 2025 году был открыт новый, рассчитанный на ближайшую пятилетку этап, основная цель которого — обеспечить более глубокую интеграцию технологий во все сферы жизни города.

В целом, как отмечают эксперты, цифровая трансформация Петербурга — это важный прецедент перехода от «лоскутной автоматизации» к единой цифровой экосистеме управления мегаполисом.

«Главным успехом петербургской модели стал переход от сбора данных к принятию управленческих решений на их основе в режиме реального времени, благодаря чему стратегия трансформировалась из регуляторного документа в эффективную институциональную среду»,— отмечает проректор по цифровому развитию, директор научно-образовательного центра урбанистики и киберантропологии Ленинградского государственного университета имени А. С. Пушкина Арсений Майоров.



АЛЕКСАНДР КОРЖОВ

СЕЙЧАС В ПЕТЕРБУРГЕ РАБОТАЕТ БОЛЕЕ 115 КАМЕР ВИДЕОНАБЛЮДЕНИЯ, КОТОРЫЕ ОБЪЕДИНЕНЫ В ЕДИНУЮ ГОРОДСКУЮ СИСТЕМУ ДЛЯ ЦИФРОВИЗАЦИИ

ЖИЗНЬ ПОД ВЛИЯНИЕМ ИИ Особые успехи, по словам независимых экспертов, город демонстрирует в части внедрения сервисов на основе искусственного интеллекта.

«ИИ сегодня без преувеличения пронизывает все сферы жизни Северной столицы,— рассказывает депутат Законодательного собрания Санкт-Петербурга, председатель постоянной комиссии по молодежной политике, делам общественных объединений и цифровизации Андрей Малков.— Его широкое внедрение позволило сформировать единый цифровой контур управления городом, повысить связность органов власти и упростить межведомственное взаимодействие».

В качестве примера он привел приложение «Я здесь живу», запущенное в 2022 году и аккумулировавшее в себе 16 городских сервисов. Сегодня, по словам парламентария, это не просто универсальный помощник, при помощи которого петербуржцы могут узнать об интересных местах в своем районе, подобрать детский сад ребенку или пожаловаться на проблемы в области ЖКХ, но и полноценный инструмент для координации городских властей и служб.

«Раньше при обращении за помощью велика была вероятность ошибок: к примеру, гражданин по незнанию адресовывал вопрос, находящийся в ведении муниципальных органов, комитету по благоустройству или наоборот,— поясняет Антон Малков.— Из-за этого нарушалась подведомственность, возникала бюрократическая волокита, а сроки решения проблем затягивались. Сегодня такие ошибки полностью исключены благодаря ИИ-агентам, которые анализируют каждую жалобу».

В числе других наиболее значимых систем и сервисов, появившихся в рамках цифровой трансформации, собеседники издания выделили нейросетевой комплекс «Городовой», интегрированный с системой «Безопасный город», которая охватывает более 80 тыс. наружных камер видеонаблюдения. Его появление позволило перевести контроль благоустройства в автоматический режим, где искусственный интеллект самостоятельно фиксирует нарушения и формирует предписания без человеческого фактора.

«В социально-управленческом контуре „Единая карта петербуржца“ и ситуационные панели „Дашборда губернатора“ обеспечили сквозной мониторинг государственных услуг, а в здравоохранении массово внедряются сервисы электронных рецептов, биометрия и алгоритмы компьютерного зрения для анализа медицинских снимков»,— заключает Арсений Майоров.

Вместе с тем ряд аспектов в цифровой трансформации города требует повышенного внимания. Так, по словам господина Майорова, внедрение и развитие некоторых перспективных систем и сервисов заметно тормозится из-за столкновения «цифровой онтологии и физической реальности».

«В частности, в секторе ЖКХ дворовое хозяйство разделено между множеством частных управляющих компаний и ТСЖ, где неоднородность данных и отсутствие единых стандартов технологического учета затрудняют создание цифрового двойника жилищного фонда,— поясняет эксперт.— Построение системы экологического мониторинга замедляется из-за высокой капиталоемкости IoT-сенсоров и необходимости импортозамещения „железа“».

Антон Малков, в свою очередь, отметил потребность в точечных улучшениях. Так, например, по словам парламентария, имеет смысл подумать о разработке и массовом применении «умных» датчиков для мусорных контейнеров, которые динамически отображали бы степень их загрузки, чтобы компании, занимающиеся вывозом ТКО, имели возможность рационально выстраивать маршруты для техники.

СИНЕРГИЯ СУБЪЕКТОВ Параллельно с Санкт-Петербургом свою цифровую трансформацию ведет и Ленинградская область. Эта работа стартовала в регионе в 2022 году и изначально включала в себя 16 направлений — от государственного управления и оказания госуслуг до транспорта, логистики, сельского хозяйства и социальной сферы.

По состоянию на 2025 год цифровизация региона продолжалась активно и успешно: так, по словам председателя комитета цифрового развития Андрея Сытника, степень цифровой зрелости отраслей экономики Ленобласти составляла 67,6%, что более чем в полтора раза превышало плановые показатели Минцифры (38,9%).

«В 2025 году наибольшее значение индикаторов, входящих в цифровую зрелость Ленинградской области, достигнуто в отраслях „Госуправление“ (99,9%), „Здравоохранение“ (97,9%), „Транспорт“ (87,5%), „Образование (общее)“ (60%). За этими цифрами стоят прежде всего упрощение и ускорение доступа к важным услугам»,— отмечал господин Сытник.

При этом, по словам экспертов, Петербург и Ленобласть, следуя давним принципам общности, цифровые экосистемы развивают во многом с опорой друг на друга.

«В сквозных векторах цифровизации Санкт-Петербург и Ленинградская область демонстрируют агломерационный резонанс, где переход на отечественный софт подталкивается нормативными дедлайнами по защите объектов критической информационной инфраструктуры, а межведомственное взаимодействие в рамках десятков ГИС обоих регионов сдерживается феноменом „ведомственной разобщенности“ и нежеланием делиться первичными дата-сетами, но подталкивается федеральной вертикалью и переходом на сервисные модели «жизненных ситуаций»,— отмечает господин Майоров.

В заключение эксперты отметили еще одно перспективное направление цифровизации в Петербурге и Ленобласти: разработку местными командами готовых решений с их последующим тиражированием или продажей в другие регионы.

«В этом плане тот же Петербург обладает прекрасной научно-производственной базой,— уточнил председатель Совета Фонда развития цифровой экономики Герман Клименко.— В качестве примера можно привести Первый мед (Первый Санкт-Петербургский государственный медицинский университет имени академика И. П. Павлова), который располагает передовыми наработками по части распознавания опасных заболеваний, таких как рак шейки матки. Даже специалисты из Москвы признают здесь его первенство».

По словам господина Клименко, серьезными драйверами этого процесса могут выступать также Университет ИТМО, СПбГУ, Политех, объединение ЛОМО. Перечень вузов говорит о том, что научно-производственный задел уже сформирован — и в будущем именно он может вывести Петербург и Ленобласть на ведущие позиции в списке тех регионов, которые не только создают цифровые решения для себя, но и являются драйверами цифрового развития всей страны. ■

Тематическое приложение к газете «Коммерсантъ» (онлайн-выпуск Северо-Запад. Guide «Цифровая экономика»)

Роман Уманский — генеральный директор АО «Коммерсантъ»
Михаил Лукин — главный редактор
Анатолий Гусев — автор дизайн-макета
Андрей Ершов — главный редактор СПб страниц
Александр Коряков — бильд-редактор
Ксения Ахметжанова — выпускающий редактор
Марина Шевченко — корректор
Василиса Сатирская — верстка
Григорий Матыжев — рекламная служба

Адрес редакции и издателя: 127006, г. Москва, Оружейный пер., д. 41. Тел. (495) 797-6970. Адрес редакции в Санкт-Петербурге: 191024, Харьковская ул., д. 8А, лит А. Тел. (812) 324-6949

Учредитель: АО «Коммерсантъ». Тематическое приложение к газете «Коммерсантъ», зарегистрировано Роскомнадзором, регистрационный номер и дата принятия решения о регистрации ПИ №ФС77-76923 от 11.10.2019 года

В печатном виде номер не выходит. Распространяется бесплатно. 16+

Фото на обложке: Евгений Павленко