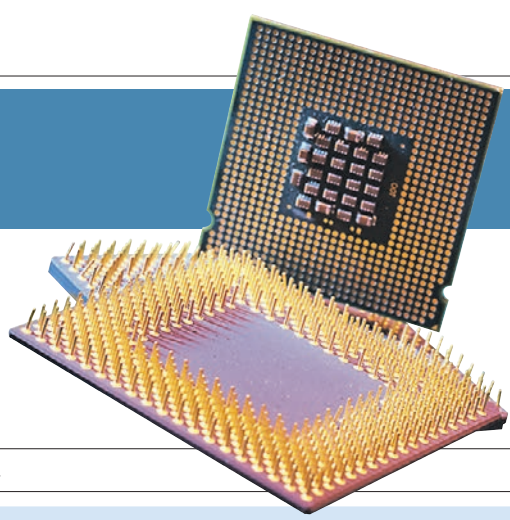




17 Как ИИ применяется в госсекторе и бизнесе в 2025 году

19 Почему финтех оказывается востребован в промышленности

22 Как меняются подходы бизнеса к кибербезопасности в 2025 году

IT сбавляет обороты

В 2025 году рост российской IT-индустрии начал замедляться, в то же время компании столкнулись с новыми правилами для включения в реестр отечественного программного обеспечения, который дает преимущества для госзакупок. Минцифры также ужесточило правила, по которым IT-бизнес может получить аккредитацию и претендовать на налоговые и другие льготы. С какими итогами индустрия заканчивает 2025 год и какие прогнозы дает на 2026-й, разбирались «Ъ-Информационные технологии».

— компании и рынки —

Цифры и факты

В 2025 году динамика роста российского IT-рынка значительно замедлилась. По оценке ВШЭ, только за первое полугодие индустрия выросла на 14,6% по сравнению с аналогичным периодом прошлого года и достигла 1,9 трлн руб., в то время как в 2024 году за первые шесть месяцев рынок вырос на 60% год к году, заявлял глава Минцифры Максуд Шадаев. Однако пока индустрия растет все еще быстрее показателя по экономике в целом, который в 2025 году составлял 3,2%. По прогнозам, совокупно по итогам года рост сектора может составить 15% (3,85–4 трлн руб.). При этом инвестиции IT-отрасли за первое полугодие 2025 года составили 300 млрд руб. и столько же вложили компании в радиоэлектронику за последние три года. Об этом сообщил премьер-министр Михаил Мишустин на форуме «Цифровые решения».

Основными драйверами являются развитие облачных сервисов, импортозамещение, цифровая трансформация бизнеса, а также повышение спроса на решения в области ИИ и высокопроизводительных вычислений, что связано с растущими потребностями в обработке данных и машинном обучении. Доля российских разработок, по оценке ITGlobal.com, достигла более 50% в ряде сегментов, включая инфраструктурное ПО, а в некоторых категориях, например в системах виртуализации, уже превышает 70%.

Однако из-за высокой ключевой ставки компании сталкиваются со сложностями в обслуживании кредитов и привлечении финансирования. На форуме «Цифровые решения» директор департамента по работе с эмитентами Московской биржи Наталья Логинова заявила, что прогнозирует консолидацию для IT-рынка в 2026 году: «Скорее всего, в IT-секторе мы увидим консолидацию, когда крупные игроки начнут увеличивать долю рынка за счет М&А. Поэтому следующий год для IT-индустрии на рынке капитала будет реально тяжелым».

Реестровые войны

В 2025 году IT-отрасль столкнулась с новым регулированием, которое, с одной стороны, наложило на нее

новые обязательства, а с другой — открыло возможности для роста. В частности, ужесточились правила включения в реестр отечественного ПО, который дает преференции при госзакупках. Минцифры добавило требование о совместимости ПО с двумя российскими операционными системами. Также в реестре появилась информация о соответствии программы требованиям доверенного ПО. Помимо этого, вводится понятие «контроль» для коммерческой организации. Теперь при включении в реестр ПО будут учитываться особенности корпоративной структуры компаний. Например, кому принадлежит большинство акций, через какие механизмы принимаются решения и т. д. Получить IT-аккредитацию при Минцифры тоже стало сложнее: министерство разработало новые требования к сайтам IT-компаний, которые вступили в силу в ноябре.

В числе ключевых законодательных нововведений сам бизнес отмечает изменения в закон «О безопасности КИИ». «Также это публикация 117-го приказа ФСТЭК России и его вступление в силу в марте 2026 года. Он переформатировал требования к защите информации и ввел общую логику мер для разных типов информационных систем. Это не обновление пунктов, это новая методология: журналирование, контроль доступа, управляемость уязвимостей, обеспечение непрерывности теперь должны выполняться по единым, значительно более строгим критериям», — отметил технический директор ЦЗИ ООО «Конфидент» Дмитрий Шангин. Он напомнил, что новые требования к совместимости с отечественными ОС для вендоров означают, что «бездоказанного соответствия и прозрачного жизненного цикла доступ к крупным корпоративным проектам закрыт».

Если говорить о позитивных изменениях, то заметно ужесточилось регулирование в части импортозамещения, но это не всегда воспринимается как плюс, хотя для рынка это действительно драйвер, поскольку заказчики активнее переходят на отечественные продукты, добавляет гендиректор вендора инфраструктурного ПО «Базис» Давид Мартиросов. По его мнению, важным шагом стала инициатива Минцифры по



созданию двухуровневого реестра: «Мы давно выступали за подобную систему и считаем ее появлением значимым и полезным событием».

В целом 2025 год показал рост лояльности заказчиков к российскому ПО, говорят участники рынка. «Первичный скепсис ушел, и стало очевидно, что на отечественных решениях можно стабильно работать каждый день и они выдерживают серьезные нагрузки — наши внедрения это подтверждают. Появились и национальные „чемпионы“, которые сохраняют высокую динамику даже в условиях активного импортозамещения», — заключает Давид Мартиросов.

Налоговые прения

Если говорить о негативных факторах, то это в основном дополнитель-

ная нагрузка на заказчиков и продолжающаяся оптимизация IT-бюджетов, отмечают участники рынка. Дело в том, что сейчас НДС для всех компаний составляет 20%, но для IT-сектора с 2021 года действует нулевая ставка. Она была введена в рамках «IT-маневра», утвержденного правительством в 2020 году. В сентябре Минфин предложил отказаться от нулевого НДС для отечественного ПО, а также увеличить льготный тариф страховых взносов для IT-компаний с текущих 7,6% до 15%. Эти инициативы вызвали негативную реакцию отраслевых ассоциаций, в результате в октябре курирующий отрасль вице-премьер Дмитрий Григоренко заявил, что льгота по НДС для отечественных разработчиков программного обеспече-

ния будет сохранена. Однако повышение страховых взносов все еще обсуждается.

В связи с этим в ноябре участники рынка снова обратились в правительство. Среди новых предложений — постепенное увеличение страховых взносов вместо разового с 2026 года, списание задолженности при отрицательном салдо и сохранение преференций для IT-компаний — резидентов «Сколково». Эти предложения были направлены в начале ноября рабочей группой по цифровизации при уполномоченном по защите прав предпринимателей в Москве министру финансов Антону Силуанову.

Сейчас компании вынуждены вкладывать значительные ресурсы, чтобы соответствовать новым тре-

бованиям, строить комплаенс-процессы, IT-аудит и внутренние обучающие программы, отмечает советник гендиректора по юридическим вопросам ГК «Цифра» Андрей Яцков: «Новое регулирование ускоряет консолидацию рынка вокруг крупных игроков, способных создать устойчивые технологические стеки, соответствующие требованиям безопасности и технологического суверенитета». Консолидацию рынка прогнозируют и на Мосбирже, о чем заявила директор департамента по работе с эмитентами Московской биржи Наталья Логинова на форуме «Цифровые решения».

При этом малые и средние компании мигрируют на модели SaaS и партнерские экосистемы, сокращая операционные расходы на собственные инфраструктуры, фокусируясь на прикладных и нишевых продуктах, говорит Андрей Яцков: «Усиление требований к ПО из реестра в то же время делает отрасль более зрелой, растет качество продуктов, ускоряется устранение уязвимостей, внедряются высокие стандарты развития и поддержки программных продуктов».

Присущий всем ИИ

Санкционная изоляция в значительной степени стимулирует локальный IT-рынок к созданию собственного суверенного технологического стека, однако глобальные тренды, например развитие искусственного интеллекта и наращивание кибербезопасности, все же влияют на наш рынок, отмечает Андрей Яцков. В числе главных трендов 2025 года он перечисляет импортозамещающее ПО, встраиваемые финтех-решения, развитие суверенной цифровой инфраструктуры, новые технологические стандарты безопасности, платформенные AI-сервисы и интеллектуальную автоматизацию. «Особое внимание следует обратить на проблемы совместимости ПО с отечественными процессорами и новые стандарты криптозащиты, а также освоение промышленных AI (ИИ) решений», — добавляет эксперт.

Сегодня больше всего внимания привлекает искусственный интеллект, согласен Давид Мартиросов. При этом, по его мнению, рынок заметно перегрет — тема обсуждается куда активнее, чем видны реальные прикладные эффекты. «Практикоориентированных решений пока меньше, чем хотелось бы. Но очевидно, что ИИ надолго становится частью технологической повестки, и его значение будет только расти», — прогнозирует эксперт. Исполнительный директор «Нанософт разработок» Максим Егоров также говорит о тренде в развитии ИИ: от ИИ-Spilot для проектировщиков до агентного ИИ для автоматизации DevOps — это ядро конкуренции. Еще один тренд, по его словам, — облачные и гибридные решения. «Это ключ к снижению их цены и выходу на малый и средний бизнес», — напоминает он.

Светлана Бодрова

Цифровой случай

— компании и рынки —

Рынок страхования идет по пути тесного партнерства с IT и цифровизацией. Участники рынка уже активно развивают киберстрахование как отдельный продукт и встраивают новые цифровые решения в другие проекты. Кроме того, на рынок страхования выходят маркетплейсы и классифайды. В результате может улучшиться клиентский опыт и повыситься конкуренция на страховом рынке, считают эксперты.

Страховое открытие

Большая часть страховщиков (71%) ожидает медленного, но планомерного роста рынка киберстрахования, следует из данных страхового брокера АСТ. По оценкам экспертов, темпы роста будут двузначными из-за эффекта низкой базы. В частности, по итогам 2026 года эксперты ожидают увеличения объема рынка на 15–20% (см. «Ъ» от 9 ноября). По оценкам совладельца страхового брокера Mains Сергея Худякова, по итогам 2024 года объем рынка киберстрахования составил около 3 млрд руб., а к концу этого года вырастет до 3,5–4 млрд руб.

Опираясь на рост обращений к страховым компаниям — их количество увеличилось за девять месяцев 2025 года более чем

на 50%, прогноз роста страховых премий может составить около 20% в год, отмечает заместитель гендиректора АСТ Максим Сапожников. В ближайшие два-три года при благоприятных обстоятельствах рынок киберстрахования может составить от 5 млрд до 10 млрд руб., оценивает руководитель управления страхования финансовых рисков «АльфаСтрахования» Алина Малышева.

● Киберстрахование защищает бизнес от рисков, связанных с использованием интернета, хранением и обработкой данных, а также работой IT-инфраструктурой. Полис обычно покрывает убытки, наступившие в результате кибератаки, действий нелегальных сотрудников, технических сбоев. К ним относятся потери от перерыва в деятельности, компенсация вреда третьим лицам, расходы на восстановление работоспособности IT-систем, расследование происшествий, дешифрование данных.

Значительная часть страховщиков (43%) в сегменте киберстрахования предлагает лимиты от 100 млн до 500 млн руб., 30% — от 10 млн до 100 млн руб., следует из исследования страхового брокера АСТ. Цена полиса составляет примерно 1–3% от покрытия, оценивают эксперты. Страхованием киберрисков занимаются восемь компаний, в частности такие крупные игроки,

как «Ингосстрах», «АльфаСтрахование», «Сбербанк страхование», «Согаз», ВСК.

Среди причин роста страховщики в первую очередь видят цифровизацию и рост атак на компании. «С ростом уровня цифровизации в экономике увеличивается зависимость бизнес-процессов компаний от информационных технологий, одновременно все чаще происходят кибератаки», — говорит госпожа Малышева. По словам господина Худякова, размер ущерба от кибератак за 2023–2024 годы оценивается минимум в 1 трлн руб. В среднем по одному инциденту ущерб от утечки информации достигает 11,5 млн руб., а по максимальным оценкам пострадавших организаций — более 41 млн руб.

Ужесточение регуляторных требований к хранению и обработке данных, а также введение оборотных штрафов за утечки персональной информации мотивируют компании уделять данному вопросу больше внимания, добавляет в «Согазе». При этом, по словам экспертов компании, интерес к киберстрахованию растет не только у крупного бизнеса: «Потенциал мы видим и в сегменте малых и средних предприятий, особенно работающих с персональными данными в таких сферах, как онлайн-образование, медицина, интернет-магазины, или которые являются подрядчиками крупных корпораций».

Очевиден тренд к интеграции киберстрахования в комплексной кибербезопасностью бизнеса, появлению новых продуктов и увеличению числа полисов у малых компаний, что способствует распространению культуры риск-менеджмента в цифровой среде, уверяют эксперты «Согаз». Киберстрахование, безусловно, получит гораздо более широкое распространение и станет таким же обыденным, как страхование имущества и автотранспорта, подтверждает заместитель гендиректора по андеррайтингу страховой компании «Двадцать первый век» Евгений Изотов.

Участники рынка не исключают, что киберстрахование может стать обязательным. «Можно предположить, что могут сделать страхование обязательным для определенных категорий компаний, где ущерб от киберинцидента наносится как государству, так и населению», — говорит начальник управления страхования ответственности компании «Ингосстрах» Дмитрий Шишкин.

Обязательность киберстрахования в первую очередь напрашивается в части ответственности операторов персональных данных. Случаи утечки персональных данных учащаются, и без формирования страховой защиты многие операторы персональных данных могут оказаться не в состоянии ис-

полнить свои обязательства, что в обозримом будущем потребует соответствующих действий со стороны регуляторных органов власти, поясняет Евгений Изотов.

Со стороны страхового сообщества в этом контексте целесообразно подумать о минимальных стандартах киберстрахования во избежание дискредитации клиентской ценности продукта со стороны недобросовестных страховщиков, отмечает заместитель директора департамента андеррайтинга и управления продуктами компании «Согласие» Станислав Олейников.

Вместе с тем на рынке остаются проблемы, в частности информационная закрытость клиентов. Страховщики сталкиваются со сложностями при получении информации как для оценки рисков, так и для оценки убытков, так как для клиентов информация об информационной защите очень чувствительна, говорит Алина Малышева. «Однозначно поможет готовность бизнеса говорить открыто о своих киберинцидентах и убытках, вследствие чего вырастет осведомленность рынка о проблеме. Компании должны понять, что в этом вопросе страховые компании являются надежным партнером, которому можно довериться», — считает Дмитрий Шишкин.

информационные технологии

Управление данными: выход из хаоса

Большинство корпоративных данных так и не становятся инструментом для бизнеса: они хранятся в разрозненных системах и не используются в аналитике. Специалисты отмечают, что переход к управлению жизненным циклом данных становится ключевым условием внедрения и устойчивой работы ИИ.

— Big Data —

Компании в России и мире продолжают накапливать данные быстрее, чем успевают выстраивать процессы управления ими. По оценкам аналитиков, до 90% корпоративной информации остается так называемыми темными данными: фрагментированными, частично или полностью неструктурированными, недоступными для анализа. Согласно недавнему международному исследованию в области искусственного интеллекта и управления информацией, 64% организаций работают с массивами от 1 петабайта, а 41% — с объемами более 500 ПБ. Однако значительная часть этих данных либо не используется, либо хранится в изолированных системах, создавая расходы и дополнительные риски.

В РФ проблема усугубляется технологической разнородностью корпоративных IT-систем. В крупных компаниях данные распределены между сотнями устаревших и новейших IT-систем: от CRM и call-центров до локальных Excel-файлов сотрудников. В отсутствие единых правил обработки и понятной структуры ответственности данные становятся источником операционного хаоса: разные подразделения опираются на несогласованные сведения, а решения принимаются на неполной или противоречивой информации. Дополнительным фактором давления остаются регуляторные требования. Без четкой классификации и контроля доступа компании трудно обеспечить соответствие нормам, включая 152-ФЗ и отраслевые стандарты безопасности. По данным Ро-

скомнадзора, за первое полугодие 2025 года обнаружено 35 утечек персональных данных, из-за которых в открытом доступе оказалось более 39 млн записей пользователей.

Еще один негативный эффект «темных данных» связан с увеличением рисков при использовании ИИ и аналитики. Модели машинного обучения работают на том, что им предоставлено, и при отсутствии контроля качества выдают некорректные, а иногда и потенциально дискриминационные выводы. В этих условиях «темные данные» становятся тормозом цифровых проектов: без понимания их происхождения, структуры и актуальности компания не может гарантировать достоверность расчетов и защиту информации.

Решение проблемы связано с переходом от простого накопления информации к управлению ее жизненным циклом. Такой подход включает создание единой архитектуры данных, закрепление ответственности, формирование каталогов, отслеживание изменений и контроль качества. Эта схема предполагает автоматизацию ключевых операций, таких как описание и классификация данных, что снижает объем ручной работы и делает информацию более доступной.

На рынке давно существуют инструменты, которые упрощают внедрение подобных практик. Речь идет о платформах класса Data Governance, позволяющих описывать данные, отслеживать их происхождение, проверять корректность, контролировать доступ и готовность к использованию в аналитике. Одна из отраслей, в которой



интеллектуальный анализ «темных данных» может принести огромную пользу обществу, — это здравоохранение. В этой отрасли генерируется около 30% всех данных в мире. Вместо того чтобы выбрасывать, их можно анализировать, выявлять закономерности в медицинских записях, улучшать диагностику и оптимизировать планы лечения.

Российские решения Data Governance показывают достаточно высокий уровень зрелости, сопоставимый с зарубежными аналогами. В этом году международная биофармацевтическая компания AstraZeneca выбрала российско-го разработчика TData для одного из ключевых проектов в рамках

цифровой трансформации — внедрения российского продукта для управления большими данными. RT.DataGovernance создает единую экосистему для управления всем информационным массивом. Кроме того, практики Data Governance сокращают время на поиск и подготовку данных. По оценкам компаний, внедривших эти подходы, обучение сотрудников работе с данными занимает уже не месяцы, а недели. Этому способствует централизованный каталог, где каждому набору данных присвоены метаданные — источник, формат, правила доступа, владелец. Автоматизированная разметка и проверка качества снижают число ошибок и обеспе-

чивают прослеживаемость — от исходного источника до аналитической модели.

«Когда данные не описаны и не имеют владельцев, ИИ работает вслепую. Data Governance дает понять, откуда берется информация, кто отвечает за ее качество и можно ли использовать ее в моделях», — говорит гендиректор TData Станислав Лазуков. По его словам, именно прозрачность и управляемость данных становятся основой для внедрения ИИ-агентов и аналитических сервисов: модели могут работать корректно только в том случае, если исходная информация структурирована, проверена и доступна для контроля.

Эксперты полагают, что в ближайшие годы значение системного управления данными будет только возрастать. ИИ-агенты становятся основными потребителями корпоративной информации. Поэтому компании будут уделять больше внимания происхождению данных и их подлинности. Корректность аналитических систем и моделей ИИ определяется качеством исходных данных, на которые они опираются. Соответственно, прежде чем масштабировать цифровые решения, организациям придется обеспечить управляемость собственных данных — это становится фундаментом для развития ИИ и аналитики.

Константин Анохин

Совместимость как стратегия

— IT-инфраструктура —

Российские компании тратят до 15% годового IT-бюджета на поддержку интеграций между устаревшими и новыми системами, показывают данные российских и зарубежных исследований. Сегодня цифровые проекты тормозятся не разработкой, а отсутствием слаженного взаимодействия систем: разные приложения и сервисы не могут полноценно обмениваться данными между собой. И вопрос совместимости становится стратегическим. Поэтому компании переходят от точечных интеграций к единой архитектуре, которая позволяет соединять старые и новые системы без лишних задержек.

По оценкам экспертов рынка, в сложившейся ситуации важная стратегическая задача каждого крупного заказчика — обеспечить устойчивую совместимость старых и новых систем. «Сегодня важно не просто соединить два сервиса между собой. Важно выстроить архитектуру, которая позволит развивать бизнес независимо от того, на каких технологиях работают его системы — на старых, новых или тех, которые появятся завтра», — говорит генеральный директор Bergic Андрей Богданов.

Этот подход отвечает на главный вызов для бизнеса — необходимость одновременно работать с разнородными IT-системами. В корпоративном ландшафте соседствуют продукты SAP, 1C, отечественные IT-решения, open source инструменты, облачные сервисы, а также множество систем, построенных десять или более лет назад. Любое новое приложение встраивается в эту среду через набор интеграций, которые часто создаются под конкретный проект и редко имеют единую архитектуру. За годы таких решений накапливается множество отдельных интеграций, каждая из которых требует поддержки. То, что на старте успешно обслуживалось инхаус-командой разработчиков, начинает выходить из-под контроля и оттягивать на себя и ресурсы, и деньги. В результате значительная часть IT-бюджета уходит на обслуживание инфраструктуры, которая фактически возникает стихийно.

Из-за этого бизнес сталкивается с интеграционным долгом — накопленными техническими связками, которые тянут на себя ресурсы и усложняют запуск новых сервисов. Для запуска сервиса необходимо не только написать код, но и подключить его ко всем системам, от которых зависит работа продук-

та. В некоторых отраслях это приводит к задержкам на месяцы: новые функции в банковских сервисах или телеком-платформах выходят позже запланированного срока, а в промышленности интеграционные ошибки отражаются на операционных процессах.

Многие компании сегодня стремятся уйти от набора разрозненных интеграций и предпочитают выстраивать платформенную модель: обмен данными проходит через единый хаб, который задает общие правила, контролирует изменения и упрощает расширение системы. Такой подход позволяет централизовать обмен данными, отслеживать изменения, управлять нагрузкой и подключать новые сервисы без перестройки старых связей. Для бизнеса это означает сокращение сроков запуска продуктов, прогнозируемость архитектуры и меньшее количество ошибок при изменении инфраструктуры.

Примером могут служить российские интеграционные платформы, которые используют событийную модель, управление API и инструменты для работы с данными. Они собирают в одном контуре системы, созданные на разных технологиях, и постепенно заменяют хаотичные точечные связки более прозрачной архитектурой. В результате ти-

повые интеграции внедряются быстрее — не за месяцы, а за недели, а расходы на разработку заметно снижаются. Такая схема особенно востребована там, где соседствуют старые и новые решения: в банках, промышленности и телеком-отрасли. Подобные решения становятся ключевым элементом цифровой трансформации.

Важную роль в интеграционной архитектуре играют данные. При интеграции важно знать не только то, по какому каналу идут данные, но и что именно передается: структура, качество, происхождение и чувствительность информации. Если нет возможности управлять метаданными, интеграция быстро превращается в систему, где трудно понять, какие данные ходят между сервисами, насколько они корректны и как на них опираются модели ИИ. Поэтому современные интеграционные платформы включают инструменты каталогизации и отслеживания происхождения данных, что уменьшает количество ошибок и позволяет проще проверять, как именно данные проходят через систему.

Но одними технологиями такой переход не обеспечить — менять приходится и организационные подходы внутри компании. Для этого компаниям приходится менять

процессы разработки, договариваться между командами о единых правилах работы с данными и постепенно уходить от старых интеграций. Как правило, изменения начинают с небольших «пилотов»: компании запускают интеграционный хаб на одном-двух сервисах, получают измеримый эффект и затем масштабируют модель.

Скорость вывода продуктов на рынок сегодня определяется не только командами разработки, но и тем, насколько гибко соединены системы внутри компании. Без продуманной интеграционной архитектуры цифровые проекты неизбежно сталкиваются с задержками, ростом издержек и ограничениями при внедрении новых технологий. Ответом на эти риски становятся интеграционные платформы и хабы, которые централизуют обмен данными и задают общие правила взаимодействия между системами. Они позволяют постепенно заменить хаотичные точечные интеграции прозрачной и управляемой моделью, а архитектуру сделать предсказуемой и расширяемой. Поэтому интеграция перестает быть техническим этапом и становится базовым условием успешной цифровизации.

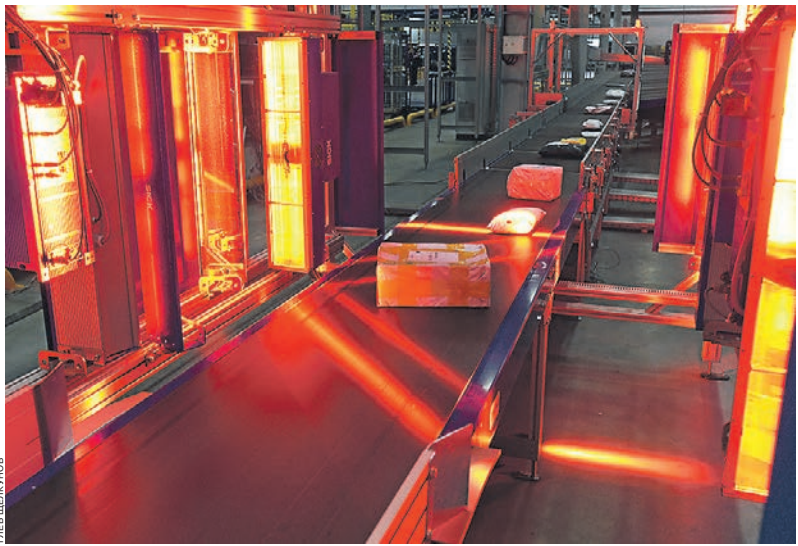
Константин Анохин

На письмо поставят киберпечать

— защита инфраструктуры —

Кибербезопасность в России уже перестала быть технологической абстракцией — это вопрос повседневной устойчивости бизнеса и инфраструктуры. Участники рынка все чаще фиксируют появление новых хакерских групп и рост утечек. Так, по данным компании RED Security, в третьем квартале 2025 года число атак выросло на 73% год к году, до более чем 42 тыс. Вместе с тем в России растет и рынок ИБ. Согласно прогнозам экспертов, по итогам 2025 года российский рынок кибербезопасности достигнет 374 млрд руб., а к 2030 году может увеличиться до 968 млрд руб. при совокупном среднегодовом росте в 21%.

Драйвером сегмента выступают внутренний спрос и государственная политика технологического суверенитета, ранее отмечала заместитель гендиректора Центра стратегических разработок Екатерина Кваша (см. «Ъ» от 17 ноября). Однако рынок все еще видит вызовы в виде высокой ключевой ставки, санкций и регуляторного давления. При этом «громкие события» стало сложно замалчивать», особенно когда речь идет о целенаправленном уничтожении инфраструктуры крупных компаний, заявлял директор центра мониторинга и противодействия киберугрозам IZ.SOC



«Информзащиты» Александр Матвеев (см. «Ъ» от 28 июня 2024 года).

Крупные стратегические корпорации стараются ответственно подходить к работе с кибербезопасностью. Например, за январь—ноябрь 2025 года «Почта России» выявила и заблокировала 44 фейковых сайта и 214 Telegram-ботов, использующих бренд почтового оператора. «Почта» стремится максимально обезопасить данные клиентов и делает все возможное по части коммуникации и ИБ-контура, чтобы огрaдить их от угроз как внутри страны, так и извне. В том числе привлекая опытных партнеров, которые занимаются ки-

бербезопасностью уже много лет», — сообщают в компании.

Так, «Почта России» договорилась с крупными ИБ-игроками, такими как ГК «Солар», Positive Technologies и «Лаборатория Касперского», о сотрудничестве для совместной разработки программы по построению ИБ-инфраструктуры. Она включает в себя разделы о совместном формировании подходов к построению архитектуры комплексной системы ИБ, разработке и тестировании многофункциональных решений компаний и консолидации лучших отраслевых практик в области кибербезопасности. Также компании будут органи-

зовывать и поддерживать мероприятия, которые помогут экспертам из отрасли развивать свои навыки и знания, обмениваться опытом и строить карьеру. За три года планируется реализовать 66 ИБ-проектов, которые охватят всю инфраструктуру «Почты России» по стране. «На базе проекта с «Почтой России» мы с коллегами сейчас фактически вырабатываем золотой стандарт построения киберустойчивости геораспределенной инфраструктуры — особенно в части процессов взаимодействия, механизмов контроля и оценки итогов», — отмечал ранее директор департамента архитектуры стратегических проектов ГК «Солар» Антон Ефимов. Так, платформенный подход сможет одновременно защитить серверы и рабочие станции от массовых атак и помешать внедрению угроз в систему промышленности и логистики.

На одной из сессий SOC Forum 2025 года заместитель гендиректора по цифровой трансформации «Почты России» Дмитрий Чудинов также подчеркивал, что в компании отказались от запуска большого количества проектов в пользу создания одного масштабного продукта с единой архитектурой. «Реализация такого подхода помогла нам внедрить результативное ИБ-решение для наших клиентов», — поясняет эксперт. Информационная безопасность — одна из стремительно развивающихся отраслей последние несколько лет, этот

сегмент ускоряется, так как появляется все больше угроз с повышенной сложностью, наша задача — своевременно на них реагировать, добавляет он. С ним соглашается руководитель дирекции информационной безопасности «Почты России» Роман Шапиро: «Наша команда нашла новые особенности инфраструктуры, которые заключаются не в отсутствии „слепых“ зон или покрытия средствами защиты информации, а в архитектурных особенностях работы информационных систем — это совершенно другой взгляд на обеспечение кибербезопасности в отдельно взятой организации».

«Заключенное соглашение позволит нам делиться собственным опытом разработки для реализации в других компаниях. Мы провели масштабную тренировку, чтобы посмотреть, как все ИБ-подсистемы инфраструктуры будут работать в реальных условиях, и реализовывали это именно на тех ресурсах, которые нам доступны. То ядро, которое мы создали, в настоящий момент прошло апробацию кибертренировки, и мы готовы к тиражированию данной инфраструктуры на все субъекты, где присутствует „Почта России“, — объясняли в компании. При этом почтово-логистический оператор комментирует, что каждая подсистема проекта внедряется вендором для дальнейшей работы в совокупности внутри инфраструктуры, но все они должны пройти от-

дельную верификацию: соответствовать требованиям ТЗ, частного ТЗ, проектной документации и отдельно подтвердить критерий обнаружения и устранения в каждом из сценариев всех или как минимум одного события информационной безопасности.

Касательно соответствия требованиям NGFW в «Почте России» отмечают, что всегда использовали либо сертифицированные отечественные решения, либо из дружественных стран. «Вопрос импортозамещения идет, но в рамках целевой картины после окончания сроков полезного использования. Все результаты легли в основу создания проектной документации, к завершению второй фазы мы точно сможем понять, кто из игроков рынка сможет это реализовать», — говорит господин Шапиро. «В России импортозамещение имеет жесткую регуляторику, это создает сложности для производства высококонкурентного продукта. В ряде сфер ужесточение правил действительно имеет место быть, но с аккуратным подходом, чтобы не вызывать обратного эффекта для бизнеса и не усложнять построение ИБ-инфраструктуры», — добавляет он. Важно обеспечить стабильную работу, защиту наших клиентов и гарантированных им государством социальных функций при минимальной себестоимости и оптимальной реализации, заключает Дмитрий Чудинов.

Василиса Аксенова

информационные технологии

Устойчивость вместо скорости

Во многих компаниях IT-подразделения в последние годы развивали гибкие форматы работы, чтобы быстрее реагировать на запросы бизнеса. Но сегодняшняя реальность требует другого подхода: процессы должны оставаться стабильными и предсказуемыми даже при сбоях, высоких нагрузках или перестройке инфраструктуры. Обеспечить такую стабильность позволяют сервисные модели управления, которые задают единые правила работы и охватывают не только IT, но и HR, офисные и административные функции.

— компании и рынки —

Во многих компаниях инфраструктура исторически складывалась фрагментарно: разные решения, разные команды, разный уровень зрелости сервисов. В такой среде любое изменение превращается в марафон согласований, а сами процессы — в непрозрачный набор шагов, где сложно понять, кто отвечает за конкретный сервис, как измеряется его качество и какие параметры критичны для бизнеса.

К тому же на рынке по-прежнему сильно классическая, ресурсная модель: IT-служба отвечает за то, чтобы «железо» и софт работали, опирается на регламенты и инструкции и решает задачи в рамках имеющихся ресурсов. Но, как отмечает генеральный директор цифровой экосистемы «Лукоморье» Арсен Благов, главный недостаток такой модели в том, что она часто изолирована от

бизнеса: IT знает инфраструктуру, но не всегда понимает, какие именно сервисы нужны пользователям и что для них является ценностью. В результате компания видит расходы на IT, но не видит, какую пользу они приносят.

Альтернативой становится сервисный подход, или IT Service Management (ITSM). Он смещает фокус с оборудования на пользователя: IT рассматривается как поставщик услуг, которые должны соответствовать ожиданиям заказчика — внутренних или внешних. Работа выстраивается как набор повторяющихся процессов с понятными ролями, ответственностью, сроками реакции и измеримыми параметрами качества. Такой подход делает сервисы предсказуемыми и позволяет поддерживать их стабильную работу даже при кадровых перестановках или изменениях в инфраструктуре.



При этом в России сервисная модель развивается по своей логике. Если в международной практике компании часто сначала выбирают платформу, а затем стараются подстроить под нее процессы, то в российском контуре логика обратная: сначала проектируется сервисная модель, а технология подбирается уже под нее. Это связано с особенностями локальных отраслей. В банках ITSM встраивается в насыщенные IT-ландшафты и должен учитывать требования ЦБ к управлению IT-рисками. На про-

мышленных предприятиях сервисные процессы связаны с АСУ ТП и системами безопасности — ошибка в заявке может привести не только к простоям, но и к угрозам на производстве. В ритейле ключевым параметром становится строгое соблюдение SLA: единичная задержка в обработке заказа напрямую отражается на выручке. Поэтому российский рынок в целом предъявляет более высокие требования к адаптивности решений — ценится не набор функций, а способность платформы работать под реаль-

ную бизнес-логику и обеспечивать предсказуемость процессов.

Поддерживать такую трансформацию организациям помогают инструменты управления процессами: по-сcode платформы, которые позволяют быстро формировать новые сервисы, и цифровые двойники процессов, обеспечивающие тестирование изменений без вмешательства в реальную работу. Для компаний это шанс уйти от устаревших схем и выстраивать процессы, которые можно гибко адаптировать под новые требо-

вания. Одновременно такие инструменты создают основу для автоматизации рутинных задач, разгружают команды и повышают прозрачность операций.

Российский рынок движется именно в эту сторону. По оценкам экспертов, по итогам 2025 года его объем может достигнуть 18–22 млрд руб., и рост идет не только за счет миграции с западных решений, но и благодаря расширению сервисной модели на новые подразделения. Спрос формируется там, где требуется предсказуемость: в банках, промышленности, ритейле — везде, где сбой в процессе может привести к прямым потерям. Помимо функционала, компании ожидают от платформ также умения работать в сложных IT-ландшафтах и поддерживать реальные бизнес-процессы.

Поэтому управление процессами становится базовым элементом операционной устойчивости. Компании стремятся не только реагировать на события, но и строить систему, где процессы остаются работоспособными при любых внешних изменениях. Сервисная модель в этом смысле становится естественным инструментом: она снижает риски, повышает предсказуемость и формирует единый стандарт работы. ITSM становится стратегической платформой управления бизнесом, а не вспомогательным инструментом. Российский ITSM сегодня — это не про «замещение», а про собственный путь развития: гибкий, ориентированный на бизнес и строящийся на глубокой экспертизе. И в этом его главное преимущество», — резюмирует Арсен Благов.

Константин Анохин

Бизнес берет образование в свои руки

— подготовка кадров —

Спрос на цифровые решения растет быстрее, чем система образования готовит специалистов. Компании внедряют новые технологии, но выпускникам часто не хватает практики и понимания того, как устроены рабочие процессы. Поэтому бизнес все чаще берет подготовку кадров на себя: создает собственные модели подготовки кадров и интегрирует обучение в проектную деятельность.

За 2022–2024 годы рынок ИТ-услуг рос почти вдвое быстрее, чем в предшествующий период (2019–2021 годы): до 17% вместо 8–9%. Такой скачок обеспечили инвестиции и создание новых информационных систем. В ближайшие годы вложения в цифровую трансформацию и обновление инфраструктуры продолжат стимулировать рост рынка. Повышение требований к результативности приведет к более сложным проектам и, как следствие, к увеличению спроса на специалистов с глубокими компетенциями.

Однако здесь проявится системный разрыв. По данным исследования «Яков и партнерс», с 2016 года более 100 университетов добавили ИТ-специальности в свои програм-



мы. Но традиционная система подготовки кадров не всегда успевает за темпами рынка: выпускники хорошо знают основы, но не сталкивались с настоящими системами, данными, требованиями к безопасности и надежности.

За последние десять лет взаимодействие бизнеса и университетов значительно усилилось. Формат обычных стажировок постепенно уступает место более глубоким моделям: корпоративным ака-

демиям, совместным трекам, кейс-чемпионатам и внедрению добровольного квалификационного экзамена.

В 2021–2025 годах представители бизнеса в рамках госпрограммы «Приоритет 2030» инвестировали в российские университеты 214 млрд руб. В 2026 году крупные ИТ-компании с выручкой более 1 млрд руб. в год и численностью сотрудников от 100 человек для сохранения аккредитации будут обязаны заключать соглашения с про-

фильными вузами и отчислять им 3% от сэкономленных от налоговых льгот средств. Компании займются разработкой образовательных программ по профильным специальностям. Пока из 500 ИТ-компаний, которые соответствуют критериям, лишь 20% взаимодействуют с системой образования.

Поэтому компании, ориентированные на технологическое развитие, начинают пересматривать подход к обучению, выстраивая собственные практики и стандарты. По мнению директора по развитию стратегических проектов «Ростелекома» Владимира Татаринцева, технологический рынок рождается там, где появляется новое поколение специалистов: не только в базовой среде образовательной организации, но и в среде, сочетающей науку, инженерные задачи и производственную инфраструктуру.

Технологическая среда, в которой студенты с первого курса работают с новыми решениями, где смещен фокус на 60% и более на практическую подготовку. Новая среда должна включать корпоративные дисциплины, лаборатории на базе вузов и доступ к рабочей инфраструктуре. Это позволяет создавать бесшовные прототипы, которые мож-

но сразу выводить в производство. Такой подход формирует конвейер базовых инженеров с прикладным знанием рыночных решений, что, в свою очередь, снижает затраты компаний на адаптацию и их доучивание. Целевое будущее — формирование технологических мастерских на базе образовательных организаций, где участие партнеров, разработчиков становится обязательным.

Крупнейший в России интегрированный провайдер цифровых решений «Ростелеком» одним из первых начал выстраивать такую среду. На базе вузов создаются специализированные лаборатории, где студенты работают с продуктами и системами «Ростелекома»: от облачных платформ до инструментов для управления данными. Это позволяет им получать практический опыт на тех же инструментах, которые используются в государственных и коммерческих организациях, и лучше понимать требования к качеству разработки, надежности и безопасности информационных систем. За последние три года программы «Ростелекома» в вузах охватили около 60 тыс. студентов и 2,5 тыс. преподавателей. Это практико-ориентированные направления — инженерия, разработка, аналитика и цифровая поддержка, где обучение

строится вокруг практических задач и инфраструктуры компании.

Особое внимание «Ростелеком» уделяет подготовке междисциплинарных инженеров — специалистов, которые понимают не только код, но и контекст применения: энергетику, транспорт, промышленность. Через формат R&D+P (от исследования до прототипа) студенты проходят полный цикл разработки: от идеи до внедрения решения в реальную инфраструктуру.

«Для нас важно не просто подготовить специалистов. Важно, чтобы у ребят появилась среда, в которой они могут пробовать, ошибаться, находить свои решения и расти как инженеры. Это уже не про учебный курс, а про людей, которые через несколько лет будут определять, как развивается в стране ИТ-отрасль», — подчеркивает Владимир Татаринцев.

Такая подготовка востребована и за пределами ИТ: цифровые двойники, аналитика и автоматизация входят в задачи энергетики, транспорта и промышленности. Поэтому бизнес берет на себя роль квалифицированного заказчика и помогает формировать спрос на инженеров, которые понимают и технологию, и ее применение.

Константин Анохин

Цифровой прототип для аналоговой проблемы

— микроэлектроника —

Актуальный вопрос после событий 2022 года для производителей электронной компонентной базы не физическое производство, а цифровое проектирование. Резкий уход зарубежных гигантов, таких как Ansys, Cadence и Suporsys, разорвал для российских разработчиков электронки цепочку CAE — систем компьютерного инженерного анализа. Без этого современная разработка высокотехнологичных устройств в нынешних реалиях практически невозможна. На заполнение сегмента рынка бросились как небольшие студии, так и крупные технологические холдинги. Почему игроки идут в этот сложный и наукоемкий бизнес, каковы его границы и станет ли это решением проблем для отрасли, выясняли «Ъ-Информационные технологии».

Инвестиционная логика

Стимул для крупных инвестиций лежит в области технологической безопасности и прямой экономической выгоды. «После ухода международных поставщиков встал вопрос не просто замены, а создания собственных инженерных инструментов, которые обеспечивают предсказуемость и устойчивость технологических процессов», — объясняет директор центра компетенций «Т1 Интеграции» Александр Собачкин. Для холдинга, который получил от Мин-

промторга субсидию в 2,5 млрд руб. и вложил собственные средства, это стратегический переход от статуса интегратора к роли разработчика критического софта, отмечают в компании.

Запрос исходит от производителей электроники, для которых моделирование стало базовым элементом жизненного цикла. «Главное — это поддержка пользователей и интеграция», — утверждают в пресс-службе производителя электроники ГК «Элемент», подтверждая, что рынок готов апробировать российские решения. Для компаний — разработчиков электроники, как отмечает Т1, моделирование — «базовый элемент жизненного цикла». Внедрение CAE (Computer-Aided Engineering) позволяет радикально сокращать дорогостоящие натурные испытания, что в конечном счете и формирует спрос на такие платформы со стороны промышленности. CAE — это компьютерный инженерный анализ. Если САПР (CAD) помогает создать цифровую 3D-модель изделия, то CAE-системы позволяют провести на этой модели виртуальные испытания: рассчитать, как она будет вести себя под нагрузкой, нагреваться, взаимодействовать с электромагнитными полями или жидкостями. Это позволяет находить и устранять недостатки, оптимизировать конструкцию еще до изготовления физического прототипа, что экономит время и средства.

Однако рынок не только большой — он по-прежнему критически зависит от импорта. Согласно

данным, представленным на форуме «Электроника России-2025» 26 ноября замдиректора департамента цифровых технологий Минпромторга Иваном Кузьменко, по состоянию на 2025 год 61% предприятий радиоэлектронной отрасли используют иностранные решения в сегменте CAE. При этом только 27% используют автоматизацию в этой области, что указывает на низкую зрелость процессов даже у тех, кто имеет доступ к ПО. Таким образом, спрос на отечественные CAE-платформы подстегивается не только уходом вендоров, но и потенциалом для внутреннего роста и цифровизации.

Мультидисциплинарность как новый стандарт

Российские разработчики не просто копируют старые решения, а пытаются предложить новый стандарт. Господин Собачкин напоминает, что в современной электронике с ее высокой плотностью компонентов тепловые, электрические и электромагнитные процессы тесно связаны. Раздельный анализ приводит к ошибкам.

Мультидисциплинарное (мультифизическое) моделирование — это подход, при котором в единой цифровой среде одновременно рассчитывается взаимное влияние разных физических процессов. Например, в электронике нагрев элементов (тепловой анализ) меняет их электрические свойства, что, в свою очередь, влияет на распределение электромагнитных полей. Анализ этих

процессов по отдельности может не выявить критические ошибки, которые возникают именно из-за их взаимодействия. Этот подход считается единственно возможным для устройств нового поколения: от интегральных схем до антенн. Он позволяет увидеть кросс-эффекты, невидимые при изолированном моделировании, которые могут стать причиной отказа изделия.

Системные ограничения: от математических моделей до структуры рынка

Однако даже самая совершенная платформа не станет панацеей. Есть как минимум три фундаментальных барьера. Во-первых, это технологический потолок. Главный вызов, по словам Александра Собачкина, — это «разномасштабность современных изделий». В одном устройстве соседствуют процессы на уровне нанометров (элементы микросхем) и метров (корпус). Для этого требуются математические модели и алгоритмы высочайшей сложности, разработка которых нетривиальная задача даже для команды в 100 специалистов, собранной Т1.

Также отрасль испытывает кадровый голод. В электронике «революции» происходят каждые несколько лет, а инженерные школы не успевают аккумулировать десятилетний отраслевой опыт», признает представитель Т1. Рынок испытывает острый дефицит инженеров-расчетчиков, способных не просто нажимать кнопки в программе, но и понимать

физику процессов. Без них даже самый продвинутый софт бесполезен.

Экономический и структурный парадокс. Глава АРПЭ Иван Покровский указывает на обратную сторону кризиса: в условиях, когда отрасль остро нуждается в новых инструментах, она не может сформировать на них устойчивый платежеспособный спрос. «По нашим оценкам, сокращение рынка и объемов производства электроники составляет в 2025 году 25%, а средства проектирования и моделирования — это инвестиционные расходы компаний, которые в этих условиях сокращаются еще больше», — отметил он. Господин Покровский объясняет это тем, что львиная доля рынка сегодня занята локализованной продукцией зарубежной разработки, выпускаемой по готовой документации: «Особенно тяжело в этих условиях российским разработчикам микросхем. Трудно рассчитывать, что, находясь в режиме выживания, они смогут создать спрос на развитие отечественных CAD и CAE». Выход из этого круга, по его мнению, лежит в изменении госрегулирования и постановке общей цели для отрасли — «переход на аппаратные платформы российской разработки». Только такие амбициозные сквозные проекты, а не запреты смогут создать реальный заказ для всей цепочки, включая разработчиков CAE.

Проблема усугубляется высокой стоимостью и сложностью внедрения цифровых решений в существующие процессы. Как показывают

те же данные Минпромторга, средняя стоимость внедрения системы управления жизненным циклом изделия (PLM) на предприятии радиоэлектроники составляет 300 млн руб., причем 56% этой суммы уходит на инфраструктуру, а не на сами лицензии (2%). Годовое сопровождение обходится еще в 45 млн руб. Эти цифры на порядок превышают стоимость лицензий на CAE-софт и означают, что успех любой новой платформы упирается в готовность компаний к многолетним и дорогостоящим цифровым преобразованиям. При этом 83% предприятий либо только планируют внедрение PLM, либо не обозначили сроков, что свидетельствует о колоссальном отставании в создании полноценной цифровой среды (Digital Thread), в которую должна встроиться CAE-платформа.

Таким образом, создание CAE-платформ — это необходимый, но недостаточный шаг. Резюме, представленное Минпромторгом, предполагает четкий план действий для промышленности: участвовать в стандартизации, тестировать решения и давать обратную связь разработчикам. Это путь от разрозненных инвестиций к формированию работоспособной экосистемы. От того, последует ли рынок этой логике кооперации, а не замкнутой самодостаточности, зависит, станут ли новые инструменты вроде «Таумерикс» основой для технологического рывка или останутся сложными игрушками в руках немногих.

Филипп Крупанин

информационные технологии



Промышленность под датчиками

Рост требований к эффективности делает простые и ошибки планирования особенно чувствительными для промышленных компаний. Чтобы быстрее собирать информацию о состоянии оборудования и контролировать процессы, предприятия переходят к технологиям обработки данных в режиме реального времени. На этом фоне промышленный интернет вещей (IIoT) становится ключевым элементом цифровой инфраструктуры. «Ъ-Информационные технологии» обсудили со специалистами группы компаний ЛАНИТ, какие IIoT-подходы уже работают на российских предприятиях и какой эффект они дают.

— **технологии в промышленности** —

Рынок IIoT: от спада к восстановлению

Российский рынок промышленного интернета вещей за последние несколько лет вышел на стабильную траекторию роста. Согласно отчету TelecomDaily за 2024 год, сегмент IIoT демонстрирует восстановление после спада 2022 года. По оценкам аналитиков, по итогам 2023 года он увеличился на 5%, до 144,4 млрд руб., а к 2026 году составит 188,9 млрд руб. при ежегодной динамике роста в 11%.

Наиболее активно IIoT внедряется в энергетике, машиностроении, металлургии и транспорте — там, где мониторинг оборудования, цифровые двойники и предиктивная аналитика уже формируют новый уровень управления производством.

TelecomDaily также отмечает факторы, сдерживающие развитие отрасли: дефицит специалистов, сложность интеграции новых решений со старыми системами и зависимость части проектов от госфинансирования. Тем не менее к 2025 году рынок IIoT перешел от восстановления к устойчивому росту благодаря импортозамещению, цифровизации отраслей и появлению новых отечественных платформ.

«Импортозамещение стало ключевым фактором: многие компании использовали зарубежные системы и сейчас вынуждены переходить на российские», — подтверждает эти тенденции директор департамента прикладных решений «ЛАНИТ-Терком» Дмитрий Медведев. Экономический контекст также играет роль: компании стремятся снижать издержки и повышать операционную устойчивость. Руководитель отдела интеллектуальных платформ «ЛАНИТ-Проекты» Максим Гречнев добавляет, что высокая ключевая ставка и высокий процент по кредитам побуждают компании к оптимизации внутренних затрат и поиску технологических решений, позволяющих сделать производственные процессы более эффективными.

Фокус на платформах

Еще несколько лет назад предприятия рассматривали IIoT как набор от-

дельных инструментов для мониторинга или автоматизации отдельных участков. Сегодня рынок смещается в сторону комплексных платформ. Промышленность стремится к единой цифровой среде, в которой данные собираются, обрабатываются и используются для принятия решений в режиме реального времени.

Одним из ключевых факторов, который подталкивает компании к этому переходу, становится безопасность. Множественные разрозненные системы повышают риск потери контроля над данными и доступами. «Если у предприятия 10–20 отдельных решений, всегда можно упустить что-то в плане безопасности. Единая платформа проще в управлении и контроле», — отмечает Дмитрий Медведев.

Но дело не только в безопасности. Дело в том, что производства устроены очень по-разному и универсальные «коробочные» решения часто оказываются недостаточны функциональными — не покрывают все потребности. Отсюда — спрос на платформы, которые позволяют гибко настраивать модули под отдельный определенный процесс.

Именно поэтому на рынке преобладает платформенный подход, помогающий подбирать модули под специфические задачи. «IIoT-решения сегодня — это многомодульные платформы, что-то вроде конструктора. Их можно адаптировать под специфику бизнеса и развивать дальше. При этом современные платформы дают не готовые пользовательские сценарии, а инструменты, которые позволяют собирать интерфейсы и логику под конкретную

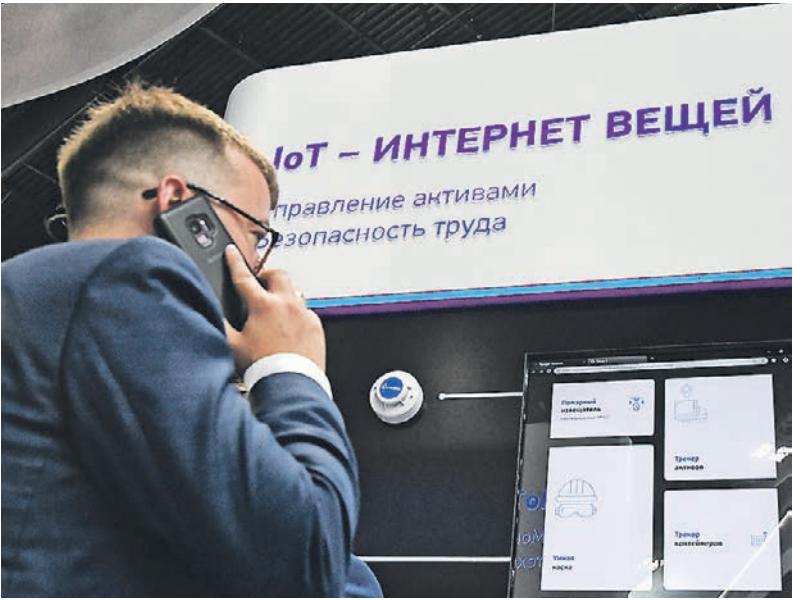
задачу», — говорит Максим Гречнев. Интерес к экосистемам вместо отдельных систем связан и с ростом требований к операционной эффективности. По мнению Максима Гречнева, предприятия ставят акцент на управлении эффективностью и устойчивостью бизнес-процессов, а платформа дает возможность планировать, анализировать и сокращать время внедрения изменений.

Такой подход меняет и сам характер внедрений: пилотные проекты все чаще строятся как шаг к масштабируемым решениям, а не как изолированный эксперимент. Компании ожидают, что результаты «пилота» можно будет оперативно перенести на другие площадки и процессы. «Переход от „пилота“ к промышленной эксплуатации требует партнерского подхода и гибких методологий — только так можно быстро адаптировать решения и находить наиболее подходящие сценарии», — комментирует Дмитрий Медведев.

В результате IIoT перестает быть набором специализированных инструментов и превращается в основу цифровой инфраструктуры предприятия — такой же системообразующий элемент, как SCADA, MES или ERP. Именно через такие платформенные экосистемы компании стремятся обеспечить прозрачность процессов, предсказуемость работы оборудования и управляемость распределенных производств.

Выход за рамки

Переход к платформенным IIoT-решениям меняет характер управления производством: предприятия получают возможность работать с



оборудованием и процессами не по фактум, а в режиме постоянного мониторинга. Такой подход позволяет снижать риски, оптимизировать ресурсы и планировать обслуживание заранее, а не в момент аварии или сбоя.

Самым востребованным направлением становится предиктивная аналитика. Именно она позволяет прогнозировать потенциальные неисправности по данным датчиков — вибрации, температуре, нагрузкам — и формировать рекомендации по обслуживанию. «По сути, можно заранее выявить отклонения и предотвратить незапланированные простои, продлевая срок службы оборудования», — объясняет Дмитрий Медведев.

Вторым важным направлением становится управление энергопотреблением. Рост стоимости ресурсов и общий курс на повышение эффективности делают энергоменеджмент одной из ключевых задач. Как считает Максим Гречнев, управленческие энергии — часть общей оптимизации производственных процессов: предприятия стремятся снижать издержки в условиях высокой ставки и давления на себестоимость.

Значительно меняется и роль искусственного интеллекта в промышленных системах. В отличие от потребительских сервисов, где широко применяются большие языковые модели, производственные компании используют ИИ гораздо острее — им критичны предсказуемость и строгое соблюдение порогов точности. «LLM дают вероятностный результат, а нам нужны гарантированные уровни точности», — поясняет Дмитрий Медведев. Поэтому такие технологии применяются лишь там, где можно обеспечить контроль качества. В большинстве случаев предпочтение отдают классическим методам машинного обучения: они позволяют работать с точными пока-

зателями датчиков, задавать пороги допустимых отклонений и формировать предиктивные модели на основе исторических данных.

IIoT также стал основой для создания цифровых двойников — компьютерных моделей предприятий, оборудования и технологических маршрутов. Такие системы моделируют работу сотен станков, рассчитывают оптимальную последовательность операций, перераспределяют ресурсы и поддерживают принятие решений на уровне диспетчерских служб и инженеров. Цифровые двойники уже используются в крупных производственных комплексах, позволяя оптимизировать загрузку оборудования и снижать время переналадки.

Неотъемлемой частью современных IIoT-систем становится работа с высокими объемами и скоростью данных. Производственные линии генерируют миллионы событий в сутки, и традиционные реляционные СУБД не справляются с такой нагрузкой. «Вендоры применяют нереляционные базы, колоночные хранилища, память-ориентированные решения — это позволяет обрабатывать большие массивы телеметрии в реальном времени», — уточняет Максим Гречнев.

Таким образом, функции IIoT выходят далеко за рамки «набора датчиков». Это единая цифровая среда, в которой собираются, анализируются и используются данные для управления оборудованием, планирования обслуживания, оптимизации маршрутов и энергопотребления. Именно эта связка — данные, предиктивность, моделирование и интеграция — формирует основу современной автоматизации промышленности.

Рецепты созревания

Рынок промышленного интернета вещей в РФ в ближайшие годы будет

расти не только за счет замены устаревших систем, но и благодаря расширению функциональности отечественных решений. Компании начинают рассматривать IIoT как фундамент для построения цифровых производств — от автоматизации отдельных операций до управления распределенными активами.

Предприятия продолжают углублять автоматизацию процессов, включая операции, которые ранее выполнялись вручную, и одним из ключевых направлений станет обработка данных «на периферии», полагает Дмитрий Медведев: «Периферийные вычисления позволяют обрабатывать данные ближе к оборудованию, что особенно важно для систем реального времени: сокращаются сетевые задержки, и система быстрее реагирует на изменения».

Технологии машинного обучения будут занимать все более заметное место в аналитике. Сейчас большинство решений еще работают на классических моделях предиктивного анализа. В перспективе же они станут стандартной частью платформенных инструментов. По словам Максима Гречнева, этот переход уже начался: «Технологии искусственного интеллекта постепенно будут перетекать в платформенные решения и предоставляться из „коробки“, как любой другой инструмент».

Отдельное направление — повышение требований к безопасности. С ростом числа подключаемых устройств предприятиям требуется обеспечить защищенность данных, учитывать отраслевые стандарты и соответствовать регуляторным требованиям. В этой части, по мнению экспертов, роли отечественных платформ и стандартов будут усиливаться, а работа по унификации подходов продолжится.

Сегменты, в которых IIoT уже демонстрирует высокий потенциал, расширяются. Логистика, энергетика, нефтегаз, строительство и сельское хозяйство — отрасли, где растет потребность в непрерывном мониторинге и прогнозировании состояния оборудования. «Во многих из этих сфер IIoT уже становится обязательным элементом управления, а потенциал для адаптации решений значительный», — подчеркивает Дмитрий Медведев.

В целом эти факторы формируют тренд на переход от отдельных IIoT-систем к более зрелой цифровой архитектуре, способной адаптироваться под разные отрасли и изменяющиеся условия. Российский рынок движется к тому, чтобы IIoT стал не опцией, а базовой составляющей производственной инфраструктуры — инструментом повышения устойчивости и конкурентоспособности предприятий.

Константин Анохин

На киберфронте без перемен

— **кибербезопасность** —

Подводя предварительные итоги 2025 года, эксперты в области кибербезопасности констатируют качественное изменение угроз: атаки становятся целенаправленными и разрушительнее, а их продолжительность растет. Финансовый ущерб для бизнеса увеличивается — максимальный запрошенный выкуп достиг 400 млн руб., что на 67% выше показателя прошлого года. Киберпреступные группировки окончательно структурировались, переняв модели легального IT-бизнеса, а искусственный интеллект перешел из разряда гипотетических рисков в рабочий инструмент обеих сторон.

В предварительных итогах 2025 года в сфере кибербезопасности ИБ-специалисты сходятся во мнении, что рост числа инцидентов сохраняется, однако оценки его динамики среди экспертов разошлись. С одной стороны, по данным центра мониторинга киберугроз компании «Спикател», за десять месяцев года число атак увеличилось на 38% по сравнению с аналогичным периодом 2024-го, до 16 тыс. инцидентов. Директор по продуктам Servicepire Михаил Хлебунов подтверждает, что и количество инцидентов продолжает расти, и профессионализм злоумышленников повышается.

Более сдержанную и, по всей видимости, более обоснованную оценку дают эксперты крупных игроков рынка. Руководитель департамента комплексного реагирования на киберугрозы экспертного центра безопасности Positive Technologies Денис Гойденко полагает, что гипотеза об экспоненциальном росте не подтверждается: «Подобной динамики не наблюдалось, и предпосылок для нее не было. Однако устойчивый линейный рост действитель-

но присутствует». Эту точку зрения разделяет директор центра информационной безопасности «Инфосистемы Джет» Андрей Янкин. «Рост числа атак действительно продолжается, но скорее линейно. При этом качественные изменения очевидны: основной ущерб сегодня несут шифровальщики и вайперы (уничтожают данные без возможности восстановления. — «Ъ»), — отмечает господин Янкин. Гендиректор VolgaBLOB Александр Скакунов добавляет, что для крупных компаний и госсектора вызовы года заключаются не в увеличении числа атак, к которому уже привыкли, а в повышении их сложности и большей направленности.

Финансовая мотивация остается ключевой для злоумышленников. По данным Михаила Хлебунова, около 60% атак совершаются ради выкупа или кражи средств. При этом, как отмечает CEO компании F6 Валерий Баулин, максимальная запрошенная сумма первоначального выкупа в 2025 году увеличилась на 67%, составив 400 млн руб. Андрей Янкин акцентирует внимание на изменении модели атак: «Большинство теперь нацелены не просто на получение выкупа, а на полное уничтожение инфраструктуры с целью сделать восстановление невозможным и парализовать операционную деятельность жертвы». По его словам, средняя продолжительность простоя выросла, так как атакующие действуют скрытно и методично, не раскрывая себя, пока не доберутся до систем резервного копирования и виртуализации.

Эволюция кибергруппировок, по мнению экспертов, в первую очередь выматывает, продолжается в сторону большей структуризации и профессионализма. «Действительно, тренд последнего года — группы киберпреступников все чаще демонстрируют бизнес-подход, то есть ведут себя как коммерческие орга-

низации: масштабируют успешные атаки, оптимизируют ресурсы, оказывают «услуги», продают инструменты, инвестируют в инфраструктуру», — констатирует господин Хлебунов. Валерий Баулин развивает эту мысль: «Финансово мотивированные киберпреступные группировки, включая вымогателей, шифровальщиков, скамеров, выстраиваются по модели самой современной IT-компании. В их структуре действуют отдельные подразделения, которые занимаются техническими вопросами, такими как разработка, R&D, техническая поддержка, пен-тесты, и обеспечением деятельности». Александр Скакунов приводит в пример появившуюся у вымогателей подписную модель, в рамках которой пострадавший может купить годовую гарантию, что утекшая база или чувствительные данные не будут опубликованы. «Некий сертификат, скрепленный кодексом хакерского слова, с одной стороны, и платежом в криптовалюте — с другой», — добавил он.

Практически все эксперты едины в оценке самого слабого звена в защите компаний. «Это люди. В частности, причиной 74% утечек данных прямо или косвенно был человеческий фактор», — заявляет Михаил Хлебунов. Руководитель направления аналитических исследований в Positive Technologies Ирина Зиновкина подтверждает, что социальная инженерия как была, так и остается одним из основных методов атаки, что говорит о недостаточной подготовке сотрудников. Технический директор «Лаборатории Касперского» в России Евгений Бударин в качестве самой типичной ошибки называет «ненадлежащее невинимательное взаимодействие корпоративных пользователей с внешними ресурсами». Андрей Янкин видит проблему шире: «Если говорить об общих ошибках, то это инерция мышления. Злоу-

мышленник воспринимается как неодолимый вирус, который будет бессмысленно ломиться в периметр компании. На деле это живые люди, которые делают все, чтобы не выдать себя раньше времени».

Угрозы для критической информационной инфраструктуры (КИИ) и госсектора остаются на высоком уровне. «По официальным данным, две трети всех атак направлены на КИИ», — говорит Михаил Хлебунов. Ирина Зиновкина уточняет, что во второй половине 2024-го и первых трех кварталах 2025 года наибольшее количество кибератак пришлось на промышленные организации (17%) и государственный сектор (11%). Эксперт по информационной безопасности «Инфосистемы Джет» Никита Мусиенко отмечает, что именно КИИ, включая госсектор, остается главной мишенью и ключевой угрозой является технологическая зависимость от иностранного программного обеспечения, обновление которого в большинстве случаев стало невозможным.

Статистика инцидентов демонстрирует четкую отраслевую и векторную картину угроз. По словам Михаила Хлебунова, наиболее часто под удар попадают промышленный сектор (27% атак) и телекоммуникационные компании (24%). Среди типов атак лидируют сетевые (41%) и атаки вредоносным ПО, преимущественно шифровальщиками (35%). Валерий Баулин сообщает, что с начала года зарегистрировано 154 публикации баз данных российских компаний в Telegram-каналах и на андерграундных форумах, в открытый доступ попало около 200 млн строк данных пользователей. Лидером по утечкам стал ритейл, на который пришлось 37% публикаций. При этом, как уточняет Денис Гойденко, доля атак через подрядные организации увеличилась с 15% до 28%, а доля атак, в которых злоумыш-



ленникам удалось нарушить бизнес-процессы, выросла с 32% до 55%.

Искусственный интеллект стал неотъемлемой частью кибербезопасности, выступая инструментом как для защиты, так и для нападения. «Тренд 2025 года — появление атак, выполненных практически полностью с помощью участия искусственного интеллекта почти без участия человека», — констатирует Михаил Хлебунов. Эксперт по информационной безопасности «Инфосистемы Джет» Андрей Захаров считает, что ИИ уже перестал быть просто «новым инструментом» и постепенно превращается в ключевой драйвер трансформации всей кибербезопасности. «Формируется новая реальность, в которой ИИ-агенты защитников все чаще сталкиваются с ИИ-агентами атакующих, и обе стороны непрерывно расширяют свой арсенал», — отмечает господин Захаров. При этом, как предупреждает Александр Скакунов, применение ИИ для кибернападения развивается быстрее, чем для защиты, что связано с низким порогом входа для ИИ-хакеров. Григорий Филатов резюмирует: «ИИ не панацея, а усилитель возможностей с обеих сторон. Ну а побеждает тот, кто внедряет технологии быстрее и грамотнее».

Главным вызовом 2026 года эксперты видят необходимость перехо-

да от тотальной защиты к обеспечению киберустойчивости. «Главная задача 2026-го, на мой взгляд, это переход от попыток предотвратить взлом периметра к обеспечению возможности нормальной работы бизнеса в условиях неминуемых кибератак, то есть киберустойчивости. Возлают рано или поздно всех — вопрос в том, к чему это приведет: к остановке бизнеса или ограничению ущерба и быстрому восстановлению нормальной работы», — объясняет Андрей Янкин. Евгений Бударин в качестве ключевого риска называет рост угроз, связанных с внедрением искусственного интеллекта в корпоративную среду. Ирина Зиновкина прогнозирует, что кибератаки в 2026 году чаще будут приводить к комбинированным последствиям — одновременным утечкам данных и нарушениям бизнес-процессов, а также обращает внимание на растущие риски атак на цепочки поставок. Григорий Филатов видит вызов в комплексной проблеме на стыке кадрового дефицита, стремительной эволюции ИИ и растущих финансовых нагрузок, советуя компаниям сосредоточиться на стратегическом развитии внутреннего персонала и интеграции адаптивных платформ.

Филипп Крупанин

информационные технологии

Перестройка облачного будущего

После ухода глобальных облачных провайдеров рынок российских облачных решений переключился на ускоренный режим развития. Компании начали активно перестраивать архитектуры, а отечественные платформы расширили набор сервисов: от управляемых баз данных до инструментов разработки. В итоге заказчик получил не замену западных решений, а технологические среды, которые позволяют строить гибридные контуры под локальные требования безопасности и производительности.

— облачная инфраструктура —

От облаков — к экосистемам

Российский рынок облачных сервисов за последние два года перестроился быстрее, чем за предыдущие десять. По данным «Яков и партнеры», рост остается двузначным, а спрос смещается от базового IaaS к более комплексным сервисам: платформам управления, средам разработки и отраслевым решениям.

Исследование iKS-Consulting фиксирует переход к распределенным архитектурам: в приоритете безопасность, управляемость и возможность быстро разворачивать прикладные решения. Растет доля компаний, использующих несколько облаков, что позволяет гибко распределять нагрузки. В крупных организациях закрепились схема: публичные облака — для масштабируемых задач, частные контуры — для чувствительных данных, локальная инфраструктура — для систем, привязанных к критичным внутренним процессам.

Так облако превращается в часть многоуровневой цифровой среды. Для бизнеса приоритет смещается к предсказуемости и удобству управления: применение гибридных решений становится эффективным способом снизить риски и обеспечить контроль. Сегодня уже более 70% компаний работают в гибридной модели. При этом IaaS используется практически повсеместно, а проникновение PaaS и SaaS достигает 65–66%.

Сегмент public cloud растет быстрее других: к 2030 году его объем в России почти утрояится, и значительная часть увеличения связана с PaaS — управляемыми базами данных, Kubernetes, аналитическими и AI-сервисами. По данным iKS, эти решения формируют основной спрос: компании разворачивают не виртуальные машины, а готовые прикладные стеки.

Российские облака сегодня предлагают экосистемы инструментов, из которых бизнес собирает собственный цифровой контур — управляемый и соответствующий повышенным требованиям безопасности. То есть на рынке востребованы платформы, работающие как часть всей архитектуры и обеспечивающие предсказуемость при высокой нагрузке.

Запрос — ответ

Усложнение корпоративных ИТ-ландшафтов стало нормой: приложения работают в разных контурах, данные распределены между площадками, а требования к безопасности растут ежегодно. При этом просто облачной платформе заказчиков уже недостаточно. Для решения современных задач им требуется среда, способная объединять разнородные инфраструктуры и сервисы в единый управляемый контур. Именно здесь возник запрос на современные облачные платформы. На первый план выходят решения,

которые работают как общий слой управления поверх разных контуров.

Этому запросу отвечают платформы, построенные на принципах распределенной, безопасной и предсказуемой архитектуры, например «Турбо Облако». Их задача — обеспечить сквозную автоматизацию управления ресурсами клиента в любой облачной среде. Такие решения рассчитаны на работу в гибридных сценариях и могут разворачиваться на доверенной инфраструктуре, формируя единый технологический слой поверх локальных ресурсов, частных сегментов и публичного облака. Ключевой принцип — единый слой абстракции над инфраструктурой, который позволяет разворачивать сервисы без ручной интеграции разнородных компонентов. Это снижает зависимость от конкретных вендоров и упрощает перенос приложений между контурами, обеспечивая гибкость и контроль в условиях сложного ИТ-ландшафта.

В отличие от инфраструктурных решений прошлого поколения, различные облачные сервисы строятся вокруг сервисной модели. «Турбо Облако» не является исключением. В этом случае компании-заказчику доступны вычислительные мощности, системы хранения, управляемые базы данных, Kubernetes, CI/CD-инструменты и сервисы безопасности. Преимущество такой схемы в том, что размещение на площадке с прямым доступом к операторским ресурсам снижает сетевые задержки и обеспечивает надежную работу высоконагруженных сервисов: от аналитики до потоковой обработки данных.

Суверенитет имеет цену

Уход глобальных облачных провайдеров стал для российского рынка заметной точкой перелома: он наглядно показал, насколько глубоко бизнес опирался на технологии, которые долгие годы считались отраслевым стандартом. В первую очередь это сказалось на выборе инструментов — с уходом AWS, Azure и GCP корпоративные ИТ-команды лишились привычных сервисов, выстроенных экосистем и интеграций, на которых держалась значительная часть цифровых процессов.

«ТУРБО ОБЛАКО» ДЛЯ ХОККЕЙНОГО КЛУБА	
«Турбо Облако» (входит в коммерческий ИТ-кластер «Ростелекома») перенесло цифровую инфраструктуру олимпийского ХК «Авангард» в облако, чтобы обеспечить устойчивость сервисов при пиковых нагрузках.	
Задачи:	переход от монолита к микросервисной архитектуре; стабильная работа онлайн-продаж билетов и атрибутики во время матчей и акций.
Решения:	развертывание систем в управляемом Kubernetes-кластере; контейнеризация сервисов и автоматизация CI/CD; использование DBaaS, объектного хранилища и сервисов мониторинга.
Результат:	предсказуемая работа сервисов при пиковых нагрузках; снижение операционных рисков; оптимизация затрат на поддержку.

Генеративное государство

— развитие искусственного интеллекта —

Глобальное развитие технологий генеративных нейросетей не проходит бесследно и для госсекторов, которые внедряют ИИ с акцентом на автоматизацию услуг, улучшение принятия решений и обнаружение мошенничества. В России ведомствам было поручено представить правительству свои предложения по интеграции искусственного интеллекта в свои информационные системы, а для развития технологии пишутся «дорожные карты» и составляются концепции. Однако пока в области нейросетей остается много правовых вопросов, что сдерживает его массовое проникновение как в бизнес, так и в госсектор.

Анализ и прогноз

В российском госсекторе внедрение искусственного интеллекта активно развивается — в частности, ИИ уже используется в системе мониторинга и управления национальными проектами и госпрограммами. Правительство применяет ИИ для анализа выполнения мероприятий и прогнозирования рисков, что повышает эффективность государственного управления и цифровизации аппарата. Об этом заявил вице-премьер Дмитрий Григоренко в ходе выступления на «правительственном часе» в Совете Федерации 26 ноября.

«Правительство на сегодняшний день использует искусственный интеллект, в том числе и для анализа прогноза невыполнения различного рода программ и мероприятий. В частности, мы используем ИИ в системе управления нацпроектами и госпрограммами. Искусственный интеллект анализирует запланированные мероприятия, процессы их выполнения и прогнозирует риски. Точность такого прогноза уже достигает 96%.

Это важно, потому что наша задача не фиксировать по факту, что где-то что-то не сделано, а делать так, чтобы все было исполнено», — отмечал ранее Дмитрий Григоренко. Вице-премьер также подчеркивает, что искусственный интеллект не принимает финального решения, а является инструментом, упрощающим работу человека.

Подготовить предложения по дальнейшему внедрению ИИ в информационные системы госсектора господин Григоренко поручил ведомствам по итогам Всероссийского форума контрольных (надзорных) органов в Красноярске. Анализ предложений проведет Минцифры, министерство должно отобразить их в ведомственных планах цифровой трансформации на 2026 год, сообщила «Ведомости».

Минцифры летом разработало проект концепции развития регулирования отношений в сфере технологий ИИ до 2030 года. Свои предложения к документу, в частности, давал Альянс ИИ (входят «Сбер», «Яндекс», РФПИ, МТС, «Вымпелком» и др.). В документе закреплён человекоориентированный подход и установлены жесткие ограничения для применения ИИ, включая требования к маркировке сгенерированного контента. Согласно «дорожной карте» по развитию технологий ИИ до 2030 года, федеральный бюджет вложит 33,3 млрд руб., а внебюджетные источники — 112,6 млрд руб.

Однако пока регулирование ИИ находится в России в серой зоне, хотя разрабатывается законопроект «О регулировании систем искусственного интеллекта в России», а также утверждена национальная стратегия развития ИИ до 2030 года. Также на базе Аналитического центра при правительстве был сформирован Центр развития искусственного интеллекта. Одна из его задач — систематизация внедрения ИИ по всей стране.

Участники рынка отмечают, что с точки зрения регулирования сейчас было бы важ-



ВЫПУСКНОЙ РИМОВА / ГОСПОД

Выросла и стоимость владения инфраструктурой. Российские решения пока не имеют масштаба глобальных платформ, поэтому автоматизация и поддержка обходятся дороже. Для многих компаний переход на локальные облака стал скорее не экономией, а перераспределением затрат — от аренды готовых сервисов к росту собственной инженерной нагрузки.

Еще одно последствие — снижение гибкости. Отечественные платформы не всегда успевают за обновлениями международных экосистем, и это усложняет внедрение современных DevOps-практик, разворачивание CI/CD-контуров и интеграцию с зарубежными SaaS-сервисами. Для бизнеса это означает более длинные циклы внедрения и необходимость адаптировать процессы под новые ограничения.

Проблемой стал и кадровый дефицит: специалистов, хорошо знакомых с отечественными облаками, пока меньше, чем экспертов по AWS или Azure. В результате обучение команд затянулось, а компаниям пришлось перераспределять часть ресурсов от разработки к поддержке инфраструктуры. Наконец, усилился риск технологической изоляции. Глубокая зависимость от локальных решений усложняет интеграцию с международными партнерами и выход на зарубежные рынки.

С этими факторами столкнулся бизнес при переходе на локальные решения. На этом фоне и появился запрос на решения нового класса, которые могли бы компенсировать потери и вернуть компаниям предсказуемость и гибкость.

Гибкая компенсация

За последние два года российский рынок выработал собственные механизмы компенсации. Бизнес понял, что отсутствие глобальных сервисов можно частично перекрыть за счет архитектурной гибкости и появления платформ нового поколения, которые позволяют распределять нагрузку между несколькими контурами и не зависят от одного источника технологий.

Ключевым инструментом стали гибридные и мультиоблачные инфраструктуры. Использование нескольких кластеров одновременно — локальных ЦОДов, частных сегментов и публичных облаков — позволило компаниям минимизировать риски, связанные с переоями, ограничениями доступа или изменением регуляторики. Такой подход возвращает управляемость: критические системы остаются под прямым контролем, а переменные нагрузки — в облаках.

«Наш опыт подтверждает, что облака экономят средства не только на закупке оборудования, но и на его эксплуатации, размещении, обеспечении сетевой связности, отказоустойчивости и соответствии стандартам. Мультиклауд-решение объединяет все эти преимущества, избавляя компанию от крайне затратной самостоятельной реализации единой системы управления», — отмечает генеральный директор «Турбо Облака» Александр Обухов.

Второй компенсирующий фактор — развитие сервисных моделей внутри отечественных платформ. Управляемые базы данных, Kubernetes, системы хранения, CI/CD-инструменты и сервисы для аналитики стали способом закрыть потребность в автоматизации, которую раньше обеспечивали глобальные экосистемы. Для компаний при этом сокращается инженерная нагрузка и появляется возможность выводить продукты на рынок быстрее, чем позволяла бы собственная инфраструктура и кадровые ресурсы.

Постепенно усиливается и сервисная интеграция: отечественные платформы начинают поддерживать единые правила доступа, встроенные механизмы безопасности и сегментирования данных, что ранее обеспечивалось крупными зарубежными вендорами. Это помогает бизнесу выстраивать

предсказуемую модель управления и снижает риск технологической фрагментации.

В итоге, даже потеряв доступ к глобальным сервисам, компании смогли выстроить устойчивые распределенные архитектуры: данные размещаются там, где безопаснее, а сервисы — где быстрее работать. Современные платформы, такие как «Турбо Облако», становятся способом вернуть бизнесу гибкость и управляемость с инструментами, адаптированными под российские требования и ограничения.

По мере развития ИТ-ландшафтов выбор между облаком и локальной инфраструктурой перестал быть ключевым. Компании уже работают в средах, где публичные облака, частные сегменты и собственные площадки выполняют разные роли: критические сервисы остаются в защищенных контурах, а аналитика, тестовые и рабочие пространства для разработки перенесются туда, где их проще масштабировать.

В такой модели важны не типы развертывания, а характеристики данных и требования к скорости обработки. Российские провайдеры подстраиваются под эту логику, развивая экосистемы из IaaS, PaaS- и AI-сервисов, которые можно комбинировать в едином контуре без сложных интеграций. На практике компании выбирают не облако как таковое, а конкретное решение под задачу. Это может быть среда для пилотных проектов, изолированный контур, доступ к GPU и платформам данных.

В таких условиях и востребованы облака, которые обеспечивают предсказуемость при росте нагрузки. По словам Александра Обухова, инфраструктура будет только усложняться из-за роста объемов данных и сервисов и единственный способ сохранить гибкость — правильно распределять нагрузки между контурами. «Зрелость наших облаков растет, и мы уже полностью соответствуем мировым аналогам. Заказчики размещают все более сложные информационные системы. Например, пять-шесть лет назад банки вообще не думали о переносе элементов своей инфраструктуры в облака — теперь ситуация изменилась кардинально. В этой связи отечественный облачный рынок растет быстрее зарубежных аналогов и до 2028 года мы ожидаем прирост около 30% ежегодно», — резюмирует он.

Константин Анохин

но закрепить статус «доверенного ИИ». В этой части, отмечает директор по ИИ группы «Астра» Станислав Ежов, есть два проблема: «Во-первых, нет четкого разделения ответственности разработчика и пользователя при сбоях (особенно в госуслугах), второе — отсутствуют механизмы для тиражирования типовых решений». Следующим шагом, полагает эксперт, нужно внести в закон требование сертификации и единый реестр ИИ-систем для госсектора и объектов критической информационной инфраструктуры.

Господдержка нашла с ИИ общий язык

В 2025 году отечественный бизнес, развивающий большие языковые модели, получил значительную поддержку от государства. Было выделено 7,7 млрд руб. из бюджета, гранты до 100 млн руб. от «Сколково» и Минцифры для LLM и компьютерного зрения, субсидии на облачные GPU. Центр развития ИИ при правительстве начал тиражировать готовые решения», — отмечает Станислав Ежов. Но, по его мнению, в текущей стратегии властей есть упущение: доступ стартапов к вычислениям остается лимитированным. Имеет смысл расширить госмаркетплейс облачных сервисов и создать «цифровые кафедры» в каждом регионе, считает он.

Эпоха «чудо-ботов» прошла, и, по сути, мы наблюдаем переход от экспериментов к инфраструктуре, отмечает директор производственного направления, президент «Девелоники» FabricaONE.AI (ГК Softline) Роман Садрисламов: «Когда совместно с опорой на практический опыт IT-отрасли и запрос бизнеса формируются методологии, стандарты данных, требования к качеству и прозрачности решений, становится обязательным для качественной реализации IT-проекта проверять корректность кода, те-

стировать интерфейсы, документировать результаты на каждом этапе проекта».

Поэтому фокус государственной политики смещается в сторону практического применения, замечают участники рынка. Акцент делается на безопасности данных, совместимости решений и повышении прозрачности процессов. «Сложность в том, что структурам часто приходится работать на стыке импортозамещения и инноваций. Задача — встроить модели и ИИ в архитектуру решений, а не просто показать, что мы развиваем свой независимый путь. Для компаний, которые занимаются заказной разработкой, это означает необходимость работать по конкретным единым стандартам качества. Они вырабатываются в симбиозе и взаимодействии с участниками рынка: вендорами, интеграторами и поставщиками регуляторов», — объясняет Роман Садрисламов. Поэтому, добавляет он, для разработчиков важно не только соответствовать требованиям, но и выстраивать процессы по принципам безопасной разработки: от архитектуры до тестирования. «Так, стандарты РБПО и требования ФСТЭК формируют новую норму рынка, где ценится не скорость вывода продукта, а его устойчивость, управляемость и доверие со стороны заказчика», — заключает эксперт.

Станислав Ежов прогнозирует, что в генеративном ИИ будет развиваться несколько перспективных направлений: «В финтехе будут LLM-ассистенты для клиентов и синтетические данные для fraud-detection. В промышленности — документооборот, дизайн деталей через генеративные модели, которые сокращают время разработки с лет до месяцев. В энергетике — генерация рекомендаций диспетчерам».

Риски и нерешенные вопросы

В то же время внедрение ИИ в госсекторе вызывает опасения у экспертов из-за ряда ри-

сков. В их числе отмечают возможные утечки данных, ошибочные обучающие данные, ошибки на критичных процессах в здравоохранении и производстве. «Организациям стоит вводить системный ИБ в ИИ, изоляцию данных, обязательную подпись специалиста на решения ИИ», — отмечает Станислав Ежов.

Есть также юридические риски, связанные с нарушением авторских прав на генерируемый контент, добавляет эксперт центра ИИ СКБ «Контур» Дмитрий Иванков. По его словам, они также этические (ошибочные или дискриминационные решения ИИ в чувствительных сферах), а также риски, связанные с информационной безопасностью (упрощение создания дипфейков, недостоверных текстов и проч.). Минимизировать их можно как за счет адекватной регуляции, так и методами маркировки контента, добавления дополнительных проверок человеком в критичных процессах, полагает эксперт.

Главным риском становится не сама технология, которая стремительно пришла во все направления, а именно скорость и спешка внедрения этой технологии, считает Роман Садрисламов: «Нужны методологии и метрики, должны быть практические компетенции с учетом разной отраслевой специфики и бизнес-задач». Масштабировать стоит только то, что прошло проверку и имеет понятные механизмы сопровождения, убежден он. «На практике нам уже встречались проекты, когда в спешке внедрялись ИИ-агенты или модели без проверки и без учета архитектуры. И потом исправить ситуацию становится в разы дороже и дольше — нужно откатывать системы, дополнительно тестировать совместимость, перепроверять безопасность и выстраивать процессы по инженерным метрикам и бизнес-метрикам», — заключает Роман Садрисламов.

Светлана Бодрова

информационные технологии

«Что всегда было сильно и в Советском Союзе, и в России — это математические мозги»

Сегодня все российские банки, особенно крупнейшие, активно заменяют импортное программное обеспечение и «железо» на российское. О том, где удалось добиться полного успеха, а какие сегменты еще отстают, „Ъ“ рассказал заместитель руководителя технологического блока — старший вице-президент ВТБ **Сергей Безбогов**.

— мнение —

— На сколько процентов ВТБ удалось импортозаместиться и реально ли это сделать на 100% по «железу»?

— Если мы говорим про ИТ-инфраструктуру, то в этой части мы уже давно покупаем только российское, где это возможно, и на сегодняшний день мы импортозаместились более чем на 80%. Есть постановление правительства и стратегия цифровой трансформации — это два документа, которые нам определяют режим закупок по «железу», и довольно жестко. Для значимых объектов ключевой информационной инфраструктуры (ЗО КИИ) мы в принципе ничего не российско-го покупать не можем. А для всего остального есть нормативы, которые варьируются в зависимости от состояния рынка и наличия на нем необходимых отечественных продуктов. Если говорить о том, чего не хватает, — это высокопроизводительные коммутаторы, коммуникационное оборудование, межсетевые экраны. Этой проблеме не один год. — Для чего нужны коммутаторы и межсетевые экраны?

— Коммутаторы — это сетевое оборудование. Любая большая сеть состоит из разного типа коммутационного оборудования, которое связывает различные приборы между собой. Есть аппаратура, которая стоит на крайних точках сети и требует от коммутаторов не очень большой производительности, но то, что стоит в центре сети и связывает большое количество машин, испытывает очень большую нагрузку. Через эти узлы идут концентрированно большие потоки информации. И для них высокопроизводительных и надежных коммутаторов в российском реестре нет. Это то, что мы называем ядро сети. Коммутатор можно отдаленно сравнить с роутером, который у вас в квартире раздает сигнал на телевизоры, компьютеры и телефоны. Только у вас в квартире два, три, четыре, пять устройств, а в банке их сотни и тысячи.

Межсетевой экран — это фильтр. Такие организации, как ВТБ, получают огромные потоки информации, и им требуется производительность таких фильтров на уровне 100 гигабит в секунду. Межсетевые экраны позволяют фильтровать этот входящий трафик, в том числе отсекая вредоносный. Те российские межсетевые экраны, которые сейчас есть в доступе, могут обеспечить производительность в несколько десятков гигабит в секунду в лучшем случае. Для нас этого недостаточно. Мы пытаемся распределять потоки, ищем какие-то варианты и, где возможно, используем их. Но там, где идет большой поток, через одну «трубу», что называется, там нужно поставить правильно, хорошо работающий, надежный фильтр.

— Есть ли какая-то перспектива производить их в России?

— С межсетевыми экранами история следующая: мы долгое время использовали американскую и израильскую технику, причем это были программно-аппаратные комплексы, своего рода черные ящики, про которые толком никто не знал, что внутри. Сейчас во-



прос в том, найдется ли какая-то иностранная или совместная компания, которая откроет этот «черный ящик» и лицензирует его на российской территории, предьявив все внутренности — и «железо», и программное обеспечение. Одна израильская компания рассматривала возможность выйти на российский рынок, но потом начались события в самом Израиле, и вся история затормозилась. Из того «железа», которое российские компании умеют производить, программисты выжали все или почти все — я имею в виду специальный фильтрующий софт. Теперь нужно делать следующий шаг, но он возможен только на другом «железе», а его пока нет. Стандартное оборудование сейчас тоже разное, становится более производительным, но очень медленно. Ищем различные варианты, может быть, начнем использовать более широко компьютеры со специальными графическими процессорами (GPU). Но вот сейчас, в моменте, мейнстрима, который нас вынесет в нужное русло, не видно.

— Возможно ли закупать какое-нибудь «железо» в дружественных странах?

— Для госкомпаний все, что не является российским, то есть включено в российский реестр, является иностранным вне зависимости от того, дружественное оно или недружественное. Другое дело, что если смотреть на иностранное оборудование, то, конечно, надо выбирать то, что произойдется в дружественных странах. Например, очевидно, что вряд ли нам сейчас имеет смысл бросаться догонять передовые страны по производству уже упомянутых, графических процессоров. В этой области есть Nvidia. Но ей уже на пятки наступают пять-шесть китайских компаний. И они по производительности отстают, но уже не на порядок, а всего лишь в два-три раза. При этом их продукция дешевле, и уже становится экономически целесообразно с учетом всех накладных расходов покупать китайские чипы. Да, их потребуется несколько взамен одного «недружественного», но и цена, и производительность будут сравнимы. Поэтому мы сейчас вместе с нашим партнером T1 всерьез рассматриваем переход на китайские GPU. Если такой чип поставить в российский сервер, то он там будет единственной иностранной деталью, и есть неплохие шансы, что такое устройство сможет пройти сертификацию и будет включено в российский реестр, а значит, станет доступным для импортозамещения. По нормативным доку-

ментам по каждому виду оборудования есть вполне конкретный набор параметров. Следуя им, нужно набрать определенное количество баллов, чтобы изделие попало в российский реестр и стало российским. Понятно, что там не сто процентов российских деталей, но тем не менее это вполне реальный выход. И мы подобную российскую технику уже покупаем. Более того, я думаю, что нерационально все делать самим и догонять тех, кто ушел в серьезный отрыв в каких-то областях. У нас никогда не будет прорыва, если мы будем все время только догонять того, кто делает что-то передовое. На мой взгляд, надо искать другие подходы.

— Может этим прорывом быть квантовый компьютер?

— Эти компьютеры сейчас уже есть, они умеют делать какие-то простые операции, но с ними работать крайне тяжело пока, потому что они требуют специальных алгоритмов. Второй момент, который меня в них смущает сейчас, — что у нас нет достаточного запаса для инвестиций в эту область, чтобы обойти всех остальных. А американцы и китайцы уже вложились в это направление, и нам, получается, опять придется играть с ними в догонялки. Другой пример: ВТБ не стал делать свою большую языковую модель, потому что инвестиции в это колоссальные, и мы считаем, что две такие модели на страну — это более чем достаточно. Особенно имея в виду, что китайцы вообще разрушили весь рынок искусственного интеллекта, выставив открытые модели для общего использования. Безусловно, они на этом собирают для себя большой бенефит, потому что весь мир туда закладывает огромный массив данных, которые китайские производители ИИ естественным путем никогда бы не собрали. Что всегда было сильно и в Советском Союзе, и в России — это математические мозги, и именно это направление нам и следует развивать. Сегодня одна из главных проблем — необходимость экономить вычислительные мощности. Их уже не хватает, несмотря на бешеную производительность, которая к тому же потребляет огромное количество электричества. И чтобы все это вместе было экономически целесообразно, нужно искать новые алгоритмы, которые будут работать более эффективно. И мне кажется, что Россия сильна как раз в этом.

— Если наша сильная сторона — мозги, то с программным обеспечением, в отличие от «железа», у нас должно быть все более или менее хорошо?

— Да, вот с ПО, могу сказать с полной уверенностью, у нас все хорошо. Мы прошли путь по импортозамещению систем, которые работали на высокопроизводительных промышленных решениях типа системы управления базами данных (СУБД) Oracle, которая требовала высокопроизводительного «железа» IBM. Когда и то и другое стало недоступно, мы поменяли полностью архитектуру и теми средствами, которые нам доступны, полностью заменили эту СУБД на обычном «железе». Понятно, там еще есть шероховатости, безусловно, мы что-то доделываем, оптимизируем, но в целом мы решили проблему производительности и надежности. Сейчас наша система совершенно по-другому устроена.

Oracle — это десятилетиями оптимизированная система под проведение большого количества транзакций, в том числе платежей. Например, карточные транзакции — это большая интенсивность, большое количество транзакций в единицу времени по всей стране. Мы сейчас убрали Oracle, взяли Postgre, которая не является такой хорошей высокопроизводительной СУБД — она немножко под другое настроена, но мы научили ее работать со скоростью Oracle, используя другую архитектуру.

— Основной плюс Postgre в том, что она с открытым кодом?

— Да, у нее открытый код и мы и не ограничены никаким «черным ящиком» и санкциями. И плюс есть хорошие профессиональные компании, которые в состоянии ее поддерживать и развивать как продукт внутри России.

— Есть ли интерес со стороны иностранных компаний к тому ПО, которое разрабатывается в России в рамках импортозамещения?

— Мы смотрим на Восток и на Юг. Ряд наработок, которые мы делаем сейчас, безусловно, перспективные и могут быть востребованы. Но и там большинство компаний все-таки ориентированы на западные продукты. Я не думаю, что до тех пор, пока у них не начнутся проблемы, они станут думать о том, чтобы вложить достаточно большие деньги в замену ПО. Мы проводили определенные переговоры, но сейчас пока интерес к нашим решениям не очень высок. К России в целом и к тому софту в частности, который мы предлагаем, пока осторожное отношение. Вот, например, в Китае сейчас мы создали совместное предприятие, которое будет продавать там автоматические системы управления технологическими процессами. У нас есть определенные наработки, и совместно с китайскими коллегами мы планируем осваивать китайский рынок. Это непростая история, но попытки делают почти все, кому есть что предложить.

— У нас грядет внедрение открытых API в банковской системе. Когда об этом только заговорили, все банки были в шоке — боялись делиться своими клиентами, сейчас это уже не кажется большой проблемой — что изменилось?

— Каждый год последние пять лет мы проводим API-хакатон ВТБ, который начинался как совсем небольшая технологическая тусовка, на которой технари, энтузиасты открытых API обсуждали, как это может работать в банке. В этом году у нас было 1,5 тыс. регистраций. В прошлом году к нам пришли два банка, а в этом году — уже четыре. Два-три года назад бизнес очень космически смотрел на открытые API, потому что считается, что от этого выигрывает тот, кто меньше: он делится меньшей базой клиентов, а получает доступ к большей базе. Но сейчас, если вы обратите внимание, «пилоты» в этой сфере делают пока только самые крупные банки. Просто мы понимаем, что можем правильными ограничениями в этом узком кругу обеспечить, чтобы конкуренция была равновеликой. Сбербанк тут стоит особняком, а у остальных вполне сравнимые базы, исчисляющиеся десятками миллионов клиентов. При этом подход друг к другу в этом плане у всех банков очень аккуратный и взвешенный, потому что все понимают, что те-

ма очень чувствительная, поэтому каждый шаг мы всегда согласовываем. Сейчас пока идет притирка. Мы выходим на новый уровень конкуренции, мы начали понимать, что тот, кто владеет приложением как каналом общения с клиентом, тот, собственно, и его вниманием владеет вне зависимости от того, где лежат деньги.

— Владеете — в смысле можете предлагать свои продукты более активно, нежели конкуренты, чьи продукты тоже будут доступны в этом приложении?

— Конечно, и так оно и будет на самом деле. То есть сейчас первая задача не отобрать клиентов, а сделать так, чтобы он через наше приложение шел за всеми финансовыми продуктами, даже чужими. Но и открытость, и закрытость при этом должны быть равные, то есть это будет однозначно совершенно паритетная структура. Сейчас на базе ассоциации «ФинТех» создается оператор открытых API, который будет следить за соблюдением правил игры.

— Но в итоге все должны будут открыть все продукты друг другу или это вопрос договоренности между банками?

— Это вопрос договоренности даже не двух банков, а это вопрос договоренности всего банковского сообщества. Законодательство эту тему не регламентирует, это скорее сейчас под надзором ЦБ. Мы двигаемся постепенно, в настоящий момент это двусторонние отношения, и сейчас можно только посмотреть текущие счета в приложении другого банка. Дальше понятно, что развитие достаточно широкое, вплоть до того, что клиент одного банка из своего приложения сможет заплатить со счета в другом банке. Я думаю, что в конечном счете будут стандартны, к чему, собственно, АФТ и стремится.

— В рамках открытых API ВТБ сотрудничает с главным конкурентом — Сбербанком, а его ИИ будете пользоваться, раз вы говорите, что свой создавать не планируете?

— У нас же, кроме Сбербанка, еще «Яндекс» разрабатывает собственную большую языковую модель. Мы очень уважаем те усилия, которые делает наш крупнейший конкурент, но при наличии альтернативы мы все-таки будем обращаться к ней. Кроме того, есть китайские ИИ. Мы сейчас общаемся с «Яндексом», но это не значит, что мы не обратимся к китайским аналогам. Будем сравнивать.

— К слову о новых технологиях — ВТБ осуществляет прием биометрических платежей в московском и питерском метро, а кроме метро, это где-то еще используется?

— В Московском метрополитене коммерческая биометрическая система (КБС) используется не наша, а самого метрополитена, но все остальное на нас: вся обвязка, которая позволяет идентифицировать человека, провести транзакцию. В Питере мы будем делать уже на нашей КБС. Сегодня мы насыщаем свою эквайринговую сеть терминалами для приема платежей с помощью биометрии. Но ведь биометрия нужна не только для осуществления платежа — в частности, она может использоваться для борьбы с фродом. Гололовая идентификация полезна не только при удаленном общении, но и при обслуживании в офисе. Можно использовать для прохода на мероприятия. Например, мы сделали проход на выставку «Россия» на ВДНХ в прошлом году — человек один раз зарегистрировался на выставке, дальше проходил по лилуте туда и обратно.

— Скажите, есть ли у вас какие-нибудь технологические разработки, которые могут стать прорывом?

— Мы сфокусированы в первую очередь на импортозамещении — в эту сторону направлены наши основные технологические усилия. И мы хотим это сделать максимально быстро и качественно. Мы делаем прорыв на фронте внутреннего архитектурно-технологического периметра, закладываем себе перспективу не меньше чем на десять лет, чтобы точно не пришлось его перерывать.

Беседовал Максим Буйлов

Цифровой случай

— компании и рынки —

По словам Алины Малышевой, есть проблема, которую российский рынок еще не прочувствовал. Это кумуляция рисков, связанных с многочисленными провайдерскими инфраструктурных услуг: крупными ЦОДами, облачными сервисами, операторами связи. Об этой проблеме российские страховщики пока знают теоретически из опыта западных рынков, но уже готовятся и собирают информацию о концентрации рисков, отмечает она.

Конкурентные маркетплейсы

В 2025 году на рынке страхования появляются новые игроки: на него выходят цифровые площадки. О намерениях развивать страховое направление уже заявляли Ozon, «Яндекс» и «Авито» (см. „Ъ“ от 3 октября и 19 ноября 2024 года). Ozon пошел по пути white label, который предусматривает создание страховых продуктов на базе лицензий других страховых компаний. «Яндекс» работает по агентской схеме — продукт разрабатывается вместе со страховой компанией, продается под брендом сервиса, но внутри пользователь получает страховой полис. «Авито» развивает модель встроенных сервисов. Wildberries также запускает совместные проекты со страховщиками.

«Озон Страхование» фокусируется на развитии e-sop и банковского страхования как для физических лиц, так и предпринимателей — продавцов, владельцев ПВЗ, транспортных компаний, уточняет глава направления Денис Гаврилов.

«Мы работаем по партнерской модели: страховой продукт создается страховой компанией, а мы нативно интегрируем его в клиентский путь. Компенсации и урегулирование происходят на стороне страховой компании, а мы обеспечиваем удобство и понятность оформления. Такой принцип уже реализован в страховании объектов в краткосрочной аренде, ОСАГО, страховании ипотеки и связанных рисков», — рассказывает директор по финансовым сервисам «Авито» Татьяна Жаркова. В «Яндексе» и Wildberries не ответили «Ъ-Информационным технологиям».

По словам страховщиков и экспертов, маркетплейсам страхование выгодно. Интерес маркетплейсов к страхованию также продиктован стратегией формирования замкнутой экосистемы сервисов и одновременно необходимостью повышения жизненной ценности пользователя, добавляет директор департамента «Страхование» компании «Рексофт» Никита Евсеев. Такая модель существенно продлевает жизненный цикл клиента, минимизирует отток и позволяет монетизи-

ровать уже сформированные цифровые профили пользователей, поясняет он. Это прежде всего позволяет получить дополнительные доходы от комиссий по страховым продуктам, считает Евгений Изотов.

Партнерская модель хороша тем, что снимает с маркетплейса регуляторную нагрузку: не нужно формировать резервы, управлять страховыми рисками, получать лицензию — площадка отвечает только за витрину и продажи, говорит старший менеджер практики кибербезопасности «ТеДо» Антон Мерцалов. Минусами такой модели, по его словам, являются ограниченный контроль над продуктом и тарифами, а также необходимость делиться частью маржи со страховым партнером.

Впрочем, для перехода на новый этап цифровым игрокам стоит приобрести страховые компании, полагают эксперты. Когда маркетплейсы поймут, что для следующего их качественного шага в сегменте страхования требуется страховая лицензия, а минусы и риски многократно перекрываются плюсами и возможными синергиями, то они тут же обозначат свое присутствие в страховании, отмечает гендиректор НСИС Николай Галушин. Собственная страховая компания дает полный контроль над продуктовой политикой и финансовым результатом, но требует больших вложений и постоянно-

го соблюдения регуляторных, финансовых и ИБ-требований, говорит господин Мерцалов. «Если маркетплейсу хочется быстро запускать продукты, создавать новые правила игры на рынке, он может приобрести страховщика и необходимые страховые компетенции. Приобрести страховщика с лицензией может быть быстрее, чем создавать с нуля», — подтверждает господин Худяков.

При этом создание собственной страховой компании — это другая индустрия, другой уровень регулирования и капитала, поэтому технологической платформе эффективнее усиливать пользовательский опыт через партнерства и точную интеграцию страховых продуктов, отмечает Татьяна Жаркова. Вместе с тем на сегодня известно, что только Wildberries находится в поиске страховой компании (см. „Ъ“ от 30 октября).

Если маркетплейсы будут выходить на страховой рынок со своими компаниями, то возможно серьезное перераспределение рынка, полагает господин Галушин. В зоне пересечения интересов страховщиков и маркетплейсов наибольшим потенциалом обладают простые, стандартизированные и ситуативные страховые продукты — продукты, соответствующие общей философии транзакций через маркетплейс — «быстро, просто, удобно», отмечает партнер Б1 Татьяна Самсонова.

Точечная цифра

Эксперты выделяют другие важные тренды цифровизации страхования. В частности, по словам Антона Мерцалова, параллельно растет использование машинного обучения и ИИ для персонализации продуктов, прогнозирования страховых случаев и борьбы с мошенничеством. Многие передовые решения на рынке связаны с внедрением в бизнес-процессы технологического машинного обучения и искусственного интеллекта, что позволяет существенно ускорить и повысить качество оценки рисков, улучшить маршрутизацию и оценку при урегулировании, более эффективно противостоять недобросовестным практикам, подтверждают во Всероссийском союзе страховщиков.

Увеличивается доля удаленных сервисов — дистанционные осмотры, оформление заявок и урегулирование убытков через онлайн-платформы, которые делают процесс страхования автоматизированным, говорит Антон Мерцалов. Тренды ведут к постепенной смене традиционной модели страхования: оно превращается в сервис, который используется в повседневных сценариях и становится частью другой услуги, что делает рынок более массовым, поясняет он.

Юлия Пославская

информационные технологии

«Банки становятся интеллектуальным партнером промышленности»

Российские банки продолжают совершенствовать цифровые технологии в конкурентной борьбе за корпоративных клиентов. Какие стратегии они выбирают для развития цифровых решений для предприятий, примеры ли созданные для оборонно-промышленного комплекса инновации в гражданском секторе и насколько технологичны российские производства, „Ъ“ рассказал старший вице-президент, руководитель блока развития и цифровизации ОПК ПСБ **Алексей Захаров.**

— мнение —

— На чем сейчас банки делают акцент в развитии решений для промышленности?

— На сегодняшнем банковском рынке борьба за клиентов зачастую сводится к конкуренции цифровых платформ и качеству пользовательского опыта. Важный фактор лидерства — умение слышать клиента и оперативно дорабатывать системы под индивидуальные потребности как гражданских предприятий, так и ОПК.

Мы продолжаем разрабатывать и улучшать наши сервисы так, чтобы взаимодействие клиентов с банком было максимально комфортным: сокращаем время предоставления услуг, создаем дополнительные инструменты цифровой безопасности, автоматизируем различные виды отчетности, интегрируем банковские сервисы с корпоративными системами API. Отдельное внимание уделяем модели Banking as a Service — прорабатываем варианты встраивания своей инфраструктуры, банковских продуктов в бизнес-процессы контрагентов с учетом выявления такой потребности и заинтересованности с их стороны.

— Как происходит эволюция банковских решений для промышленности? Вы следите за запросом предприятий или сами предлагаете инновации?

— При разработке новых решений мы сочетаем нашу отраслевую экспертизу, потребности предприятий и анализ больших данных. Это позволяет действовать на опережение: внедрять технологии до того, как они станут рутинной. И, конечно, подстраиваем цифровые сервисы под процессы клиента, а не наоборот. Сначала наши клиентские и продуктовые менеджеры, ИТ-специалисты глубоко погружаются в клиентский бизнес, в специфику производственных процессов предприятий, их методологию и культуру рабо-



PHOTOGRAPH BY ALEXANDER KURBANOV

но происходит при соблюдении жестких требований к защите данных — обязательно многоуровневая проверка на соответствие стандартам безопасности и устойчивости процессов.

— В каких отраслях цифровые банковские решения наиболее востребованы и какая их доля приходится на гражданский бизнес, а какая — на ОПК?

— Гражданский сектор более активно пользуется цифровыми продуктами, что обусловлено объективным фактором — им проще оперативно внедрять ИТ-изменения. ОПК, как стратегическая отрасль, обеспечивающая суверенитет страны, работает в условиях высоких стандартов безопасности, что стимулирует создание новых особо защищенных технологических решений.

Соотношение цифровых банковских продуктов в ОПК и гражданских отраслях уже постепенно меняется: ОПК наращивает тем-

пам образом. Объективные факторы, повторюсь, жесткие требования к информационной безопасности и необходимость использования импортозамененных решений. Надо учитывать и возможные сложности, возникающие при интеграции новых решений с legacy-системами в процессе перехода на целевые платформы. На всех этапах — от проектирования до эксплуатации — мы исходим из действующих регуляторных норм, касающихся безопасности критической инфраструктуры, обеспечивающих защиту государственной, коммерческой и банковской тайны. ПСБ организовал в структуре банка специализированный контур для гособоронзаказа, который направлен на строгое соблюдение высоких стандартов защиты чувствительных данных оборонных предприятий при предоставлении банковских услуг и сервисов.

— Можно ли адаптировать те цифровые решения и продукты, которые вы разрабатываете для ОПК, для использования гражданскими предприятиями?

— Да, можно. Большинство цифровых решений и продуктов, разработанных для предприятий ОПК, могут быть успешно использованы предприятиями гражданских отраслей. Но тут важно понимать, что военные стандарты информационной безопасности и сертификации могут быть избыточными для гражданских задач, соответственно, при тиражировании могут понадобиться определенные доработки. Также существуют риски технологической несовместимости: отдельные решения ОПК могут не иметь простого способа интеграции с существующей гражданской ИТ-инфраструктурой, например, из-за недостаточного уровня импортозаменения в последней.

ИННОВАЦИОННЫЕ РАЗРАБОТКИ ПРЕДПРИЯТИЙ ОПК

Платформа IIoT.Istok для промышленности и медицины

Научно-производственное предприятие «Исток» имени Шокина холдинга «Росэл» госкорпорации «Ростех» разработало платформу промышленного интернета вещей IIoT.Istok для удаленного мониторинга, диагностики и оптимизации работы технологического и инженерного оборудования, производственных линий и других объектов с возможностью интеграции в корпоративные информационные системы. По совокупности функциональных возможностей на текущий момент IIoT.Istok не имеет аналогов среди отечественных решений и может применяться в самых разных отраслях: от промышленности до строительства. Система уже внедрена на ряде оборонных предприятий и используется в рамках федерального проекта «Персональные медицинские помощники».

Платформа в автоматическом режиме собирает данные со множества встроенных датчиков и объединяет их в единую систему диспетчеризации, позволяя создавать цифровые двойники промышленного оборудования и дистанционно управлять установками. Благодаря встроенным алгоритмам искусственного интеллекта платформа проводит автоматическую диагностику неисправностей и предиктивный анализ технического состояния в режиме реального времени.

В рамках проекта «Персональные медицинские помощники» цифровое решение обеспечивает дистанционный мониторинг состояния здоровья людей с хроническими заболеваниями: артериальной гипертензией, сахарным диабетом, гестационным сахарным диабетом, гипертензивными расстройствами во время беременности. Платформа собирает результаты измерений с различных устройств — портативных носимых медицинских изделий, которые пациент может использовать самостоятельно в домашних условиях без помощи

врача, — и передает эти измерения в электронные карты пациентов в медицинских информационных системах. Дополнительно осуществляет контроль жизненного цикла устройств (проверка работоспособности, порочного периода и других технических параметров).

Система коллективного автоматизированного проектирования

Программно-аппаратный комплекс систем автоматизированного проектирования (ПАК САПР) — разработка холдинга «Росэл» госкорпорации «Ростех». Это первое полностью отечественное решение, которое объединяет программные, аппаратные средства и комплекс суперкомпьютерного моделирования. Комплекс обеспечивает полный цикл создания изделий электронной компонентной базы, радиоэлектронной аппаратуры и сложных технических систем на высоком уровне. Ускорение процесса проектирования достигается за счет автоматизации расчетов, моделирования и тестирования, а также оптимизации маршрутов проектирования и разработки. Кроме того, запуск суперкомпьютерных вычислений дает возможность моделировать физические процессы в проектируемых изделиях и существенно ускорять решение сложных задач при создании инновационной продукции.

ПАК САПР объединяет не только мощные вычислительные ресурсы и современные российские инструменты проектирования, но и передовые технологии коллективной работы. Это означает, что сразу несколько специалистов могут работать над проектом, используя облачные технологии для обмена данными и совместной работы.

Универсальный комплекс может применяться в различных отраслях промышленности, включая микро- и радиоэлектронику, приборостроение, аэрокосмическую аппаратуру, изделия машиностро-

— Для нужд оборонно-промышленного комплекса вы разрабатываете новые механизмы?

— Все опять же зависит от потребности предприятия — либо адаптируем существующие отраслевые решения под особые требования ОПК, их производственную и операционную специфику, либо разрабатываем принципиально новые продукты. Мы помогаем предприятиям ОПК решать разного уровня цифровые задачи, в частности для обеспечения прозрачного контроля за цепочками поставок и исполнения обязательств по гособоронзаказу.

— Насколько технологичны российские производства и какие из них наиболее технологичные — гражданские компании или ОПК?

— Не стоит противопоставлять гражданскую промышленность и ОПК — эти секторы экономики имеют свою уникальную специфику, но во многом взаимодополняют друг друга и вместе работают в интересах технологического суверенитета страны. Сегодня предприятия стремятся задействовать новые технологии и искусственный интеллект для совершенствования производственных процессов. По разным оценкам, к 2030 году внедрение искусственного интеллекта в разных отраслях экономики принесет России дополнительный доход в размере более 11 трлн руб. При этом 35% российских промышленных предприятий уже так или иначе используют ИИ, а 25% — находятся на разных стадиях его внедрения.

Уже сейчас ИИ помогает следить за оборудованием предприятий: анализирует и прогнозирует неисправности критически важных механизмов, предотвращает проблемы до их фактического появления. Отмечу аэрокосмическую отрасль, где ИИ следит за состоянием работы авиационного двигателя и прогнозирует запас температуры газов в турбине на основе проводимого анализа. Такой мониторинг реализован и работает на отечественной платформе. Очевидное преимущество искусственного интеллекта — это его гибкость и универсальная применимость для широкого круга задач и возможность адаптации решений на его основе практически для любой отрасли. Например, технологии компьютерного зрения, изначально созданные

Соотношение цифровых банковских продуктов в ОПК и гражданских отраслях уже постепенно меняется

для беспилотного транспорта, сегодня успешно используются для промышленного контроля качества в цехах, распознавания дефектов и в навигационных системах дронов.

Для ОПК искусственный интеллект может облегчить исполнение гособоронзаказа за счет повышения эффективности и точности производственных процессов. Мониторинг качества изделий может обеспечивать компьютерное зрение, цифровые двойники позволяют оптимизировать характеристики изделия еще на этапе проектирования и повысить скорость выпуска новых образцов техники, а роботизированные комплексы уменьшают вероятность операционных ошибок в рутинных процессах. В роли финансового и цифрового партнера в ПСБ выстроена надежная «экосистема» поддержки предприятий при модернизации производственных мощностей.

— Какие стратегии выбирают предприятия в цифровом развитии — это оптимизация ИТ-ландшафта, внедрение каких-либо точечных решений или все же более глобальная трансформация всех бизнес-процессов?

— Если говорить о крупных предприятиях с госучастием, то здесь компании, и в том числе

банки, движутся по двум взаимосвязанным направлениям цифрового развития. Первое — выполнение обязательных требований государства. Правительством РФ и Минцифры России утверждена система нормативов в области цифровой трансформации. У каждого крупного предприятия должна быть своя стратегия в этой области, планы по переходу на отечественные решения и по повышению киберустойчивости. По закону субъекты критической информационной инфраструктуры обязаны полностью перейти на отечественное ПО и оборудование в жесткие сроки. Поэтому многие компании сфокусированы на оптимизации всего ИТ-ландшафта и выполнении регуляторных требований.

Второе направление — адресные проекты, направленные на повышение эффективности. Компании, у которых уже есть надежный ИТ-фундамент, активно запускают инициативы, например, с использованием того же искусственного интеллекта. Именно производственная отрасль лидирует во внедрении этой технологии. Во многом это стало возможным благодаря большому количеству данных, готовых к использованию на производстве, а эффект от внедрения инициатив четко измерим, например, при снижении дефектов или оптимизации ресурсов.

— Какие специалисты нужны для предприятий в процессах цифровой трансформации?

— Цифровизация — это сложный процесс, включающий, помимо технологического обновления, стратегическую трансформацию бизнес-модели и даже корпоративной культуры. Конечно, эти процессы невозможны без высокопрофессиональных кадров, умеющих работать с данными, алгоритмами и информационными системами. Нужны специалисты, которые одновременно понимают бизнес-логику, цифровые технологии и производственные процессы.

Внимание к подготовке кадров обращено на самом высоком уровне — действует проект «Цифровые кафедры» в рамках национального проекта «Молодежь и дети», призванный обеспечить приоритетные отрасли экономики высококвалифицированными кадрами, обладающими цифровыми компетенциями. Благодаря партнерству с ПСБ студенты смогут получить практический опыт,

что сделает знания применимыми. Наличие специалистов, способных говорить с промышленниками на одном языке, снижает барьеры внедрения цифровых решений и позволяет учитывать специфику производства при цифровизации.

— Как, по вашей оценке, будет идти дальнейшее развитие цифровых сервисов и продуктов с использованием ИИ для предприятий промышленности?

— Отмечу большие перспективы технологии цифровых двойников, которая позволяет воспроизводить характеристики изделия в реальных условиях эксплуатации. С учетом физики процессов, внешних воздействий, ресурсных ограничений и сценариев боевого применения цифровые двойники сокращают время на реальные испытания без потерь в качестве изделия.

Текущие темпы развития агентных систем на основе искусственного интеллекта позволяют прогнозировать появление автономных цифровых «сотрудников», которые самостоятельно выполняют задачи, взаимодействуя между собой и с внешними системами, учатся на доступных данных и в отдельных случаях принимают решения.

Дальнейшая интеграция систем банка с ИТ-системами клиентов на фоне внедрения ИИ-агентов позволит пересмотреть стандарты бесшовного обслуживания. Разработанные банками ИИ-агенты будут способны оптимизировать графики платежей для недопущения кассовых разрывов и прогнозировать потребность в оборотных средствах с учетом загрузки производственных мощностей, своевременно хеджировать курсовые риски под график закупок импорта, а также подбирать наиболее подходящие клиенту условия кредитования с минимальным пакетом документов и многое другое.

В рамках производственного функционала ИИ-агенты могут не просто выявлять агрегаты и узлы, подлежащие ремонту, но и проверить на складе наличие нужных комплектующих, в случае необходимости — заказать новые и отслеживать сроки поставок. Но для качественной и оперативной работы ИИ-агентов как при предоставлении банковских продуктов, так и при оптимизации производственных процессов требуется глубокая интеграция ИТ-систем, включая ERP, MES, CRM и другие.

Конечно, как бы ни были самостоятельны ИИ-агенты, они должны оставаться помощниками, «вторыми пилотами», а все основные решения — на стороне человека. В свою очередь, максимальное число рутинных задач целесообразно оставить для цифровых «коллег». И банки, обладающие одновременно отраслевой экспертизой и ИТ-компетенциями, переосмысливают роль интеллектуальных партнеров промышленности за счет поставки ИИ-агентов, которые позволяют предприятиям максимально сфокусироваться на индустриальных задачах.

Бесседовал Максим Буйлов

информационные технологии



Бизнес налаживает коммуникацию

Рынок коммуникационных сервисов переживает сдвиг от отдельных каналов к полноценной платформе. Современные решения объединяют отправку уведомлений, управление вызовами, интеграцию с CRM и аналитическими системами, что позволяет бизнесу выстраивать качественные сценарии обслуживания и персонализированные взаимодействия.

— телекоммуникации —

В этом контексте необходимые бизнесу объединенные решения предоставляет Telecom API, который становится ключевым связующим звеном между компаниями и современными коммуникационными сервисами. Так, по данным «ТМТ Консалтинг», объем российского рынка Telecom API в 2023 году увеличился на 26% год к году, до 5,8 млрд руб. При этом в 2024 году его рост прогнозировали на уровне 25%, до 7,2 млрд руб., а в 2025-м — на 23%, до 8,9 млрд руб.

По данным SNews, интеллектуализация общения становится одним из ключевых драйверов рынка: компании ищут ИИ-системы, которые в режиме реального времени могут помочь операторам подобрать оптимальные ответы. Такие технологии сокращают нагрузку на сотрудников колл-центров и повышают рост качества их работы за счет автоматизации процессов. «С точки зрения использования технологий в голосовых коммуникациях может показаться, что все уже изобрели. Но это не так. У голоса открывается второе дыхание. И именно сейчас новый комплекс решений — маркировка, ИИ-ассистенты, речевая аналитика — начинает формировать у клиентов новые паттерны потребления и иные привычки. Норма взаимодействия с бизнесом становится другой», — напоминает гендиректор MTC Exolve Рамиль Биккужин.

Согласно CNewsMarket, в 2025 году лидером рейтинга провайдеров Telecom API стал MTC Exolve. На втором месте — Voximplant, на третьем — «Телфин». Так, в MTC Exolve рассказали „Ъ“, что по итогам девяти месяцев 2025 года выручка компании увеличилась на 26%, а выручка от продуктов Telecom API — на 45%. Развитию бизнеса и лидирующим позициям в рейтинге способствует большое количество релевантных потребностям рынка решений. В частности, компания уделяет много внимания разработке на основе искусственного интеллекта (ИИ). «Искусственный интеллект ускоряет производительность и позволяет автоматизировать рутину. В своих продуктах мы масштабно используем технологии с ИИ — например, когда выстраиваем коммуника-

ционную стратегию для клиента», — отмечает господин Биккужин.

Параллельно нарастает тренд консолидации коммуникаций: компании стремятся объединить все каналы коммуникаций с клиентами на единой платформе. Это дает им возможность адаптировать маршрутизацию, сценарии и интеграции под специфические бизнес-задачи. Голос на цифровой платформе превращается в самостоятельный и многофункциональный канал: голосовые API теперь используются не только для звонков, но и для аутентификации, верификации номеров, запуска роботов и сбора обратной связи. В условиях трансформации у бизнеса появляется потребность и в прозрачности связи. Перспективы рынка связаны с углублением симбиоза облачных коммуникационных платформ и традиционной связи. «Главный тренд — это повсеместное внедрение программно-определяемого подхода, который позволяет бизнесу быстро адаптироваться к изменениям и масштабироваться без капитальных вложений в „железо“», — считает руководитель практики UC и ПО для совместной работы «K2Tech» Владимир Сергеев. В этом контексте компании ищут технологии, которые также повышают уровень безопасности, снижают риск мошеннических звонков от имени бренда и шанс попадания номеров под спам-фильтры операторов. Наконец, рынок Telecom API испытывает ускоренное развитие и от архитектурных изменений — облачные и serverless-модели, готовые SDK и инструменты отладки снижают порог входа для разработчиков и позволяют быстрее запускать новые сценарии. «Отечественный рынок CPaaS находится в особых условиях по сравнению с общими рынками — сказываются в том числе и текущие ограничения популярных мессенджеров. Это является своего рода дополнительным драйвером роста данного сегмента», — говорит гендиректор хостинг-провайдера RUVDs Никита Цаплин.

Среди основных векторов развития технологий бизнеса — создание голосовых роботов. Эта разработка представляет собой виртуального сотрудника для автоматизации рутинных разговоров, неотличимых от живого собеседника. По данным MTC



Exolve, внедрение робота может эффективно заменить до 1 тыс. сотрудников колл-центра за счет способности совершать и принимать звонки по скрипту, а также отправлять СМС-сообщения. Виртуальный помощник использует адаптивный синтез естественной речи, распознает запросы клиента и использует данные из внешних информационных систем, а затем передает детальную информацию о своей работе в CRM, BI системы и сервисы сквозной аналитики.

«Компании отошли от экспериментального использования API к их стратегическому внедрению в ключевые процессы. В новых условиях бизнесу требуется не просто набор сервисов, а целостная коммуникационная система», — говорит Владимир Сергеев. «Именно CPaaS-платформы отвечают на эти вызовы, они являются тем самым фундаментом, который позволяет бизнесу консолидировать все каналы коммуникаций». Он добавляет, что ключевые потребности отрасли сегодня — это гибкость, безопасность и бесшовная интеграция. Время разрозненных решений, которые сложно масштабировать и поддерживать, окончательно ушло, напоминает эксперт.

Еще одно важное направление Telecom API — развитие речевой аналитики. Данный инструмент работает на стыке лингвистики и машинного обучения. «Речевая аналитика позволяет охватить 100% звонков и увидеть, как сотрудники общаются, определить все проблемные участки. Сотрудники пони-

мают, что некорректно кому-то ответить уже не получается — речевая аналитика считает каждый случай. Сейчас это одна из топовых услуг, которая очень востребована: все хотят выстраивать долгосрочные отношения с клиентами», — объясняет Рамиль Биккужин. На востребованность инструмента влияют и его возможности: речевую аналитику можно использовать и для текстового общения в режиме реального времени — система Co-Pilot анализирует вопросы клиента и подсказывает правильный ответ.

MTC Exolve недавно запустил новую версию виртуальных контактных центров на базе отечественного ПО, которое может защитить заказчика от утечек данных и перебоев в работе инфраструктуры. Теперь сервис позволяет использовать ИИ-технологии, такие как речевая аналитика и Co-Pilot, и омниканальные инструменты: голос, чат, мессенджеры и email, в одном интерфейсе для целостного управления инфраструктурой бизнеса. В виртуальных центрах также можно использовать сторонние GPT-модели для улучшения оптимизации клиентского обслуживания. На это же влияет и интеллектуальная маршрутизация обращений на анализе данных из CRM.

«Мы движемся от продажи отдельных услуг (канал, номер, СМС) к созданию целых коммуникационных экосистем, на горизонте трех-пяти лет будут появляться платформы, которые объединяют несколько задач и несколько инструментов», — считает

Рамиль Биккужин. Помимо «драйверных» ИИ-решений, компании уделяют внимание и улучшению своих API-технологий. Например, в MTC Exolve Voice API помогает быстро подключать стандартные SIP-телефоны, строить голосовые интерфейсы и при необходимости быстро масштабировать систему. С SMS API бизнес может создать инфраструктуру рассылок, следить за отчетностью и изменениями и интегрировать статистику в свои ресурсы. Numbering API позволит настроить местные, короткие, мобильные и многоканальные номера для задач бизнеса, а Mobile SDK — снизить затраты и нагрузку на традиционную телефонию, ускорить соединение и упростить инфраструктуру за счет передачи звонков, ID клиента и контекста.

«Уровень автоматизации в коммуникациях с клиентами в малом и среднем бизнесе продолжит расти благодаря этой гибкости. Очевидно, что компании не хотят тяжелых, больших, дорогих решений — они хотят простые сервисы, которые решают конкретную задачу», — напоминает Рамиль Биккужин. С ним соглашается Никита Цаплин: «Решения CPaaS работают как единое окно, обеспечивая максимальную эффективность коммуникации. Они дают большую экономическую выгоду по сравнению с обычными коммуникационными средствами». Другими важными преимуществами использования подобных систем являются расширенные аналитические возможности и применение индивидуального подхода при общении с клиентами, добавляет эксперт.

«Главный вызов — обеспечить не просто технологическую замену, а стратегическую трансформацию коммуникаций в актив, который повышает устойчивость и эффективность бизнеса в долгосрочной перспективе», — считает Владимир Сергеев. Развитие рынка связано с углублением симбиоза облачных коммуникационных платформ и традиционной связи, добавляет он. В дальнейшем рынок также будет искать точки роста во внедрении RCS и расширении аналитических возможностей, а объем отрасли продолжит увеличиваться «как минимум до начала следующего десятилетия» и может нарастить финансовые показатели почти в два раза по сравнению с нынешним периодом, прогнозирует Никита Цаплин. «Бизнесу, который хочет оставаться эффективным, придется перестроиться под новую парадигму. Будущее — за интеллектуальными, предсказуемыми и уважительными коммуникациями, где технологии служат цели создания настоящего диалога с клиентом», — заключает Рамиль Биккужин.

Василиса Аксенова

«Для злоумышленника важен не размер компании, а наличие у нее данных»

— мнение —

В конце года Positive Technologies выпускает коммерческую версию своей антивирусной технологии, встроенной в продукт MaxPatrol EPP. О том, почему бизнесу любого размера сегодня нужна комплексная защита конечных устройств — компьютеров, виртуальных рабочих мест и серверов — от массовых и целевых атак, как выполнить требования регулятора без лишних затрат и почему «еще один антивирус» не замедлит работу инфраструктуры, в интервью «Ъ Информационным технологиям» рассказал руководитель департамента разработки средств защиты рабочих станций и серверов Positive Technologies СЕРГЕЙ ЛЕБЕДЕВ.

— Согласно вашему исследованию, каждую пятую успешную кибератаку на компанию сегодня составляют массовые атаки. Почему даже крупный бизнес, уже инвестировавший в информационную безопасность, остается уязвим для таких, казалось бы, простых угроз?

— Основная причина в том, что фокус защиты сместился на сложные целевые атаки. Средства защиты от них требуют высокой квалификации специалистов и сложны в настройке. В результате базовые, но критически важные средства защиты от массовых атак, которым не нужно глубокое погружение, могут быть не установлены или выключены в угоду производительности. Дело в том, что массовые атаки — это базовый вектор, от которого должна быть защищена любая компания. Если его игнорировать, злоумышленник получит легкую точку входа в инфраструктуру, что сведет на нет все инвестиции в защиту от целевых угроз.

— Вы делаете акцент на важности построения комплексной защиты конечных устройств (endpoint security). Почему сегодня недостаточно просто иметь антивирус? В чем принципиальная разница между защитой от массовых и целевых атак и почему продукт должен покрывать оба вектора?

— Классический антивирус — это необходимая основа, но он в основном защищает от известных, массовых угроз по сигнатурам. Целевые атаки используют неизвестные уязвимости (нулевого дня), уникальное вредоносное ПО и скрытные методы, которые нельзя обнаружить только сигнатурным анализом. Разница очень большая: массовая атака — это как спам, который приходит тысячам компаний одновременно. Целевая — это точечное, тщательно подготовленное воздействие на конкретную организацию для кражи данных или останова важных бизнес-процессов. Наше решение MaxPatrol EPP является частью общей концепции защиты конечных устройств, которая объединяет в себе классический антивирусный модуль для отражения массовых угроз и продвинутые технологии класса EDR, которые вовремя определяют вредоносную активность для обнаружения сложных целевых атак по аномальному поведению. Это позволяет закрыть оба вектора одним агентом на конечном устройстве. Про-



дукт должен защищать и от тех, кто только «стучится в дверь», и от тех, кто уже тихо проник внутрь.

— Вы говорите об экономии ресурсов за счет «одного поставщика». Можете объяснить на конкретных примерах, как консолидация защиты на одной платформе снижает операционные затраты и общую стоимость владения?

— Экономика формируется на нескольких уровнях. Первый и самый очевидный — это один агент вместо нескольких. Компании больше не нужно думать о совместимости разных продуктов, закупать лицензии у разных вендоров и тратить значительное время и бюджет на их сложную интеграцию в инфраструктуру. Это прямая экономия на закупках и внедрении.

Второй уровень — это единая консоль управления. Специалист по информационной безопасности видит все события в одном интерфейсе: от срабатывания антивируса на массовую угрозу до подозрительного поведения процесса, выявленного с помощью глубокого анализа распределенных по времени событий — это умеет MaxPatrol EDR, продукт для обнаружения и реагирования на сложные и целевые атаки. В результате сокращается время на рассматривание и расследование инцидентов, на обучение сотрудников работе с разными системами и снижаются операционные риски из-за возможной ошибки человека при переключении между интерфейсами. Проще говоря, один специалист может эффективно контролировать большую инфраструктуру.

Третий уровень — это оптимизация жизненного цикла. Работа с одним поставщиком по единому контракту упрощает процессы технической поддержки, обновлений и расширения лицензий. В конечном счете для компании это означает минимизацию затрат на одного пользователя, сокращение операционных расходов на сопровождение и предсказуемость бюджета на кибербезопасность.

— Раньше считалось, что сложные решения кибербезопасности — это удел крупных корпораций. Вы же заявляете, что ваше решение актуально и для среднего, и даже малого бизнеса. Что изменилось?

— Изменились сама природа угрозы и ее бизнес-последствия. Сегодня жертвами киберпреступников становятся не только крупный бизнес и госструктуры, но и абсолютно любая компания, даже из сегмента малого и среднего бизнеса. Для злоумышленника важен не размер компании, а наличие у нее данных, денег на счетах или вычислительных ресурсов. Кибератака может привести к полной остановке операционной деятельности, необратимой потере критичных данных, крупным финансовым штрафам со стороны регуляторов, невосполнимым репутационным потерям и требованиям выкупа. Для малого бизнеса с ограниченными резервами такой инцидент часто равнозначен закрытию. Наш подход позволяет предложить таким компаниям доступное по цене, но при этом комплексное решение «из коробки». Оно не требует для своего обслуживания целого штата экспертов.

— Вывод на рынок антивируса Positive Technologies — это ответ на запрос рынка или часть долгосрочной стратегии по созданию экосистемы собственных решений безопасности?

— Это последовательное выполнение нашей долгосрочной стратегии по созданию полноценной экосистемы решений безопасности. Мы планомерно двигались к тому, чтобы сейчас у компаний появился надежный инструмент для защиты конечных устройств от массовых атак. Выполняем обещания, данные в начале года после покупки доли в белорусском вендоре «ВИРУСБЛОКАДА». Сейчас мы предлагаем рынку не просто еще один антивирус, а готовый, встроенный модуль для защиты конечных устройств в рамках единой платформы. И следующим шагом антивирусная технология будет доступна в нашем продукте для обеспечения киберустойчивости промышленных инфраструктур PT ISIM, а в песочнице PT Sandbox станет центральным элементом безопасности. Это напрямую отвечает на запрос рынка на комплексные, интегрированные решения от одного проверенного поставщика.

— Вы упоминаете новые требования ФСТЭК к сертификации (CAV3 и COP). Насколько готовы российские компании к их выполнению и как бизнесу закрыть этот вопрос без лишних затрат и сложностей?

— Существующие требования ФСТЭК к средствам антивирусной защиты (CAV3) и новые требования к средствам обнаружения и реагирования (COP) — это серьезный нормативный вызов, особенно для компаний, которым важно выполнять требования регулятора и

работать с чувствительной информацией. Многие организации не готовы к самостоятельному, сложному и дорогостоящему процессу приведения своих разрозненных систем защиты в соответствие с этими требованиями — для этого требуются специальная экспертиза и ресурсы. Наше решение, будучи сертифицированным, снимает с компании эту задачу. Мы предоставляем уже готовый продукт, соответствующий требованиям регулятора, который можно внедрить в существующую инфраструктуру. Это означает значительную экономию времени, экспертных и финансовых ресурсов компании. Особенно это важно для организаций, которые относятся к критической информационной инфраструктуре. Для них соответствие не просто рекомендация, а необходимое условие для непрерывности деятельности.

— Один из главных страхов IT-директоров при внедрении нового защитного решения — что оно «положит» производительность рабочих станций и серверов. Как вы решаете этот вопрос?

— Для нас это было одной из основных инженерных задач. Антивирусный модуль создавался с учетом современных проверенных технологий оптимизации и минимального потребления ресурсов. Мы провели большую работу, чтобы минимизировать нагрузку на основные компоненты: центральный процессор, оперативную память и дисковую подсистему. В результате внедрение не приводит к заметному для пользователя или бизнес-процессов замедлению работы рабочих станций или серверов. Мы добились того, что продукт обеспечивает безопасность, не ставя под угрозу непрерывность и продуктивность бизнеса.

— Как мы понимаем, антивирусный модуль — это лишь часть большой картины. Как он интегрируется с другими вашими продуктами и что это даст клиентам в будущем?

— Глубокая интеграция является фундаментом для построения экосистемы. Антивирусный модуль становится частью единого агента для защиты конечных устройств, что обеспечивает взаимосвязь на уровне данных, управления и реагирования.

Это открывает для клиента новые возможности. Во-первых, данные с антивирусного модуля, например о заблокированной массовой угрозе или о подозрительном файле, автоматически поступают в движок корреляции событий MaxPatrol EDR. Это позволяет проводить поведенческий анализ и выявлять сложные многоэтапные атаки, которые по отдельным, разрозненным событиям могли бы остаться незамеченными. Во-вторых, любой подозрительный объект, вызвавший сомнение у аналитика или системы, можно в один клик отправить на углубленный динамический анализ в PT Sandbox. Это дает точный ответ на вопрос, является ли файл частью целевой атаки, даже если его сигнатура неизвестна. В будущем такая же глубокая интеграция планируется с другими продуктами, например с разрабатываемым почтовым шлюзом PT Email Security для анализа вложений из почтового трафика.

Интервью взял Филипп Крупанин

информационные технологии

Технологии бизнес-масштаба

Российский ИТ-рынок в последние годы активно трансформируется и все больше начинает играть роль одного из значимых драйверов экономики. Однако после периода бурного импортозамещения, спровоцировавшего не менее бурный рост ИТ в стране, компании—потребители технологий перешли к более взвешенным инвестициям и фокусируются в первую очередь на повышении эффективности уже внедренных технологий, развивают прикладные решения, платформы, аналитику и системы информационной защиты.

— цифровизация —

Как результат в ИТ-холдинге Т1 уверены, что по итогам 2025 года динамика отечественного сегмента продажи ИТ-услуг, ПО и ИТ-оборудования для В2В-сектора замедлится и рост рынка в этой части составит около 3%. Хотя к следующему году ожидается, что кривая снова пойдет вверх более выраженно и речь сможет идти уже о десятипроцентном приросте год к году. В компании отмечают, что основными направлениями развития отрасли остаются программное обеспечение (ПО) и ИТ-сервисы. Позитивная динамика этого сегмента по итогам 2025 года и по прогнозу на 2026 год произойдет именно за счет стандартизации внедрений, повышения зрелости уже существующих решений, перехода к управляемым облачным сервисам и «операционализации» ИИ.

Тем не менее сегодня устойчивость российской экономики невозможна без технологической независимости. И практика отдельных отраслевых лидеров такова, что их подходы к развитию ИТ и внедряемые решения способны двигать вперед весь рынок: от импортонезависимой облачной инфраструктуры и процессинга до автоматизации критической инфраструктуры. Подобные проекты становятся драйверами технологического развития, а иногда и ИТ-суверенитета страны.

Во главе угла взвешенный подход

Бизнес все более четко определяет приоритеты использования ИТ, а эксперты анализируют ключевые тренды и выделяют перспективы развития различных сегментов рынка для масштабирования своей деятельности.

«Сегодня рынок прошел важный этап — от вынужденных изменений к осмысленному, взвешенному развитию», — замечает директор департамента развития сервисов рабочего пространства «Вымпелкома» Роман Филатов. Он добавляет, что в случае «Вымпелкома» фокусом последних лет стало обеспечение бесперебойности работы не только точек продаж (то есть точек прямого взаимодействия с клиентом), но и обеспечение сопоставимого уровня в работе офисов компании по всей стране. К примеру, телеком-оператор с помощью своего технологического партнера («Т1 Сервионики») сумел прийти к тому, чтобы каждый новый сотрудник «Вымпелкома» получал полностью преднастроенное оборудование в свой первый же рабочий день, а для выполнения такой операции, как, скажем, подключение принтера, теперь требуется только телефон, на котором есть сканер QR-кода. Общее количество обращений на одного пользователя сократилось как минимум в два раза, более 70% инцидентов закрывается в течение четырех часов (для сравнения: в среднем этот показатель варьируется в зависимости от сложности инцидента от четырех-восьми часов до нескольких дней), а выполнение SLA по обращениям достигает 99,8%. Количество сбоев, выявленных автоматически, включая триггеры вероятности потенциальных проблем, увеличилось на 62%, в том числе за счет сочетания умных систем диагностики, напоминает Роман Филатов.

Постоянно растущая угроза кибератак, которую отмечают и ИБ-эксперты коммерческих компаний, и регуляторы, за последние годы практически сделала информационную безопасность обязательной частью любой ИТ-архитектуры. Компании переходят от точечной работы по устранению уязвимо-

стей к построению проактивных систем защиты. В совокупности это позволяет сегменту ИБ сохранить позитивную динамику роста по итогам 2025 года даже в условиях общего охлаждения ИТ-рынка, хотя и более умеренную, чем раньше. В ИТ-холдинге Т1, к примеру, отмечают, что по итогам года сегмент может вырасти на 6%, а вот в 2026-м — уже на 12%. Причем спрос будет смещаться в сторону сервисных моделей ИБ и управляемых услуг, добавляют они. Бизнес сегодня безусловно уделяет вопросу информационной безопасности много ресурсов и времени, и особенно в части защиты критической инфраструктуры и данных.

Страховые компании работают с огромнейшими массивами данных граждан, поэтому вопрос безопасности обрабатываемых данных для них максимально высок. Так, к примеру, «Росгосстрах» построил мощную систему обезличивания данных на базе отечественной платформы инструментов и сервисов управления и автоматизации цикла создания ПО «Сфера». Это позволило, с одной стороны, гарантировать безопасный доступ к базам данных для подрядных организаций в рамках разработки ИТ-систем страховой компании, а с другой — выполнить задачи импортозамещения. И если раньше ИТ-команда страховщика обезличивала данные с помощью самописных скриптов, то после внедрения централизованного решения она получила стабильный механизм, который сохраняет консистентность данных на всех интеграционных средах и позволяет повысить качество и скорость тестирования, поясняет директор департамента качества СК «Росгосстрах» Кирилл Золотухин. Он добавляет, что, используя обезличенные данные, компания также теперь может привлекать ИТ-подрядчиков для разработки с использованием этих данных.

Импортозамещение по-крупному

Безусловно, импортозамещение все еще остается одним из главных трендов рынка, и особенно это актуально для промышленных систем на объектах критической инфраструктуры, уверены в компании «Северсталь-инфоком». В решение этой задачи вовлечены как вендоры, так и сами игроки ключевых отраслей. В качестве примера руководитель управления внешних продаж «Северсталь-инфокома» Юрий Гушчин приводит комплексную ITSM-систему, построенную на базе платформы SimpleOne, которую в интересах «Северсталь-инфокома» разработали эксперты «Т1 Интеграции». Эта система смогла объединить все процессы взаимодействия с клиентами в «одном окне» и максимально упростить коммуникацию между клиентами, службой поддержки и разработчиками. «Новый инструмент обеспечил цифровую поддержку внешних клиентов, приобретающих программные продукты компании, и стал ключевым элементом в развитии клиентского сервиса. Сотрудники службы поддержки при этом получили инструменты для мониторинга SLA и оперативного взаимодействия с командами разработки», — добавляет господин Гушчин.

Решения по импортозамещению необходимы предприятиям всех отраслей, значимых для отечественной экономики. Например, крупнейший российский электроэнергетический холдинг «РусГидро» запустил глобальный проект по переходу компании с SAP на отечественную платформу 1C, обеспечивающую автоматизацию финансово-



экономического управления холдинга. «Мы долго готовились к этому проекту и вошли в активную фазу реализации полтора года назад. ИТ-холдинг Т1 тогда победил в открытом конкурсе, и подчеркну, что в таких сложных проектах крайне важно иметь надежного партнера», — замечает директор департамента информационных технологий и цифрового развития компании Сергей Хомяков. В рамках проекта система ERP будет заменена по основным модулям: бюджетирование, казначейство, РСБУ, налоговый и складской учет, поясняют в «РусГидро». Проект охватывает в совокупности более десятка функциональных и технологических областей, а также отличается сложнейшей интеграцией с другими информационными системами.

Другой пример — из сферы транспорта. РЖД вместе с крупнейшим в России ИТ-холдингом реализует масштабную программу импортозамещения корпоративного хранилища данных, отражающего все аспекты деятельности транспортной компании. Уже сегодня сформирована доменная архитектура хранения данных, охватывающая основные бизнес-процессы 27 бизнес-доменов РЖД. На текущем этапе успешно выполнена миграция более 80 систем транспортной компании, что стало значимым шагом на пути к технологической независимости. Промежуточные результаты проекта уже дают эффект: руководству доступны более точные и актуальные данные для принятия стратегических решений, ускорилось внедрение автоматизированных аналитических решений, снизилась потребность в ручной подготовке критической статистической отчетности, а также оптимизировались затраты, связанные с введением методологии подготовки данных. Работа над хранилищем продолжается — впереди следующие этапы масштабирования и развития платформы, которые позволят раскрыть весь потенциал новой архитектуры данных.

Облачный подход с осязаемым эффектом

Вместе с тем опыт 2025 года показал, что продолжает расти и облачный рынок: для бизнеса облака становятся эффективным способом быстрее запускать продукты, снижать стоимость владения и соответствовать требованиям по защите данных. Так, по оценке ИТ-холдинга Т1, в 2025 году сегмент облачных сервисов вырастет на 29%, а в 2026 году — еще на 27%. Прежде всего это происходит за счет динамики востребованности гибридных моделей, PaaS-сервисов и увеличения GPU-нагрузок.

Так, Альфа-банк при поддержке «Т1 Облако» построил гибридную облачную инфраструктуру на базе графических ускорителей (GPU). Это решение позволило банку быстро тестировать и развивать собственные технологии генеративного искусственного интеллекта, необходимые для повышения эффективности внутренних процессов и качества клиентского сервиса банка. Инфраструктура стала основой для внутренней ИИ-платформы AlfaGen, которая объединяет различные инструменты для сотрудников: от ассистента разработчика до ИИ-агентов для аналитики и тестирования. Благодаря реализованной гибридной инфраструктуре, банк получил не просто увеличенные мощности, а гибкий, безопасный и масштабируемый полигон для быстрого прототипирования и внедрения новых ИИ-сервисов, замечает руководитель департамента сопровождения информационных технологий Альфа-банка Александр Трикоз. «Это напрямую влияет на наши операционную эффективность и качество клиентского опыта, позволяя выводить сервисы на новый уровень», — добавляет он.

Перспективы: сохранить свою долю рынка и сделать ИИ стандартом

С учетом повышения зрелости многих отечественных ИТ-решений и их успешной обкатанности на сложных, территориально распределенных и высоконагруженных инфраструктурах российских компаний становится вполне ожидаемым изменение роли российских технологий в контексте экспорта. Уже сейчас отечественные компании начали получать реальные доходы от поставок ИТ-решений за рубеж, замечают в ИТ-холдинге Т1.

Говоря о перспективах развития рынка, многие участники отрасли сходятся во мнении, что его главным драйвером продолжит оставаться сегмент ПО и ИТ-сервисов. Именно он будет определять направление развития отрасли в ближайшие годы. «Спрос при этом формируется за счет прикладного программного обеспечения, облачных сервисов и инструментов кибербезопасности», — считают в ИТ-холдинге Т1. Эти тренды создают для российской экономики важный эффект: ускоряют цифровизацию отраслей, помогают бизнесу снижать издержки, повышать производительность и адаптироваться к новым условиям. При этом на рынке до сих пор сохраняется нехватка зрелых российских решений в отдельных сегментах, ограниченность кадров и необходимость ускорять выход оте-

чественных продуктов из пилотных стадий в промышленную эксплуатацию.

С этим соглашается Сергей Хомяков: «В ближайшие два-три года компании сосредоточатся на доработке уже выведенных на рынок продуктов. Их уровень качества должен позволить конкурировать в первую очередь на внутреннем рынке, а в случае возвращения в Россию иностранных компаний — не дать пользователям почувствовать необходимость возвращаться на иностранное ПО».

«Централизованные решения в области кибербезопасности будут активнее внедрять элементы с использованием искусственного интеллекта», — расставляет будущие акценты в сфере информационной безопасности Кирилл Золотухин. Значительные усилия производителей решений будут направлены на повышение скорости обработки данных, так как сейчас разовое обезличивание высоких объемов может требовать слишком длительного времени или чрезмерно высокой мощности от сервера, добавляет он.

Еще один тренд связан с гиперконкуренцией на рынке ПО, отмечают в Т1. «Лидеры рынка расширяют линейки, объединяют сервисы вокруг крупных экосистем, и борьба смещается в плоскость комплексности, возможности быстрой интеграции и масштабирования», — говорят в компании, выделяя усиливающуюся роль технологических партнерств.

Наконец, искусственный интеллект как технологический сегмент, во-первых, растет практически в два раза быстрее относительно остальных рынков ИТ-отрасли. В ИТ-холдинге Т1 отмечают, что компании активно автоматизируют обслуживание клиентов, производство, анализ данных и поиск знаний, и в 2025 году рынок ИИ увеличится на 12%, а в 2026 году — на 16%.

Во-вторых, технология ИИ сегодня проходит активную трансформацию из экспериментального инструмента в промышленный. Компании все активнее вводят управляемые ИИ-сервисы, включают модели в корпоративные решения и переходят от пилотных проектов к тиражируемым практикам. Ценность ИИ сегодня измеряется уже не точностью расчетов, а тем, сколько раз он помог человеку сохранить спокойствие, время и достоинство — свое и клиента, говорит Роман Филатов. «Мы идем шаг за шагом: сначала — для самых частых и простых ситуаций, с участием самих сотрудников в настройке. Только так ИИ становится частью команды, а не ее наблюдателем», — заключает эксперт.

Василиса Аксенова

+ | T1 | ИТ-холдинг

Наши ИТ летают

Разработка ПО Консалтинг Производство оборудования
Облачные сервисы Решения на базе ИИ Сервисная поддержка
Системная интеграция Информационная безопасность

Бигтех* для бизнеса

t1.ru

0+

РЕКЛАМА
АО "Т1" ИНН 9714075174

Бигтех (bigtech — перевод с англ. яз.) — крупные технологические компании

Изображенные части кода являются фантазийными и представляют набор символов, не имеющих отношения к реальным программным кодам или алгоритмам.

информационные технологии

Интеллектуальное внедрение

Эксперты прогнозируют рост рынка больших данных и искусственного интеллекта двузначными темпами в ближайшие несколько лет. Компании и госучреждения уже активно внедряют технологию, однако остаются серьезные проблемы, в частности отсутствие понимания реальной области применения и в связи с этим низкая эффективность работы. Вместе с тем, по словам экспертов, на рынке есть экспертиза, позволяющая преодолеть эти трудности.

— развитие искусственного интеллекта —

ИИ грянул рост

По итогам 2024 года российский рынок Big Data и искусственного интеллекта (ИИ) достиг 433 млрд руб., следует из исследования Ассоциации больших данных (объединяет «Сбер», «Яндекс», VK и др.), консалтинговой компании B1 и TAdviser. Вместе с тем по итогам 2025 года объем рынка может показать рост на 20%, до 520 млрд руб., и сохранить аналогичные темпы в ближайшие пять лет (см. «Б» от 13 ноября).

В деньгах объем рынка растет во всех отраслях экономики, в том числе в производственных, а не только в сфере услуг и финансах, хотя они остаются драйверами роста и нагрузки на аппаратные мощности, уточняет гендиректор облачного провайдера Nubes Василий Степаненко. В частности, по нашим опросам, более 80% финтех-компаний хотя бы раз применяли ИИ в своей деятельности, отмечает советник гендиректора ассоциации «ФинТех» по ИИ Алексей Сидорук.

Финансовый сектор, по словам господин Степаненко, чаще всего использует ИИ для обслуживания клиентов (чат-боты и виртуальные ассистенты), обнаружения мошеннических действий и персонализации предложений. В логистике и транспорте ИИ помогает оптимизировать маршруты, прогнозировать спрос и управление запасами, автоматизировать складские операции, в медицине — анализировать медицинские изображения, разрабатывать лекарства и планы лечения, а также справляться с рутинными задачами, продолжает он. В образовании с его помощью автоматически проверяют работы и подготавливают учебные материалы, персонализируют обучение, отвечают на вопросы студентов (чат-боты), указывает эксперт.

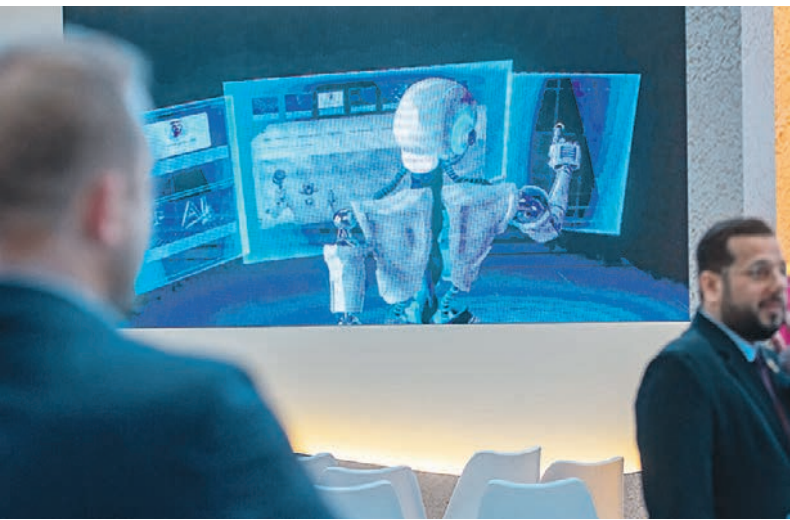
Кроме того, внедрение ИИ в госсекторе стимулирует законодательство, убеждены в ИТ-холдинге T1. Указ президента «О развитии искусственного интеллекта в Российской Федерации», подходы Минцифры России, а также основные направ-

Кроме того, по словам руководителя направления ИИ в ИТ-холдинге T1 Сергея Голицына, технологии искусственного интеллекта активно внедряются в государственное управление. Сектор использует ИИ для обработки обращений граждан, документооборота, прогнозирования поручений, а также мониторинга публикаций и социальных сетей, его возможности применяются в системах «умный город», говорит Василий Степаненко.

Для бизнеса основным драйвером использования ИИ является повышение эффективности. Технология позволяет ускорить и оптимизировать ряд рутинных операций, в том числе требующих принятия стандартизованных или типизированных решений, которые достаточно просто выводятся с изначальными условиями, поясняет MBA-профессор бизнес-практики по цифровым финансам РАНХиГС Алексей Войлуков. В конечном итоге они позволяют снижать затраты и повышать прибыль при правильном использовании, подтверждает партнер B1 Мария Егорова.

В госсекторе цели применения ИИ — не только оптимизация процессов, но и повышение прозрачности и эффективности принятия решений, уверен господин Голицын. Технологии ИИ позволяют перейти от традиционной бюрократии к управлению на основе данных, что особенно важно для органов власти, работающих с огромными объемами документов и информации, а также в контексте принципов «государство для людей», поясняет он.

Кроме того, внедрение ИИ в госсекторе стимулирует законодательство, убеждены в ИТ-холдинге T1. Указ президента «О развитии искусственного интеллекта в Российской Федерации», подходы Минцифры России, а также основные направ-



ЕВГЕНИЙ ШМЕЛОВ

ления внедрения генеративного ИИ в органы власти включают требования по созданию структуры данных, использование ИИ в анализе и подтверждении достоверности информации, работе с документами, генерацию и обработку контента официальных публичных ресурсов, первичный анализ резюме и данных кандидатов, генерацию текстовых заданий для подбора и развития сотрудников. Однако использование генеративного ИИ может быть запрещено для прогнозирования социально-экономических процессов и обработки сведений, составляющих государственную тайну, следует из проекта постановления правительства «О проведении эксперимента по использованию генеративного искусственного интеллекта в государственном управлении».

Нечеловеческие проблемы

При этом главное — чтобы внедряемые ИИ-технологии давали реальный эффект и фактически использовались при работе, считает спонсор Егорова. В современном бизнесе искусственный интеллект стал крайней популярной темой, и многие компании стремятся внедрить его повсеместно, зачастую не до конца понимая реальную область его применения, поэтому возникает проблема корректного определения сценариев, где ИИ действительно будет полезен, необходим и экономически эффективен, говорит господин Войлуков. В госсекторе «слепое» применение технологий не решает проблемы госслужбы, а даже может стать дополнительной нагрузкой — сотрудникам приходится перепровер-

ять материалы, подготовленные системами с использованием ИИ, переносить их в требуемые шаблоны, продолжает Сергей Голицын.

При этом, по словам господина Войлукова, критически важно грамотно подбирать алгоритмы, качественно проводить их обучение, а также выстраивать систему постоянного контроля за процессом самообучения модели — в частности, необходимо предусмотреть механизмы отката к предыдущим версиям и процедуры разрешения спорных ситуаций — все это требует значительных экспертных знаний и квалифицированного персонала.

Эффективное внедрение

По словам Сергея Голицына, чтобы внедрять ИИ эффективно, необходимо учитывать управление данными. Внедрение ИИ следует начинать с него, определяя и управляя источниками этих данных, что позволяет обеспечивать актуальность и достоверность информации, используемой моделями ИИ. Применение платформенных решений для управления жизненным циклом обучения моделей позволит снизить стоимость создания и применения моделей, а также организовать их автообучение на основе актуальной информации в инфосистемах, добавляет он. Заключительным этапом, по его словам, является создание сервисов и приложений для автоматизации рабочих процессов, что повысит эффективность и сократит время на выполнение задач.

Господин Войлуков выделяет несколько факторов успеха. Необходимо в первую очередь проанализировать потребности текущих процессов и выявить области, где ИИ мо-

жет принести пользу, оценить ресурсы и возможности для внедрения, отмечает он.

На следующем этапе, как поясняют эксперты, следует перейти к формированию команды и стратегии, в частности собрать экспертов и аналитиков по ИИ, представителей различных отделов компании или ведомства. «На этом этапе важно описать рабочие процессы как есть и сформировать четкое видение, как и где будет применяться технология. Разработать стратегию внедрения ИИ, определить ключевые проекты и цели. Подготовить бюджет и распределить финансовые средства», — считает Сергей Голицын.

Только после этого компании и ведомства могут переходить к выбору технологий и инструментов для реализации ИИ-проектов и проводить тестирование выбранных решений на небольших масштабах, уверен собеседник «Б» на IT-рынке. Обучение персонала — тренинги и семинары для сотрудников о базовых принципах ИИ и его применениях — последний, но значимый этап внедрения, продолжает он.

Говоря о госсекторе, Сергей Голицын выделил несколько подходов по внедрению ИИ:

1. Переход от «среднего по больнице ИИ» к доверенному ИИ, дающему точный ответ в конкретной ситуации с учетом объективных данных и актуальной документации.
2. Постоянное обновление базы знаний. Обеспечение возможности оперативного пополнения информационной базы ИИ актуальными документами и свежими данными для поддержания релевантности ответов.
3. Внедрение ИИ в рабочие процессы с документацией. Сотрудник госоргана должен получать на согласование и реализацию ответ или документ, а гражданин — достоверный ответ оперативно и в момент актуальности проблемы. ИИ в этом контексте способен «читать» (обрабатывать и анализировать) большие объемы документов. Например, почитать проект НПА, сверить его со всеми существующими документами, сформировать визуальную карту связей на основе графовой модели и замечания к проекту НПА, а также сгенерировать его обновленный вариант.
4. Автоматизация процессов коммуникации, в том числе коммуникация с гражданами, должна быть работой ИИ.
5. Аналитика данных. Модели ИИ анализируют данные и предлагают

рекомендации, основанные на актуальной информации, что повышает качество принятия решений и снижает вероятность ошибок. Например, системы поддержки принятия решений могут анализировать большие объемы данных о состоянии объектов ЖКХ и предлагать оптимальные планы ремонта и модернизации.

6. Оценка качества и результативности в ежедневной работе сотрудника ведомства.

7. Проведение специализированных тренингов и семинаров поможет сотрудникам освоить новые технологии и использовать их максимально эффективно, что снижает риск недостоверной информации и ошибок.

8. Поддержка, а не замена. Технологии искусственного интеллекта эффективны в циклических процессах, рутинных задачах и анализе больших объемов данных.

По словам экспертов, для того, чтобы максимально результативно внедрить ИИ, компаниям и госучреждениям необходимо обращаться за помощью к специалистам. «Разработка решений на базе технологий ИИ, как правило, требует совместной работы нескольких специалистов разного профиля. В первую очередь это IT-специалисты (собственные или IT-компания) с навыками работы именно с технологиями ИИ. Могут потребоваться «обычные» IT-специалисты для интеграции ИИ-решений с другими системами. Также, как в любых IT-проектах, нужна помощь аналитиков», — поясняет Мария Егорова.

Вместе с тем на российском рынке есть решения, которые способствуют автоматизации и оптимизации процессов в бизнесе и госуправлении. В частности, российские компании предлагают решения для работы с документами, которые анализируют объемы входящих материалов и генерируют уточненные документы, а также технологии, автоматизирующие создание, применение и дообучение ИИ, отмечает господин Войлуков.

Ключевым фактором успеха остается наличие экспертов-специалистов и партнеров, обладающих глубоким пониманием предметной области и готовностью принимать обоснованные риски — именно они способны сделать правильный выбор доступной технологии, уверен эксперт.

Ева Фролова

Как найти свои данные быстрее хакеров

— кибербезопасность —

Современная IT-инфраструктура бизнеса перестала быть статичной. Данные рассредоточены по гибридным средам, включая российские облака, локальные дата-центры, SaaS-сервисы, среды разработки и даже личные устройства сотрудников. Резервные копии и архивы создают дополнительные сложности. Этот динамичный ландшафт делает задачу защиты информации привычными инструментами невыполнимой. Эксперты рынка кибербезопасности рассказали «Б-Информационным технологиям», какие «слепые зоны» создает текущий подход и как меняется философия защиты данных.

Почему карта данных устаревает быстрее, чем составляется

Главная сложность — фрагментация и постоянная миграция информации. «Данные перестали быть статичными и локализованными. Они одновременно находятся в локальном дата-центре, в российском публичном или частном облаке, а также в SaaS-сервисах», — отмечает управляющий партнер ITD Group Ксения Калемберг. Проблема усугубляется среды разработки (DevOps/Data Science), где для тестирования и обучения моделей ИИ создаются временные инстансы с критичными данными, часто выпадающие из поля зрения службы ИБ, поясняет она. По словам руководителя команды киберзащиты облачного провайдера Nubes Дмитрия Шкурюпата, составить актуальную карту вручную практически невозможно из-за масштаба и скорости изменений. «Ключевая проблема — отсутствие единого, автоматизированного механизма обнаружения и классификации, который работал бы одинаково во всех этих разнородных средах», — утверждает он.

Заместитель генерального директора по инновационной деятельности «СерийИнформ» Алексей Парфентьев, выделяет две отдельные задачи: аудит статичных данных и контроль за их перемещением. По его словам, не все системы, особенно облачные и прикладные, имеют инструменты для интеграции со специализированными инструментами аудита. DLP-системы, в свою очередь, не всегда полноценно контролируют «нетиловые» каналы передачи, оставляя пробелы.



ИГОРЬ ИВАНОВ

Кошмар в «зоопарке»

Необходимость администрировать множество разрозненных инструментов — DLP, DAM, классификаторы, облачные средства защиты — создает значительные операционные сложности. «Каждая система использует свои форматы логов, собственную политику и подходы к фиксации событий. Специалистам приходится вручную сопоставлять результаты, следить за актуальностью политик и устранять конфликты», — описывает ситуацию господин Шкурюпат.

Главная боль, по мнению госпожи Калемберг, — неуправляемый рост «шума» и отсутствие единого контекста для реагирования. «DLP может сигнализировать о попытке передачи файла, DAM — о необычном запросе к базе, а классификатор — о наличии в документе номера паспорта. Но если эти события происходят в рамках одной сессии, разрозненные консоли не позволяют соединить их в картину целенаправленной атаки», — поясняет она.

Одной из ключевых трудностей также становится отсутствие единого центра управления, считает ведущий юрист продуктовой группы «Контур.Эгида» и Staffcor Ольга Попова. По ее словам, техническая несовместимость разнородных систем защиты, зачастую развернутых в одной инфраструктуре, вынуждает персонал дублировать данные и

выполнять множество ручных операций для их обработки и сопоставления. Как она отмечает, это не только увеличивает операционную нагрузку, но и создает вторичные риски для самих данных, которыми приходится манипулировать вне защищенных автоматизированных контуров.

Старший менеджер практики кибербезопасности «ТеДо» Антон Мерцалов называет фрагментацию политик основной операционной сложностью: «Каждую систему защиты приходится настраивать отдельно, вручную дублируя правила».

«Несо согласованные политики приводят к ошибкам, конфликтам и пробелам в защите», — говорит он. Владимир Ульянов из Zecurion также отмечает, что синхронизация работы разных классов продуктов требует большого объема «ручной» работы и чревата ошибками.

Розеттский камень

Когда инцидент уже произошел, необходимость вручную собирать информацию из нескольких систем становится критическим фактором. «Ручной сбор данных из независимых систем для расследования — это гарантированная потеря времени и критического контекста. Пока аналитик запрашивает логи, копирует данные и пытается синхронизировать временные метки, злоу-

мышленник может завершить атаку», — предупреждает господин Шкурюпат.

При этом эксперты «Кросс технолджис» предупреждают о дополнительном риске в процессе ликвидации последствий инцидента. По их оценке, в спешке или из-за неверных действий в таких ситуациях нередко происходит уничтожение цифровых артефактов и следов действий злоумышленников, которые критически важны для последующего расследования и могут быть использованы при взаимодействии с регуляторами. Поэтому, как подчеркивают в компании, наличие четкого, заранее отработанного плана реагирования, включающего мероприятия по сохранению доказательств, становится необходимым элементом защиты.

Много трудностей, по словам господина Мерцалова, создает резкое замедление расследования: данные приходится вручную собирать из DLP, систем аудита доступа, облачных логов, и они не совпадают по формату, времени и идентификаторам. Такое ручное сопоставление занимает часы, в течение которых злоумышленник может продолжить атаку.

Руководитель департамента развития и архитектуры «Кросс технолджис» Евгений Балк, обращает внимание на другую проблему: для расследования часто не хватает детальности логирования, а данные хранятся ограниченное время. «Мы действительно зачастую не знаем полной карты расположения чувствительных данных, множество корпоративных систем может хранить одни и те же данные, поэтому это затрудняет расследование утечек», — отмечает он.

«Слепые зоны»

По мнению экспертов, даже при наличии широкого набора решений в гибридных и облачных средах остаются плохо контролируемые участки. «Типичные слепые зоны — облачные SaaS, теневые сервисы, админские «обходные тропы», сервисные учетки, а также копии данных в дев/тест-средах и бэкапах. Все, что возникает вне формализованного процесса управления доступом, фактически выпадает из контроля», — отмечает эксперт компании «Газинформсервис» Александр Давыдов.

Антон Мерцалов относит к основным «слепым зонам» неструктурированные данные в NAS, объектных хранилищах, почте и мессенджерах, а также данные в транзите между различными сервисами в микросервисной

архитектуре. Ксения Калемберг из ITD Group добавляет, что критичной остается зона Data Pipeline — точки взаимодействия микросервисов разных провайдеров, которые часто слабо защищены и плохо логируются.

В таких условиях на первый план выходит не добавление новых «датчиков», а создание единой системы координации для данных. Накопленные операционные сложности и «слепые зоны» напрямую влияют на ключевые бизнес-показатели: время реакции на инциденты, стоимость владения безопасностью и способность выполнять регуляторные требования. «Сегодня компании тратят все больше на безопасность, однако инвестиции часто направляются на защиту отдельных частей инфраструктуры, а не самих данных», — объясняет Виктор Рязжков, руководитель развития бизнеса по защите данных в Positive Technologies (PT). При этом в компании добавляют, что инфраструктура усложняется, а объем данных растет. В результате традиционные инструменты, закрывающие только отдельные точки, не дают целостной и актуальной картины, оставляя в инфраструктуре множество «слепых зон» — и зачастую именно там и происходит утечки.

По словам Виктора Рязжкова, ответом на эти системные вызовы стал платформенный подход Data Security Platform (DSP), который Positive Technologies развивает в своем продукте PT Data Security. Точечные решения работают как «датчики» на отдельных участках: DLP — на конечных устройствах, DСАР — на файловых хранилищах, и каждый видит только свой кусок. «Наша платформа соединяет все воедино — ей не принципиально, хранятся данные в виде файлов, таблиц в базах или на внутренних порталах. Для всех типов — единый подход», — поясняет в PT. При этом PT Data Security проактивно ищет новые хранилища, подстраиваясь под динамику изменений, а не ждет, пока оператор подключит очередной источник. Это позволяет выявлять и закрывать те самые «слепые зоны».

В итоге эффективная защита данных перестает быть вопросом выбора лучшего точечного инструмента. Она требует принципиально иного — платформенного — взгляда, способного превратить хаотичный цифровой ландшафт в управляемую и безопасную среду. Без этого перехода компания обречена на нег впереди угроз, теряя контроль над своей главной цифровой ценностью.

Максим Гуляев