информационное агентство | information agency

Информационная услуга

«Тематические новости»

"Проекты в области цифровизации РФ"

Демонстрационный выпуск

Периодичность: еженедельно

-

Содержание выпуска

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Влияние кризиса на отрасль

Имущество Google во Франции арестовали по заявлению российской "дочки".

Парижский суд вынес приказ об аресте 100% акций компании Google France в связи с предстоящим рассмотрением заявления российской "дочки" Google (ООО "Гугл") к материнской компании Google International LLC, сообщил РБК партнер адвокатского бюро Art De Lex Артур Зурабян, представляющий интересы конкурсного управляющего ООО "Гугл".

Арест наложен в качестве обеспечительной меры, чтобы предотвратить возможные попытки Google инициировать банкротство своей французской "дочки". Основанием стала необходимость обеспечения исполнения решения Арбитражного суда Москвы по делу о банкротстве ООО "Гугл". Google France и Google International LLC могут обжаловать наложенный арест в суде.

В июле 2024 года конкурсный управляющий ООО "Гугл" Валерий Таляровский обратился в Арбитражный суд Москвы с просьбой признать недействительной сделку по выплате дивидендов в пользу Google International. Суд поддержал позицию истца, признав, что выплата была совершена намеренно в целях уклонения от погашения задолженности перед кредиторами. Сумма дивидендов составила €112 млн, что эквивалентно 10 млрд руб.

Зурабян напомнил, что помимо дивидендов в деле о банкротстве ООО "Гугл" также оспаривается вывод денежных средств из России после 2018 года на общую сумму свыше 140 млрд руб. Поскольку в России у Google активов нет, российские решения будут предъявляться к исполнению в иностранных юрисдикциях.

Следующим этапом, по словам Зурабяна, станет рассмотрение судом Парижа заявления ООО "Гугл" по существу. В случае удовлетворения заявления российской "дочки" на арестованное имущество будет обращено взыскание, а средства пойдут на удовлетворение требований российских кредиторов.

Google France — единственный акционер Google International LLC. Компания отвечает за продажу и перепродажу рекламных услуг американской корпорации в Европе. По итогам 2024 года выручка Google France внутри страны составила €1,31 млрд, а экспорт — €434,7 млн.

РБК направил запрос в суд, а также в пресс-службу Google France.

Это не первый арест имущества Google в поддержку исполнения решения российского арбитража. В мае 2025 года аналогичное решение принял Верховный суд Южно-Африканской Республики, арестовав имущество Google LLC на территории страны. В целом российская "дочка" добивается признания решений о взыскании средств с материнской компании более чем в десятке зарубежных юрисдикций.

Для справки: Название компании: *Гугл, ООО (Google)* Адрес: *115035, Россия, Москва, ул. Балчуг, 7* Телефоны: *+7(495)7800022; +7(495)6441400; +7(800)1004664* E-Mail: *press@google.com* Web: *www.google.ru; https://about.google/intl/ru/* Руководитель: *Сальваторе Мариа Дасаро Биондо Карло, генеральный директор* (РосБизнесКонсалтинг 11.12.25)

К СОДЕРЖАНИЮ

"Законодательство в области цифровой экономики отчетливо ужесточается". "КоммерсантЪ". 10 декабря 2025

Льготы — разработчикам, рестрикции — коду: как государство выстраивает IT-регулирование в текущих условиях

Власти продолжают ужесточать требования к софту для госзакупок, одновременно расширяя поддержку IT-отрасли через аккредитацию и налоговые льготы. Ключевым становится вектор на технологический суверенитет: видеоиграм на зарубежных движках сделали исключение для реестра отечественного ПО, а open source решения столкнулись с запретом на преференции, если их обновления идут из-за рубежа. О том, как бизнесу работать в условиях новых правил для данных, криптовалют и платформенной экономики, рассказал управляющий партнер юридической компании ЭБР Александр Журавлев.

— В последние годы мы наблюдаем, что в правовом поле появляется все больше новых законопроектов в IT-сфере. Какие нормы, принятые в отрасли за последние годы, вы считаете ключевыми?

— Знаковым я назвал бы 2022 год, ознаменовавшийся принятием указов президента о стимулировании IT-отрасли: эти документы стали основанием для новых положений, которые позволили разработчикам сфокусироваться на создании критической информационной инфраструктуры для государства, и дали значительный импульс для их развития в сложный период.

Даже разработчики видеоигр получили специальный порядок и могут пользоваться указанными льготами, включая свои продукты в реестр отечественного софта. Льготы дали не только налоговые преференции — например, принятое положение об аккредитации IT-компаний дало право на отсрочки от призыва и ипотеку. Эти меры, стимулируя и развивая спрос на отечественное ПО и программно-аппаратные комплексы, позволили стабилизировать рынок.

Особое место отведено обороту данных: принят национальный проект "Экономика данных и цифровая трансформация", и власти ищут баланс между защитой личности и развитием технологий. С одной стороны, в этом году вступили в силу изменения, которые существенно усилили защиту персональных данных граждан, а также ответственность за их оборот. С другой стороны, идет работа над безопасным использованием разных видов данных для машинного обучения ИИ и отдельными нормами, которые будут регулировать разные явления, связанные с этой технологией.

В целях обеспечения безопасности информации о рынках и потребителях проведена реформа исследовательских компаний. Она направлена на усиление контроля над иностранными игроками и защиту данных: с марта 2026 года для компаний с долей иностранного капитала свыше 20% будет действовать запрет на проведение товарных и потребительских исследований, обработку данных внутри РФ. В ближайшее время к этому закону примут подзаконные акты, и российские игроки должны будут соответствовать ему для продолжения деятельности.

Заработали экспериментально-правовые режимы для тестирования различных видов технологий, позволяющие опробовать их и формировать новое регулирование в ходе эксперимента. Благодаря этому мы наблюдаем на городских улицах, дорожных трассах, полях и реках работу разнообразных видов беспилотного транспорта; уже сейчас ваш заказ могут доставить роботизированные курьеры.

Значимым стало и внесение в ГК РФ изменений, касающихся цифровых валют и принятия специального регулирования этой отрасли: санкции дали ему второе дыхание для использования в расчетах в ВЭД.

Государство также проявляет большой интерес к обороту информации и контента — так, недавно принято регулирование рекомендательных алгоритмов, использующихся в социальных сетях и электронной коммерции. В отношении компьютерных игр, ставших элементом культуры и средством передачи смыслов и которыми государство тоже активно интересуется, обсуждается новый закон, регулирующий их разработку, издание и маркировку. Отрасль становится зрелой и сознательной — к примеру, наши разработчики до принятия закона самостоятельно начали эксперимент по контентной маркировке, механизм которой схож с контентной маркировкой PEGI ("Общеевропейская информация об играх", система рейтинга контента видеоигр, используемая в Великобритании, Европе и на Ближнем Востоке).

На рынке интернет-рекламы проведена реформа: приняты критерии для определения рекламы в сети, установлен порядок ее учета и маркировки, введен специальный сбор в размере 3% и порядок его исчисления.

— Вы участвовали в разработке "налогового маневра", вступившего в силу в 2021 году. Насколько высоко вы оцениваете эффективность налоговых льгот до текущего года?

— Действовавшие ранее налоговые льготы стали ключевым фактором устойчивости отрасли. Сначала снижение ставки налога на прибыль до 3%, а затем и до 0% позволило компаниям реинвестировать средства в разработку, и такая финансовая "подушка безопасности" дала им возможность экспериментировать и быстро адаптировать продукты — а в 2022 году это оказалось критически важным. Да, многие зарубежные вендоры ушли с рынка, но их уход не привел к его коллапсу, поскольку наши компании сумели оперативно предложить замену их решениям.

Недавние налоговые реформы, по сути, адаптируют льготы к новым реалиям. Дело в том, что раньше компании могли получать льготы по профильному ОКВЭД, что давало почву для злоупотреблений. Теперь аккредитация стала строже: государство хочет точечно поддерживать тех, кто реально создает и развивает софт, при этом для таких сфер, как EdTech, сделаны разумные исключения. Повышение ставки налога на прибыль с 0% до 5% и социальных платежей с 7,6% до 15% в этом контексте выглядит умеренным шагом, особенно на фоне значительно более высоких ставок в других отраслях. Необходимо понимать, что льготы — это выпадающие доходы бюджета и их пересмотр является вопросом баланса. Показательно, что последующие налоговые реформы в сравнении со многими отраслями практически не затронули эти льготы.

Вместо роста прямых налогов Минцифры в 2026 году будет использовать альтернативные механизмы. Одна из новелл — направить часть сэкономленных на льготах средств IT-компаний на подготовку кадров через систему целевых инвестиций в образование. Такой подход может стать компенсационным механизмом, который одновременно поддержит бюджет и подтвердит ответственность отрасли за развитие собственного кадрового потенциала.

— Можете привести примеры законодательных инициатив, которые обсуждались и были сбалансированы для IT-отрасли в части налогообложения?

— В части налогов мы вместе с коллегами из АПКИТ, АРПП "Отечественный софт" и Минцифры в конце 2024 года столкнулись с интересным кейсом, выявив правовую коллизию в новой норме Налогового кодекса, касающейся льгот для разработчиков программного обеспечения. Первоначальная цель законодателей — стимулировать льготами развитие именно отечественных IT-компаний — верна и поддерживается отраслью. Но в процессе внесения изменений была принята формулировка, которая может лишать права на льготу те компании, в структуре которых присутствует иностранное участие. На практике это означает, что под ограничение могут подпасть российские IT-компании, имеющие зарубежные R&D-центры или привлекающие иностранных разработчиков. Если созданный таким подразделением или специалистом программный модуль передается российской компании-правопреемнику, затраты на его разработку или доходы от его реализации рискуют не попасть под льготное налогообложение. Таким образом, буквальное прочтение нормы может противоречить ее

цели, создавая дополнительные барьеры для российских компаний с международной структурой разработки, а не стимулируя их рост.

Была и другая проблемная ситуация: если российский разработчик открывал за рубежом компанию совместно с иностранным партнером, это могло лишить всю группу права на налоговые льготы в РФ. Под угрозой оказались крупные отечественные игроки, которые активно выходят на международные рынки. В результате диалога с Минфином норму удалось скорректировать. Мы с коллегами предложили использовать подход, аналогичный правилам о контролируемых иностранных компаниях (КИК): если конечный контроль над иностранной структурой сохраняет российский гражданин, то делается исключение — и тогда подпавшие под него компании могут использовать ПО, разработанное их подразделениями из других стран, а также открывать офисы в иностранных юрисдикциях без риска потери льгот. Таким образом, была найдена балансирующая формулировка, которая защищает интересы российского IT-бизнеса при его развитии за границей, не противореча основной цели льгот — поддержке отечественных разработчиков.

— Сообщество разработчиков демонстрирует беспокойство насчет регулирования open source. Существуют ли сейчас законодательные ограничения на использование иностранного open source?

— Open source — важный инструмент, который позволяет небольшим, средним и даже крупным разработчикам улучшать или создавать свои продукты, используя готовые решения на основе "открытых лицензий". Как такового запрета на использование open source нет, но есть запрет на включение отдельных решений в реестр отечественного ПО. Соответственно, к технологическому стеку для госзакупок установлены повышенные требования в части безопасности. Одно из требований гласит: для того чтобы продукт не получал из-за рубежа обновлений, способных иметь скрытый функционал, в рамках лицензии также должны отсутствовать запреты на работу продукта на какой-либо территории РФ — например, Крыма или ДНР. Мировое сообщество обсуждает риски использования open source довольно активно: недавно Linux исключило 11 российских контрибьюторов из проекта по разработке ядра системы, что заставило рынок задуматься, как дальше обеспечивать безопасность работы таких продуктов. Но для коммерческих целей и без использования в государственном или финансовом секторе требования к open source довольно лояльны.

— Какие изменения вы могли бы выделить в части регулирования контента и его авторов в РФ?

— Контент — это значительная часть цифровой среды, и, действительно, такого регулирования немало: закон "Об информации", подзаконные акты Роскомнадзора, КоАП и прочее. Приняты специальные ОКВЭД для блогеров, которые могут идентифицировать их как отдельных участников предпринимательской деятельности. Для части авторов с аудиторией свыше 10 тыс. подписчиков введена процедура регистрации в реестре Роскомнадзора. Принят строгий запрет на рекламу на запрещенных интернет-ресурсах, а также усилена ответственность за его нарушение. Планируется введение маркировки контента, который сгенерирован при помощи нейросетей. Поскольку эта часть индустрии может оказывать воздействие на поведение людей, то сейчас и в будущем регуляторы будут уделять ей особое внимания.

— К каким правовым вызовам с учетом темпов разработки нового регулирования компаниям стоит готовиться в 2026 году?

— Важно подготовиться к грядущим налоговым изменениям: отсутствие моратория на налоговые проверки подталкивает задуматься о более тщательном администрировании налогов с учетом новой реформы. Если компания занимается новыми медиа и социальными сетями, ей следует быть готовой к новым поправкам закона "Об информации" — как в части рекомендательных алгоритмов, так и в части удаления противоправного контента, интернет-рекламы и идентификации пользователей. На рынке рекламы в следующем году, вероятно, пройдет реформа рекламного законодательства по аналогии с исследовательскими компаниями — в первую очередь это коснется иностранного контроля за такими агентствами.

Всем участникам электронной коммерции следует готовиться к тому, что в 2026 году будут приняты подзаконные акты к закону "О платформенной экономике", которые сейчас активно обсуждаются на разных уровнях. Они касаются многих аспектов: начиная от отношений операторов цифровых посреднических платформ с продавцами и заканчивая необходимостью более жесткого регулирования в части защиты интеллектуальной собственности и интересов правообладателей.

Указанные изменения не являются исчерпывающими. Объем и скорость законодательных и правоприменительных актов требуют от бизнеса системной и периодической ревизии разных процессов с помощью внешних и внутренних специалистов, чтобы убедиться в отсутствии рисков. Сегодня в мире формируется новое направление — выстраивание цифровых границ. Каждое государство стремится очертить свою юрисдикцию в онлайн-пространстве: контролировать, кто и как оперирует данными, какие сервисы работают с гражданами, каким образом обеспечивается цифровой суверенитет. Общая тенденция такова: цифровое пространство больше не воспринимается как нечто абстрактное и глобальное — это зона прямой ответственности государства, в которой действуют свои правила, механизмы защиты и модели регулирования. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

Программное решение. "КоммерсантЪ". 12 декабря 2025

Что значит вердикт суда о взыскании долгов с бывших клиентов SAP

Суд разрешил взыскивать деньги с бывших клиентов SAP. Речь об одном из крупнейших мировых разработчиков программного обеспечения для бизнеса, который покинул российский рынок в 2022-м. При этом часть клиентов так и не оплатили ранее купленный софт. Среди них, например, футбольный клуб "Зенит" и сеть магазинов "Окей". Общая сумма долга — около 2 млрд руб. Сначала задолженность взыскивала российская "дочка" — САП СНГ. Но вывести деньги компания не могла, поскольку расчеты с организациями из недружественных стран подпадают под ограничения. После этого САП СНГ продала весь долг российской юридической фирме "Легат" примерно за 60 млн руб., то есть всего за 3% от общей суммы.

Клиенты, задолжавшие деньги, посчитали такую сделку частью искусственной схемы, чтобы SAP все же получила средства. Но арбитражный суд нарушений не обнаружил. Впрочем, у заявителей еще есть шансы на победу в вышестоящей инстанции, отметил советник коллегии адвокатов Pen & Paper Роман Кузьмин: "Обычно иностранные правообладатели должны получать выплаты на специальные счета. По сути, они не смогут ими распоряжаться. В таких случаях зарубежные компании пробуют обойти требования указа президента, сделав уступку по российской структуре и получив по ней деньги. Дальше уже сама организация в РФ будет разбираться с должниками. В обычной практике суды эти уступки признают недействительными. Этот кейс нестандартен тем, что ее признали действительной, потому что решили, что нет никакого злоупотребления правом, нет цели обхода требования указа , что деньги по уступке уплачены не после того, как новый истец получит средства, а до. Кроме того, было принято во внимание то, что компания-должник не осуществляла никаких выплат, не открыла специальный счет и в принципе не предпринимала каких-то действий. То есть, по сути, в некотором смысле можно сказать, что должников наказали за то, что они пользуются этой ситуацией.

Пока уступку не оспорили, плату нужно осуществлять процессуальному правопреемнику, юридической компании "Легат". Она может инициировать судебное разбирательство, подать иски о взыскании. Но, скорее всего, они начнут вести претензионную работу. Я думаю, что должники не станут добровольно исполнять требования и дождутся окончания рассмотрения этого дела, надеясь на то, что сделку по уступке все-таки разрушат. В любом случае это вряд ли произойдет быстро, потому что для того, чтобы принудительно взыскать задолженность, компания "Легат" должна будет подать иск в арбитражный суд, потом обратиться к приставам, и только тогда уже могут начаться принудительные взыскания. Я думаю, что за это время решение по этому кейсу дойдет даже до Верховного суда, и у нас появится какая-то ясность".

Это дело действительно выбивается из общей практики по аналогичным спорам, и решение по нему может стать ориентиром при других разбирательствах, заметил адвокат коллегии "Клишин и партнеры" Александр Малахов: "У нас непрецедентное право, поэтому вступившие в законную силу судебные акты не дают оснований судам в последующих делах ими руководствоваться, однако и не исключают такой возможности. То есть если это решение вступит в силу, то есть в апелляции будет утверждено, а потом подтверждено вердиктом суда кассационной инстанции, то, безусловно, им в последующем могут руководствоваться. Но это не означает, что это будет происходить в обязательном порядке. Тем более если будет иметь место большее количество других судебных актов, судебных прецедентов. У нас это очень частая история, когда по одному и тому же вопросу есть разные позиции судов. Поэтому говорить, что это однозначно приведет к изменению практики, нельзя. Кроме того, данный кейс, вероятно, закончится в Верховном суде. И вот только после его мнения можно будет делать какие-то выводы".

Между тем порядка 40% российских холдингов продолжают использовать продукты SAP в 2025 году (КоммерсантЪ 12.12.25)

К СОДЕРЖАНИЮ

Есть ли жизнь после Microsoft? "IT Channel News". 15 декабря 2025

14 октября 2025 года завершилась расширенная поддержка целого ряда корпоративных продуктов Microsoft — почтовых, офисных, коммуникационных и серверных платформ версий 2016 и 2019. Эти решения остаются в инфраструктуре тысяч российских компаний, но больше не получают обновления безопасности, что значительно повышает риски эксплуатации уязвимостей и нарушений работы критически важных систем.

Завершение поддержки затронуло все ключевые сегменты корпоративной ИТ-среды: почтовые серверы, офисные пакеты, корпоративные порталы, системы управления проектами и платформы для видеоконференций. Для бизнеса это означает необходимость оперативно выстраивать стратегию перехода на отечественные продукты.

Эксперты ИТ-отрасли, участники АРПП "Отечественный софт", оценили готовность российских решений в разных классах ПО обеспечить совместимость, безопасность и устойчивую работу оставшихся без поддержки корпоративных систем.

Илья Массух, директор Центра компетенций по импортозамещению в сфере ИКТ, утверждает, что переход от продуктов Microsoft требует системного подхода: "Если говорить о Microsoft, то в первую очередь они были монополистами на нашем рынке и до 2022 года были псевдобесплатными — то есть либо предоставлялись в рамках OEM-лицензий, либо предоставляли скидки на бандлы майкрософтовских продуктов, так что определить стоимость

отдельного продукта было невозможно. Системные меры по переходу на российские продукты зависят от модели взаимодействия бизнеса с заказчиком". Эксперт поясняет, что для госсектора и компаний с госучастием ключевыми мерами могут стать субсидирование перехода и консолидация потребностей для централизованных закупок. В B2C массовый переход возможен через налоговые вычеты и регулирование рынка, включая обязательную предустановку.

Рената Абдулина, председатель Ассоциации КП ПОО, отмечает, что долгие годы сила Microsoft заключалась в единой экосистеме, где все продукты были взаимосвязаны. "В начале импортозамещения выяснилось, что ни один из отечественных разработчиков на тот момент не предлагал столь же целостного решения. В итоге крупным компаниям пришлось переходить на „зоопарк решений" и оперативно обеспечивать их совместимость в формате постоянного взаимодействия с вендорами". Сегодня ситуация постепенно меняется: появились инструменты, которые упрощают миграцию, и на рынке уже представлены зрелые решения, пригодные для перехода. "Чтобы ускорить этот процесс, ПО должно достигнуть функциональной и коммерческой зрелости". Рената Абдулина добавляет, что сохранение действующих налоговых льгот станет важной мерой поддержки, позволяя удерживать стоимость продуктов и направлять ресурсы на дальнейшее развитие.

Операционные системы

Михаил Геллерман, директор управления операционных систем "Группы Астра", подчеркивает, что сегодня российское ПО выбирают не только государственные ведомства и корпоративные заказчики, но и частный бизнес. "Операционная система — это среда, в которой пользователь запускает различные приложения и операции. Совместимость ОС с ее инфраструктурным окружением — ключ к популярности и активному использованию продукта". По оценке спикера, одной из самых острых проблем для заказчиков по-прежнему остается запуск в среде Linux отраслевых программ, часто "самописных", без которых невозможно обеспечить работу специфических бизнес-процессов. "Переход на новую операционную систему требует тщательного планирования, но это не повод откладывать проект. Наиболее эффективный подход — начать с пилотного проекта. Можно выбрать небольшую часть инфраструктуры, обычно один серверный кластер или отдел, и провести оценку совместимости всех компонентов".

Алексей Смирнов, член правления АРПП "Отечественный софт", председатель совета директоров "Базальт СПО", обращает внимание, что при переходе на российские решения в первую очередь нужно проверять совместимость прикладных программ с системным софтом: ОС, СУБД и др. "Отдельный вопрос — это поддержка отечественных процессоров. Наши операционные системы их поддерживают, но требуется также обеспечивать совместимость прикладных программ. Большую работу в этом направлении ведет АРПП „Отечественный софт". У Ассоциации есть каталог совместимости со ссылками на Реестр отечественного ПО".

Говоря о миграции, эксперт отмечает необходимость плавного перехода, чтобы рабочие процессы не останавливались. "Там, где развернуты большие информационные системы, как правило, нужен переходный период, когда старые зарубежные и новые отечественные продукты работают одновременно", — поясняет Алексей Смирнов. Успешное внедрение требует высокой квалификации специалистов, и, если таких компетенций внутри компании нет, лучше привлекать интеграторов, уже накопивших значительный опыт импортозамещения.

По словам Рустама Рустамова, члена правления АРПП "Отечественный софт" заместителя генерального директора РЕД СОФТ, вопрос совместимости в российской ИТ-среде решается через технологическое партнерство и постоянное взаимодействие с участниками рынка — от тестирования и синхронизации развития решений до сопровождения внедрения и эксплуатации. "В реальных условиях полный переход на отечественные решения невозможен сразу. Некоторое время придется существовать в гетерогенной ИТ-инфраструктуре, где совместно используется иностранное и российское ПО. Поэтому при выборе решений для миграции важно учитывать возможность работы в гетерогенной среде", — отмечает эксперт. К каждой инфраструктуре требуется свой подход, индивидуальный план сценария миграции с учетом профилей использования. Важно продумывать этапность миграции: пилотные зоны, пользовательские АРМ, серверные группы, сервисы. Определить критичные узлы, которые важно мигрировать для полного отказа от иностранного ПО.

Вячеслав Кадомский, директор по стратегическому развитию НТЦ ИТ РОСА, рассматривает совместимость как критический фактор при переходе на отечественные решения. По данным компании, для большинства заказчиков наиболее реалистичны поэтапные и контролируемые сценарии миграции. "Каждая организация выбирает собственный темп, но везде востребован единый подход: сначала проверка совместимости и пилот, затем постепенное наращивание количества рабочих мест и сервисов".

По мнению Кадомского, успешный переход требует не только методологии, но и инструментов, позволяющих автоматизировать развертывание и сопровождение инфраструктуры. Такой подход обеспечивает быстрый и безопасный переход на отечественные ОС без остановки бизнес-процессов и подходит организациям с инфраструктурой любого масштаба.

Офисное ПО

Евгений Шелковников, генеральный директор Р7, уверен, что обеспечить плавный переход с Outlook на отечественные решения сегодня реально: на рынке уже есть зрелые продукты, позволяющие перенести письма,

календарь и контакты без потери данных. "Важно просто начать ими пользоваться. Пользователи могут продолжить работу в привычном режиме без потери данных и функциональности", — объясняет эксперт.

Среди причин, которые тормозят миграцию офисных рабочих мест, Евгений Шелковников выделяет ожидания части заказчиков, надеявшихся на возможное возвращение Microsoft. По его словам, привычки пользователей и нежелание осваивать новое также играют роль. "Преодолеть это можно, акцентируя внимание на стратегических преимуществах перехода: безопасности, технологической независимости и отсутствии рисков внезапного отключения". Такой подход помогает заказчикам воспринимать миграцию не как вынужденность, а как стратегическое решение.

Антон Гуденко, руководитель департамента управления продуктами МойОфис, считает, что полностью бесшовный переход малореалистичен, но к нему следует стремиться. "Начинать нужно с глубокого аудита используемого ПО — оценить степень его интеграции в процессы и совместимость потенциальных решений. Российские вендоры уже сформировали методики такого аудита, что снижает риски на старте". После получения полной картины проводится пилот: выбираются продукты и тестируются на ограниченном контуре.

Успешный пилот становится основой для подготовки миграции: создание резервных копий, формирование детального плана перехода и сценария отката. "Внедрение должно идти постепенно, от периферии к ядру, при обязательном обучении сотрудников". Финальный этап — мониторинг и поддержка: система нуждается в донастройке и оперативной помощи пользователям. Опыт множества проектов подтверждает, что отечественные поставщики обеспечивают не только функциональные офисные продукты, но и полноценное сопровождение на всех этапах миграции.

ВКС

Иван Шехтман, руководитель проектного офиса Контур.Толка, утверждает, что внедрение нового коммуникационного сервиса неизбежно связано со сменой пользовательских привычек. "Skype для бизнеса устарел, а российские решения ушли далеко вперед по функциональности и удобству. По опыту крупных компаний адаптация к новому сервису занимает около трех месяцев. После этого пользователи не хотят возвращаться в Skype: они получают ощутимый прирост в эффективности работы".

Эксперт делится, что российские разработчики сейчас активно формируют собственные коммуникационные экосистемы.

В пресс-службе "Труконф" уверены, интеграция нового коммуникационного решения в общий ИТ-ландшафт компании — очень чувствительный процесс. "Microsoft много лет формировал замкнутую экосистему — от ОС до офисного ПО — поэтому любое альтернативное решение должно без проблем взаимодействовать с другими элементами корпоративной среды".

Эксперты "Труконф" убеждены, что вопрос безопасности напрямую связан с регулярностью обновлений. "Официальное прекращение поддержки Skype for Business и Windows 10 означает, что уязвимости больше не будут исправляться — это создает прямую угрозу для корпоративной инфраструктуры". По словам экспертов компании, зарубежные ИТ-вендоры активно переводят клиентов в облака, тогда как российские решения предлагают иной подход: система разворачивается в доверенном контуре, и заказчик сохраняет полный контроль над доступом к данным и их обработкой.

Олег Пашукевич, директор бизнес-юнита "Встречи" МТС Линк, видит ситуацию так: многие компании продолжали пользоваться Skype for Business по инерции, хотя сервис к моменту прекращения поддержки уже заметно уступал современным инструментам. Тема безопасности стала одним из главных мотивов для миграции. "Некоторые российские корпоративные пользователи уже сталкивались с внезапным отключением западных сервисов и потерей хранящихся в них данных". Требование хранить данные в России делает переход на отечественные решения еще более актуальным.

Алексей Лямин, сооснователь платформы корпоративных коммуникаций и мобильности eXpress, подчеркивает, что по сравнению с передовым решением глобального вендора — Microsoft Teams — у российских коммуникационных платформ еще есть, куда стремиться, но этот функциональный разрыв стремительно сокращается. "Уникальный плюс российского ПО для коммуникаций в том, что мы идем по собственному пути: не стремясь построить такое же облако Microsoft, только внутри России, отечественные продукты делают ставку на on-premise, позволяя заказчикам перенести или выстроить с нуля базу для цифровизации бизнес-процессов". Главным преимуществом российских коммуникационных решений Алексей Лямин называет их "гибридность": они вбирают в себя лучшие возможности мировых аналогов и делают ставку при разработке на security-first подход. Среди базовых ИБ-механизмов, которые ожидают заказчики российских корпоративных мессенджеров и **ВКС**-сервисов: локализация данных на территории нашей страны, развертывание на локальных серверах компании, end-to-end шифрование, криптоконтейнер, сертификаты государственного образца. "Несомненный положительный тренд развития отечественного рынка ИТ заключается в появлении интеграций между внутренними системами на базе платформ. Продукты „доросли" до того, что стало возможным „подружить" их между собой посредством их API".

Почтовые системы

Александр Калинин, председатель совета директоров CommuniGate Pro, определяет прекращение поддержки продуктов Microsoft как смену парадигмы, а не просто техническую проблему: "Десятилетиями российский рынок

жил в логике закрытой экосистемы одного вендора. В результате всем стало понятно, что национальный рынок не может зависеть от единственного внешнего поставщика, чьи приоритеты могут измениться в любой момент. Если первый этап импортозамещения был посвящен быстрым решениям, то сейчас крупный бизнес и госсектор научились считать совокупную стоимость владения и оценивать возможные риски". Эксперт подчеркивает, что в новой парадигме, помимо привычных характеристик (надежности, кроссплатформенности и возможности интеграции с другими корпоративными сервисами), важнейшим критерием становится безопасность продукта. Заказчики выбирают платформы, которые могут гарантировать стабильность и контроль данных на десятилетия вперед.

Антон Тен, коммерческий директор направления продуктивности VK Tech, описывает процесс миграции корпоративной почты как полностью управляемый и технически предсказуемый: "Большинство корпоративных почтовых систем оснащены встроенными инструментами миграции, которые позволяют перенести все данные: учетные записи, почтовые ящики, письма, календари, рабочие файлы и структуру папок. Организовать бесшовную миграцию можно, даже если в компании работают сотни тысяч сотрудников". Отдельные отечественные решения поддерживают параллельную работу в двух системах, что позволяет проводить переход поэтапно. После завершения миграции прежний сервер можно отключить или использовать как архив.

Антон Тен убежден, что в корпоративной почте должны быть предусмотрены интеграции с антивирусом и антиспам-системой, а также фильтры SPF, DKIM и DMARC. "Среди других средств защиты данных — интеграции с DLP и SIEM-системами, шифрование TLS/SSL (в том числе ГОСТ TLS), протоколы IMAPS/SMTPS для безопасной работы, усиленные парольные политики, вход в сервис по SSO, двухфакторная авторизация, дистанционный контроль сессий пользователей в приложениях и удаление данных с устройств, шифрование и подпись писем электронной подписью (S/MIME)".

По словам Игоря Кальметова, генерального директора ООО "Лаборатория МБК", переход на отечественные почтовые решения требует внимательного отношения к инфраструктуре и особенностям стандартных протоколов, которые используются в большинстве систем. Говоря о защите корпоративной переписки, эксперт указывает, что единый стандарт пока не сформирован, однако отечественные вендоры активно развивают собственные подходы. Игорь Кальметов добавляет, что формальные требования нередко трактуются по-разному, и рынок находится в стадии становления, но при этом уровень защищенности российских решений уже сопоставим с зарубежными: "Мы еще далеки от идеальной безопасности, но не дальше, чем Microsoft, который всегда славился уязвимостями".

Информационная безопасность

Владимир Маракшин, директор департамента стратегического развития компании "Киберпротект", замечает, что прекращение выхода обновлений фактически завершает жизненный цикл продуктов Microsoft с точки зрения информационной безопасности: "Компании, продолжая использовать эти системы без патчей и поддержки, становятся легкой мишенью для злоумышленников, которые активно эксплуатируют уязвимости. Особенно опасна ситуация с серверными решениями".

На период миграции Владимир Маракшин рекомендует сосредоточиться на минимизации поверхности атаки, изоляции устаревших систем и усилении контроля за инфраструктурой. "Критически важно обеспечить надежное резервное копирование данных до начала миграции и на всем ее протяжении", — заявляет эксперт. Кроме того, необходимо максимально снизить влияние человеческого фактора: провести обучение сотрудников, усиливать контроль за пользователями и доступом, внедрять принципы Zero Trust.

"Переход на российские системы не ведет к снижению уровня защиты — напротив, он позволяет перестроить устаревшую инфраструктуру с учетом актуальной ситуации, на основе прозрачной и управляемой архитектуры, соответствующей требованиям информационной безопасности в текущих условиях". В числе приоритетных шагов при построении импортонезависимой ИТ-архитектуры Владимир Маракшин выделяет необходимость четкой стратегии, полного аудита инфраструктуры и планирования миграции по этапам. Эксперт советует выбирать экосистемы, в которых вендоры ориентированы на технологическое партнерство и долгосрочную совместимость, уделять внимание киберустойчивости и регулярно проводить тестирование сценариев восстановления.

Андрей Арефьев, директор по инновациям и продуктовому развитию InfoWatch, полагает, что переход на отечественные решения вряд ли укладывается в несколько месяцев и потребует более длительного периода. "В такой ситуации единственный способ снизить риски — лишить злоумышленника возможности получить доступ к инфраструктуре и эксплуатировать уязвимости. Нужно учитывать и внутренние нарушения: важно усилить контроль за перемещением данных и правами доступа. Плюс к этому — использовать наложенные средства защиты, такие как NGFW и WAF. Именно сочетание этих мер с контролем данных внутри периметра позволяет закрыть значительную часть рисков".

Андрей Арефьев определяет выбор стека ОС, корпоративного каталога и систем ИБ как основу импортонезависимой ИТ-архитектуры. "Между старым сервером с незакрытыми уязвимостями и безопасной, пусть еще не полностью доработанной ОС, выбор очевиден".

Российский рынок входит в этап системной и масштабной миграции: компании отходят от решений Microsoft и одновременно выстраивают новые ИТ-ландшафты на базе отечественных технологий. Эксперты АРПП доказывают, что переход перестал быть точечным и затрагивает уже всю корпоративную инфраструктуру.

Несмотря на разный уровень зрелости продуктов, отрасль движется к формированию полноценной экосистемы: растет совместимость, укрепляются подходы к информационной безопасности, а вендоры выстраивают долгосрочные технологические партнерства.
Импортонезависимая архитектура требует времени и тщательного планирования, но вектор развития очевиден. Компании получают возможность перестроить инфраструктуру под современные требования, обеспечить предсказуемость обновлений и повысить устойчивость критически важных процессов. (IT Channel News 15.12.25)

К СОДЕРЖАНИЮ

Государственное регулирование

Интеллекту задали планку. "КоммерсантЪ". 12 декабря 2025

Утверждены правила для попадания решений генеративного ИИ в реестр российского ПО

Правительство РФ ужесточило требования к программно-аппаратным комплексам (ПАК) для генеративного ИИ, желающим попасть в льготный реестр. По новым нормативам компаниям необходимо иметь собственный центр обработки данных (ЦОД) мощностью от 10 МВт и крупные хранилища данных, что создает высокий технологический и финансовый барьер, уверены участники рынка. Собеседники "Ъ" опасаются, что это может привести к ограничению доступа к льготам малых и средних разработчиков.

Правительство РФ 9 декабря утвердило изменения в правила формирования и ведения единого реестра российского ПО, предоставляющего право на налоговые льготы и отсрочки от армии. По новым правилам производителю программно-аппаратного комплекса для генеративных моделей ИИ необходимо обеспечивать хранение данных объемом не менее 1 эксабайта (около 1,07 млрд Гб); решение задач машинного обучения не менее чем на 1 тыс. графических процессоров (GPU), а также иметь не менее одного центра обработки данных, находящего на территории России и обладающего электрической мощностью не менее 10 МВт.

Кроме того, реестр дополняется подпунктами, которые включают требования иметь чипы с матричными умножителями или их аналогами, "обеспечивающими преобладающую часть вычислительной мощности (равную 75% или более) ПАК, с вычислительной мощностью не менее 8,75 PFLOPs FP4 (показатель производительности, обозначающий квадриллион операций с плавающей запятой в секунду с использованием 4-битного формата данных.— "Ъ")", а также высокоскоростные сетевые адаптеры с пропускной способностью от 400 Гбит/с с RDMA (технология удаленного доступа к памяти минуя процессор и операционную систему). В Минцифры на запрос "Ъ" не ответили. В аппарате профильного вице-премьера Дмитрия Григоренко "Ъ" заверили, что постановление "не отсекает возможности по попаданию в реестр для ИТ-бизнеса, а лишь вводит дополнительную категорию — программно-аппаратных комплексов для генеративных ИИ-моделей". "Новых дополнительных ужесточающих требований для попадания компаний, занимающихся разработкой ИИ, в реестр не вводится",— отметили там.

Российская индустрия пока не выпускает подобные чипы, однако рынок уже выработал механизмы построения цепочек поставок, отмечает основатель WMT AI Игорь Никитин. "Эксабайт хранилища и сетевые подключения на 400 Гбит/с — это уровень крупных технологических компаний. Из-за нововведений рынок столкнется с ростом затрат на инфраструктуру на 40–70%",— прогнозирует господин Никитин. Главный риск в том, что концентрация инфраструктуры в руках небольшого числа крупных игроков может привести к росту цен и снижению гибкости для B2B-сегмента, соглашается независимый эксперт в сфере ИИ Алексей Лерон.

Источник "Ъ" в крупной ИТ-компании отмечает, что наличие вычислительных мощностей никак не гарантирует качества конечного ИИ-продукта. Правильнее устанавливать требования к итоговому ПО, а не к "железу", на котором оно тренируется, считает он. Например, китайские компании арендуют мощности за рубежом, не стремясь строить собственные ЦОДы на десятки МВт, объясняет он: "В такой ситуации требование иметь именно собственный дата-центр превращается не в гарантию безопасности, а в искусственное ограничение доступа к реестру" (о том, как правительство планирует создание органа для поддержки строительства компаниями новых ЦОДов см. на стр. 2).

Есть риск, что мелкие игроки рынка не смогут потянуть такие требования и будут вытеснены, считает советник практики интеллектуальной собственности ЮК ЭБР Кристина Мкртчян. "С другой стороны, высокая планка может стимулировать крупные компании инвестировать в сверхмощные ЦОД ради получения льгот как отечественные ПАКи. Вероятно, останется два-три доминирующих игрока с инфраструктурой мирового уровня",— предполагает он. Нишевые решения, которые можно было бы тиражировать или использовать в нескольких индустриях, теперь попадают под ограничения с точки зрения реализации ПАКов, считает директор по продажам Delta Computers Максим Терещенко. Также ведущий инженер НОЦ ФНС и МГТУ им. Н. Э. Баумана Николай Калуцкий опасается, что "если производитель разрабатывает ПО в коллаборации с производителем "железа" и из полученной синергии получается ПАК, то после принятия таких мер это сотрудничество станет невозможным или очень трудоемким". По его словам, это может существенно сократить рынок стартапов, маленьких и средних компаний. (КоммерсантЪ 12.12.25)

К СОДЕРЖАНИЮ

Общие новости рынка IT

Премьер-министр РФ Михаил Мишустин дал поручения по итогам форума "Цифровые решения".

Стратегия развития отрасли связи на период до 2035 года будет актуализирована с учётом изменения внешних и внутренних экономических условий. Поручение об этом дал Председатель Правительства Михаил Мишустин по итогам форума "Цифровые решения", проходившего в Москве с 12 по 15 ноября.

Подготовить предложения по актуализации стратегии предстоит Минцифры, Минэкономразвития, Минпромторгу, ФАС, ФСБ, АНО "Цифровая экономика" совместно с заинтересованными федеральными органами власти и организациями. Срок – до 25 марта 2026 года.

Ряд поручений в перечне направлен на расширение производства отечественных вычислительных мощностей и поддержку радиоэлектронной промышленности. Так, Минпромторг, Минцифры и Минфин до 26 февраля должны подготовить предложения, направленные на стимулирование закупок радиоэлектронной продукции первого и второго уровня, то есть полностью отечественной продукции и отечественной продукции, для производства которой использовались иностранные компоненты. Речь в том числе идёт о стимулировании закупок программно-аппаратных комплексов первого и второго уровня.

В рамках работы, направленной на обеспечение сохранности данных и бесперебойного функционирования ИТ-процессов, Минцифры, Минэкономразвития, ФСТЭК и ФСБ определят требования к облачной инфраструктуре, которая необходима для размещения на ней корпоративных систем, признанных объектами критической информационной инфраструктуры. Срок – до 27 февраля.

Кроме того, до 30 января Минцифры, Минобрнауки, ФСТЭК и ФСБ совместно с заинтересованными органами власти и организациями проработают вопрос создания центра проведения сравнительного анализа средств защиты информации для усиления противодействия новым киберугрозам и обеспечения безопасности цифровой экосистемы страны.

Несколько поручений посвящено развитию экспорта российских товаров и упрощению таможенных процедур при ввозе импортной продукции. В частности, ведомствам и организациям предстоит разработать "дорожную карту" реализации проекта по экспорту российских товаров и решений с использованием цифровых платформ. В документе в том числе должны быть отражены мероприятия по защите от продажи контрафактной продукции. Речь идёт о создании на базе маркетплейсов верифицированной цепочки поставок с применением технологий отслеживания происхождения товаров для гарантии их подлинности. Выполнять это поручение будут Минпромторг, Минэкономразвития, МИД, Минфин, Минтранс, Минцифры, ФТС, АНО "Цифровая экономика", АО "Российский экспортный центр". О результатах нужно доложить в Правительство до 31 марта.

Минфин, Минэкономразвития, Минтранс, Минцифры и ФТС до 31 марта подготовят предложения об организации пилотного проекта по использованию цифровых платформ для предоставления в таможенные органы документации на товары, необходимой для импортёров. Это должно упростить для бизнеса порядок таможенного оформления, аккумулировать его на базе цифровых платформ.

Форум информационных технологий "Цифровые решения" проводился впервые. Он объединил экспертов, лидеров ИТ-отрасли, предпринимателей, представителей государственных структур. На форуме обсуждались вопросы достижения технологического лидерства России и реализации национального проекта "Экономика данных", а также ключевые направления, определяющие дальнейшее развитие ИТ-отрасли. В рамках форума работала выставка лучших отечественных ИТ-продуктов и состоялась церемония награждения победителей ежегодной национальной премии "Цифровые решения", на которой были отмечены ИТ-проекты, внёсшие значительный вклад в цифровизацию страны. (INFOLine, ИА (по материалам Правительства РФ) 12.12.25)

К СОДЕРЖАНИЮ

Безопасные слияния. "КоммерсантЪ". 10 декабря 2025

Правила M&A для отраслей, где данные — главный актив

Правовые нюансы сделок с ИИ-компаниями плавно выходят за пределы технологий. И в условиях массового внедрения ИИ в нишевые отрасли покупка такой компании превращается в приобретение не только активов, но и целого комплекса юридических обязательств и потенциальных рисков: от дефектов прав на данные до необходимости импортозамещения. Управляющий партнер "Томашевская и партнеры" Жанна Томашевская и юрист практики корпоративного права и сделок M&A Владимир Левшук предупреждают: стандартной процедуры due diligence здесь недостаточно.

ИИ-технологии перестали быть прерогативой крупных корпораций: решения на основе моделей и данных массово внедряются и у нишевых игроков — в медицине, финансовом секторе и других отраслях, где цена ошибки в обращении с информацией особенно высока. Сделки с такими активами сопровождаются как стандартными рисками, так и достаточно специфичными — например, дефектами прав на данные или специальными ограничениями. При этом развитие новых направлений бизнеса зачастую сопровождается новым регулированием, которое не всегда положительно влияет на рынок. Так, например, Закон ЕС об искусственном интеллекте (EU AI

Act) воспринимается бизнесом скорее как барьер для инноваций из-за жесткой системы штрафов, высоких затрат на соответствие требованиям и правовой неопределенности для разработчиков моделей. Фактически, покупая сегодня ИИ-компанию, вы приобретаете не только ее текущие активы, но и обязательство активно формировать ее будущее.
В первую очередь стоит провести юридическую проверку с учетом специфики такой компании. Покупателю важно установить, кому принадлежат ключевые ИИ-активы и на каких основаниях они создавались и использовались. Отдельно следует провести аудит процессов обработки и передачи персональных данных внутри группы и третьим лицам, соблюдения требований о локализации, мер информационной защиты, наличия согласий субъектов персональных данных.
Следующим шагом для покупателя станет выявление всего объема компонентов с открытым исходным кодом и предобученных моделей. Если бизнес опирается на инфраструктуру, требующую специальных лицензий (например, на средства защиты конфиденциальной информации, шифровальные средства), нужно проверить их наличие, срок действия и соответствие фактическим видам деятельности.
Стоит учесть, что в России существует специальный статус компаний — субъекты критической информационной инфраструктуры (КИИ). Если компания относится к таким, покупатель получает дополнительные обязательства по защите значимых объектов: организационные меры, системы мониторинга и реагирования, требования к ПО и инфраструктуре, иные комплаенс-нагрузки. Это напрямую влияет на бюджет и сроки интеграции — а значит, должно заранее учитываться и в оценке актива, и в структуре сделки (включая условия закрытия и распределение расходов).
После того как компания проанализирована, важно определить структуру сделки. Покупка компании "целиком" позволяет сохранить действующие договоры, лицензии и статус оператора персональных данных, но одновременно переносит на покупателя потенциальные нарушения и регуляторные риски прошлых периодов. Покупка отдельных активов дает возможность отсечь проблемные обязательства, однако повышает сложность перехода: перенос клиентских баз, перезаключение договоров, получение согласий на обработку данных новым оператором, переоформление прав на данные и модели. На выбор конструкции накладываются и налоговые последствия, а также издержки как в момент сделки, так и в перспективе (например, при последующей перепродаже актива).
В структурировании сделки важную роль играют и регуляторные согласия. На стадии планирования нужно оценить их влияние на конкуренцию: изменится ли доступ других игроков к данным и инфраструктуре, усилятся ли барьеры входа, появится ли возможность исключать конкурентов. Заранее стоит оценить, подпадает ли сделка под требования согласования с ФАС или правительственной комиссией, в том числе с учетом имеющихся лицензий — необходимость получения согласия может удлинить сроки сделки.
Следующий важный вопрос, на который нужно обратить внимание,— управление доступом к данным и информационная безопасность (ИБ). Еще до закрытия сделки следует унифицировать политики ИБ, категоризацию информации, уровни угроз и защиты, проверить условия конфиденциальности в договорах с работниками и контрагентами, при необходимости ввести режим коммерческой тайны и регламенты о конфиденциальной информации. Важно провести ревизию учетных записей, в том числе доступов к репозиториям кода, хранилищам датасетов и контурам эксплуатации и обучения моделей, определить порядок предоставления и прекращения прав доступа.
При покупке компании не стоит забывать и о главном активе — сотрудниках. Помимо технических ролей, критичны доменные эксперты, которые понимают отраслевую специфику (например, в медицинской или финансовой отраслях). Такие ключевые специалисты зачастую работают по гражданско-правовым договорам или через подрядчиков, что повышает риски их ухода. Следует провести аудит договоров, перевести работников на более устойчивые форматы взаимодействия и предусмотреть инструменты мотивации и удержания — например, опционные программы.
Следующая стадия — так называемая миграция данных. Перед ней проводится инвентаризация: источники, объемы, форматы, права, категории данных и уровни доступа и защиты. На ее основе формируется "дорожная карта" с этапами, контрольными точками, уведомлениями регуляторов, изменениями локальных актов и договоров, назначаются ответственные за каждый этап; затраты на миграцию закладываются в финансовую модель сделки.
Финальное правило, которое особенно актуально,— импортозамещение. ИИ-решения нередко завязаны на зарубежные облака, модели и сервисы, доступность которых может измениться по внешнеполитическим причинам. Покупателю необходимо оценить зависимость актива от иностранной инфраструктуры, сценарии отказа от нее и стоимость перехода на отечественные аналоги — особенно если компания работает с госзаказчиками или подпадает под требования КИИ. Выявленные расходы на импортозамещение разумно заранее переводить в механизмы корректировки цены и условия закрытия.
Сделка по слиянию и поглощению в отношении ИИ-компаний в секторах, где данные являются главным активом,— это сделка не только про доли и выручку, но и про правовой режим данных, происхождение моделей, соблюдение требований безопасности. Комплексная юридическая проверка (due diligence), правильная структура сделки и детальное планирование интеграции снижают вероятность финансовых и репутационных потерь и помогают сохранить непрерывность бизнеса. Стоит помнить, что право в этом направлении развивается опережающими темпами и успешная интеграция приобретенного актива требует создания процессов для

постоянного мониторинга регуляторных изменений. Если вы готовите сделку с ИИ-компанией, работающей с критическими данными, имеет смысл превратить эти правила в рабочий чек-лист и заранее распределить ответственность между юристами, технической командой и службой информационной безопасности. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

Идеальный шторм. "КоммерсантЪ". 10 декабря 2025

Льготы в IT-индустрии сохраняются, но налоговые проверки становятся тотальными

ФНС возвращается к регулярным проверкам IT-сектора, используя как новые, так и классические инструменты налогового контроля. Повышение ставки налога на прибыль до 5% и снятие моратория на выездные проверки существенно изменили фискальный ландшафт для отрасли, поставив в центр внимания законность применения льгот и обоснованность расходов. Руководитель налоговой практики ЭБР Игорь Грибков - о том, почему налоговые льготы IT-компаний теперь приходится доказывать в суде.

Текущий год ознаменовался усилением фискального интереса к IT-бизнесу со стороны государства. Основанием для этого послужили в том числе изменения налогового законодательства, принятые в 2024 году. Ключевым из них, актуальным для большинства аккредитованных IT-компаний, стало увеличение ставки налога на прибыль с 0% до 5%. Не менее важным стало и повышение страховых взносов на выплаты сверх так называемой предельной величины (в 2025 году она составила 2,7 млн руб.) - до 7,6%, хотя ранее компании применяли 0%.

Кроме того, в марте 2025 года завершился мораторий на выездные налоговые проверки в отношении аккредитованных компаний. При этом назначение таких проверок в исключительных случаях допускалось и в период действия моратория, однако, как следует из судебных актов по спорам между налоговыми органами и IT-компаниями, большинство претензий предъявляется по результатам камеральных, а не выездных проверок.

Одним из последних публичных примеров такого внимания стало дело №А76-28833/2024: в нем рассматривался спор налогового органа с компанией, применившей IT-льготы в связи с осуществлением деятельности по предоставлению и разработке баз данных и CRM-систем для предприятий, работающих в сфере газоснабжения. По мнению налогового органа, фактически налогоплательщик оказывал услуги по ремонту объектов системы газораспределения и газопотребления. В ноябре 2025 года суд первой инстанции согласился с позицией налогового органа, указав в том числе, что компания не доказала факт оказания IT-услуг заказчикам.

С точки зрения налогообложения IT-компании находятся в двойственном положении. С одной стороны, новая налоговая реформа сохранила для IT-сектора значительный объем специальных налоговых льгот. К ним относятся: пониженные тарифы страховых взносов (15% вместо 30%, а по выплатам свыше так называемой предельной величины - 7,6%), льготная ставка по налогу на прибыль (5% вместо 25%), а также освобождение от НДС операций по реализации программного обеспечения, включенного в ЕРРП (вместо 22-процентной налоговой ставки). Соответствующая налоговая экономия будет иметь ключевое значение для отрасли, но стоит обратить внимание на два важных аспекта.

Первый из них - аккредитация Минцифры России, которая необходима каждой компании для применения IT-льгот. Согласно последним изменениям, утвержденным правительством РФ, для ее получения или сохранения теперь потребуется направлять не менее 3% сэкономленных на налогах средств на поддержку образовательных программ в высших учебных заведениях. В связи с этим бизнесу важно обеспечить корректный налоговый и бухгалтерский учет - например, если в ходе налоговой проверки за предыдущий период будет установлено, что фактический размер выручки компании превышает отраженный в отчетности, то экономия от льготной ставки по налогу на прибыль окажется заниженной и объем средств, направленных компанией на образовательные программы, будет меньше установленного уровня. Это может послужить основанием для утраты аккредитации и, как следствие, права на применение налоговых льгот.

Второй аспект - повышение интереса налоговых органов к отрасли в последнее время. Поскольку льготы для аккредитованных компаний существенно снижают налоговую нагрузку и непосредственно связаны с выполнением различных критериев (в том числе по структуре выручки), инспекторы все чаще обращают свой взгляд на подобных налогоплательщиков.

С другой стороны, IT-компания остается обычным хозяйствующим субъектом, в отношении которого в полном объеме применяются общие требования Налогового кодекса РФ. В частности, проверяющие могут признать неправомерными расходы и вычеты по НДС по контрагентам, деятельность которых вызывает вопросы, что приводит к доначислению налога на прибыль и НДС. Также наличие статуса аккредитованной компании не исключает правомерности проверки применения пониженных ставок по международным соглашениям об избежании двойного налогообложения, корректности внутригруппового ценообразования и наличия признаков искусственного дробления бизнеса.

Более того, цифровая специфика часто усложняет аргументацию по указанным вопросам - например, при подтверждении значительных расходов на рекламу или продвижение в сети Интернет. И хорошо, если у компании есть сотрудники, способные транслировать технологические и организационные аспекты ее высокотехнологичной деятельности в юридически и экономически релевантную плоскость. Наиболее оптимальным вариантом является

привлечение к работе специалистов, за плечами которых существенный опыт сопровождения IT-проектов и взаимодействия с ФНС.
Отдельного внимания заслуживают общие тенденции развития налогового контроля: он все больше переходит в режим фонового и фактически постоянного анализа налогоплательщиков. Об этом свидетельствует статистика: большая часть поступлений в бюджет за 2024 год обеспечена за счет контрольно-аналитических мероприятий (то есть без проведения камеральных или выездных проверок). В рамках таких мероприятий налогоплательщику сообщается о выявленных рисках и предлагается добровольно доплатить налоги и пени. При этом более чем в половине случаев налогоплательщики соглашаются с предложениями ФНС.
Цифровизация налогового администрирования усиливает эту тенденцию: информационные системы налоговых органов позволяют в автоматическом режиме анализировать, например, количество и регулярность привлечения самозанятых, оперативно формируя для инспектора массив данных для дальнейшей контрольной работы. Соответственно, в 2026 году IT-бизнесу особенно важно качественно прорабатывать свою позицию и ее обоснование по потенциально спорным налоговым вопросам. И лучше заняться этим на этапе проектирования финансовой модели и структурирования сделок, а не после получения требования от налоговой инспекции. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

IT сбавляет обороты. "КоммерсантЪ". 11 декабря 2025

Как российская технологическая отрасль адаптируется к ужесточению законодательства

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".

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 Максут Шадаев. Однако пока индустрия растет все еще быстрее показателя по экономике в целом, который в 2025 году составляет 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 M&A. 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 появится 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 Шаньгин. Он напомнил, что новые

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

требования к совместимости с отечественными ОС для вендоров означают, что "без доказанного 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 появление 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 дополнительная 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 обеспечения 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 сальдо 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 требованиям, 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 разработка" Максим Егоров также говорит о тренде в развитии ИИ: от ИИ-Copilot 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Интернет вещей и умные устройства ждет технологический прорыв в 2026 году. "РБК.Отрасли". 10 декабря 2025

2026 станет годом масштабного развития IoT в России: число промышленных подключений превысит 117 млн, а отрасль будет активно развиваться благодаря ИИ. С какими вызовами столкнется рынок и почему следующий год может стать прорывным — Павел Подколзин, МТС

2025 год стал переломным для российского рынка интернета вещей. Несмотря на макроэкономические вызовы, отрасль показала уверенный рост благодаря курсу на импортозамещение и технологический суверенитет.

Важно отметить то, как изменились запросы рынка: если раньше мы обсуждали технические спецификации, то сегодня говорим о повышении EBITDA и создании новых бизнес-моделей. Всего за несколько лет Россия прошла путь от осторожных экспериментов с IoT к полномасштабной цифровой трансформации, которая сегодня определяет конкурентоспособность целых отраслей.

По данным аналитиков, объем рынка IoT в России достиг 237 млрд руб., показав рост на 15% по сравнению с предыдущим годом. При этом количество подключенных IoT-устройств превысило 117 млн единиц, а число предприятий, использующих промышленный интернет вещей, выросло до 5762.

Особую роль в развитии IoT-экосистемы играют выделенные сети связи (Private LTE/NB-IoT/5G), которые обеспечивают надежную и защищенную инфраструктуру для промышленных применений.

Транспорт и логистика с фокусом на беспилотные технологии и роботизацию станут ключевым драйвером роста IoT в 2026 году. Синергия с IoT создает уникальные возможности: единая инфраструктура обеспечивает навигацию, телеметрию, видеоаналитику и управление автономными системами в режиме реального времени.

Три главных события и тренда 2025 года

Выделенные сети: от пилотов к стратегической инфраструктуре. В 2018 году мы только начинали обсуждать пилотные проекты Private LTE. Сегодня же мы видим, как выделенные сети становятся кровельной системой цифровых предприятий: по внутренним оценкам МТС, российский рынок Private LTE показал среднегодовой рост на уровне 20–25%. Ключевой запрос промышленности сегодня заключается в создании защищенной, предсказуемой и управляемой инфраструктуры. Компании уже не спрашивают, зачем внедрять, а интересуются, как масштабировать.

ИИ и IoT: синергия, которая перестала быть теорией. По данным Strategy Partners и ГК "Цифра", в 2025 году количество крупных и средних предприятий, использующих технологии больших данных, IoT, компьютерного зрения и генеративного ИИ, выросло на 40%. Промышленный интернет вещей стал платформой для внедрения предиктивной аналитики и цифровых двойников. Конвергенция IoT и ИИ вышла на новый уровень — 39% крупных российских предприятий уже используют ИИ-инструменты, а 25% планируют внедрение в ближайшее время.

Развитие отечественных IoT-платформ и импортозамещение. Уход зарубежных вендоров стал катализатором роста российских платформенных решений. Ожидается, что доля отечественных решений для IoT будет стремительно расти до 2030 года.

Лидирующие отрасли по внедрению и окупаемости IoT

Горнодобывающая отрасль лидирует по внедрению промышленных IoT-технологий, включая pLTE. Выделенные сети обеспечивают критическую радиосвязь, видеонаблюдение, данные от сенсоров и точное позиционирование техники и персонала. IoT усиливает промышленную безопасность: системы "антинаезда" предотвращают столкновения, датчики установок снижают риск аварий, носимые устройства позволяют быстро определить местоположение работников при ЧП.

В нефтегазовой отрасли IT-расходы выросли на 155%, до 135 млрд руб. На цифровизацию, включая ИИ и IoT, пришлось 53 млрд руб. (+17%). Датчики мониторинга трубопроводов сокращают аварийность, а, по данным Минэнерго, цифровая трансформация к 2035 году может давать отрасли до 700 млрд руб. в год. Значимая часть IoT-проектов направлена на защиту персонала: системы контроля загазованности, мониторинг здоровья в опасных зонах, автоматическое оповещение и эвакуация.

В транспорте и логистике IoT/M2M остается крупнейшим сегментом по числу подключений. Рост ускоряют проекты беспилотных транспортных коридоров, требующие развитой инфраструктуры V2X. Они уже дают экономический эффект за счет оптимизации маршрутов и сокращения операционных затрат.

Общий тренд для всех отраслей — повышение промышленной безопасности и движение к "нулевому травматизму". IoT играет в этом ключевую роль:

- системы "антинасада" предотвращают столкновения тяжелой техники с людьми;
- точное позиционирование персонала помогает при эвакуации и спасательных операциях;
- носимые устройства отслеживают пульс, температуру и усталость, предупреждая опасные состояния;

I- oT контролирует доступ в опасные зоны и соблюдение протоколов безопасности;

- датчики загазованности, вибрации, температуры и давления позволяют выявлять предварийные состояния.

Инвестиции в безопасность имеют и экономический эффект: снижение травматизма уменьшает простой, страховые выплаты и репутационные риски. Комплексные IoT-системы помогают сократить число инцидентов на 40–60%.

Ключевые нерешенные проблемы

Кибербезопасность остается ключевым вызовом. По данным RED Security SOC, в первом полугодии 2025 года на промышленные предприятия пришлось около 7500 кибератак. Исследования "Информавитин" и Positive Technologies фиксируют рост таргетированных APT-атак на 20–22%. Главная уязвимость IoT-экосистемы — незащищенная передача данных: до 98% трафика IoT-устройств передается без шифрования, отмечают в "ECA ПРО". Это делает внедрение частных защищенных сетей связи необходимостью.

Темпы внедрения IoT тормозят высокая стоимость решений и острый кадровый дефицит. Помимо общего недостатка IT-специалистов (минус 500–700 тыс. человек) особенно не хватает экспертов по IoT и по работе с промышленными системами (АСУ ТП).

Низкая осведомленность заказчиков тоже сдерживает рынок: многие компании не понимают реальных возможностей и стоимости IoT-проектов. Кроме того, на местах нередко возникает сопротивление новым технологиям из-за недоверия и опасений по поводу изменения привычных процессов.

Баланс облачной и периферийной аналитики

В 2025 году стало окончательно ясно: периферийные вычисления — не дополнение к облаку, а самостоятельная ценность. В промышленном IoT Edge-интеграция превратилась в фактор конкурентоспособности. Она снижает задержки при управлении оборудованием в реальном времени, уменьшает нагрузку и затраты на передачу данных, повышает безопасность за счет локальной обработки чувствительной информации и обеспечивает автономность при потере связи с облаком.

При этом облако остается ключевым для долгосрочной аналитики, машинного обучения и объединения данных с разных площадок. В итоге формируется гибридная модель: Edge обеспечивает оперативную обработку и принятие решений на месте, облако — стратегическую аналитику и централизованное управление. Такое сочетание улучшает работу IoT-систем и снижает риски, связанные с доступностью и безопасностью.

ИИ — самый главный тренд 2026 года

Edge AI станет главным трендом 2026 года. Сочетание IoT, искусственного интеллекта и периферийных вычислений откроет новые возможности для транспорта, медицины, Индустрии 4.0 и умных городов. Edge-инфраструктура и микро-дата-центры станут базовыми для логистики, ретейла и промышленности: обработка данных прямо на месте их генерации — в магазинах, на складах и в цехах — позволит принимать решения в реальном времени без обращения к облаку.

Для индустриальных сценариев это означает расширение IoT-инфраструктуры: выделенные сети превращаются из каналов передачи данных в интеллектуальные платформы со встроенной аналитикой. В единую инфраструктуру включаются видеоаналитика, AR, дистанционное управление и предиктивная аналитика, создавая основу для автономных производств и беспилотных систем.

Edge AI усиливает и промышленную безопасность:

мгновенно распознает опасные ситуации;

автоматически останавливает оборудование при появлении человека в опасной зоне;

анализирует поведение работников, помогая предотвратить инциденты — все это без задержек на отправку данных в облако.

Ожидаемый технологический прорыв 2026 года

Массовое внедрение цифровых двойников и предиктивных IIoT-систем выводит промышленный интернет вещей на новый уровень — от простой телеметрии к моделированию и прогнозированию процессов.

Главные направления развития:

- алгоритмы ИИ анализируют потоковые данные с датчиков и прогнозируют отказ критичных узлов за недели до инцидента. Это снижает незапланированные простой на 30–40% и уменьшает расходы на обслуживание;
- цифровые двойники технологических линий позволяют моделировать и оптимизировать работу без вмешательства в производство, снижая отклонения в качестве продукции на 20–25%;
- роботизированные комплексы становятся интеллектуальными: их оснащают компьютерным зрением и предиктивной аналитикой. Мировой рынок ИИ для робототехники растет в среднем на 25% в год, что подтверждает высокий спрос;
- формируются автономные системы управления предприятием: от автоматизации отдельных операций индустрия переходит к сквозным решениям, которые оптимизируют производственную цепочку почти в реальном времени, используя данные IoT и машинное обучение.

Главный вызов: кибербезопасность как основа доверия

Кибербезопасность датчиков, исполнительных устройств и промышленного оборудования станет главной темой IoT на ближайшие три-пять лет. Решать предстоит сразу несколько проблем.

Атаки становятся сложнее: массовые простые атаки снижаются, но таргетированные растут на 20–22% в год. IoT-устройства все чаще служат точкой входа в корпоративные сети.

Уязвимость шлюзов: взлом IoT-шлюза открывает доступ и к операционным технологиям, и к IT-системам, поэтому защита каналов связи и сетевого оборудования выходит на первый план.

Регуляторное давление: с мая 2025 года действуют штрафы за утечки данных до 3% годового оборота, что повышает спрос на экспертов и решения для защиты IoT.

Необходим комплексный подход: сегментация доменов, контроль коммуникаций, проверка подписи обновлений, IDS/IPS — все это требует серьезных ресурсов и компетенций.
Выделенные промышленные сети дают ключевое преимущество: изолированная цифровая среда сокращает поверхность атаки. Интегрированные комплексы защиты — криптошлюзы, межсетевые экраны, системы обнаружения вторжений — уже используются на критически важных объектах и становятся отраслевым стандартом. (РБК.Отрасли 10.12.25)

К СОДЕРЖАНИЮ

Технологии бизнес-масштаба. "КоммерсантЪ". 11 декабря 2025

Как ИТ помогает компаниям расширяться и повышать свою эффективность

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.
Как результат в ИТ-холдинге Т1 уверены, что по итогам 2025 года динамика отечественного сегмента продажи ИТ-услуг, ПО и ИТ-оборудования для B2B-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 уязвимостей 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 для 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 Гущин 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 Гущин.

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 1С, 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 отечественных 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Лицом к лицу. "КоммерсантЪ". 11 декабря 2025

Как развивается биометрическая идентификация в России

Наталья Бессонова, директор департамента биометрических технологий Центра биометрических технологий, рассказала "Ъ-Науке", как liveness делает биометрическую идентификацию безопаснее, есть ли у российских разработчиков зависимость от иностранного ПО и смогут ли технологии будущего считывать человеческие намерения.
Вопреки расхожим стереотипам, биометрическая идентификация в упрощенном виде появилась задолго до изобретения современных нейросетей. Фактически на лице фиксировали набор контрольных точек: уголки глаз, крыльев носа, губ, контуры овала. Затем сравнивали расстояния между этими точками на разных снимках и при совпадении делали вывод, что это один и тот же человек.
Что сделали современные нейросети, так это придали импульс развитию биометрии. Они вывели ее из разряда "экзотических" технологий в категорию массовых, которые можно безопасно и удобно применять в банках, транспорте, госсервисах и рознице.

Liveness-технологии

Одним из ключевых драйверов этого перехода стали как раз нейросетевые алгоритмы liveness — проверки "живости" пользователя. Нейросеть обучают отличать реального человека от "его копий": фотографий с экрана, распечатанных снимков, 3D-масок и т. п.
Наверное, многие видели ролик, где девушка пыталась провести оплату по фото мужа. Из полной версии этого видео понятно, что система распознала обман: на экране терминала появилось сообщение "Мы Вас не узнали".
На фоне роста числа мошеннических атак, распространения дипфейков и качественных поддельных снимков именно liveness стал центральным элементом современной биометрии. Постоянные улучшения в этой области направлены на то, чтобы блокировать мошеннические сценарии и снижать количество ошибок при работе с реальными пользователями.
Существуют два основных вида liveness-технологии. Первая — это активный liveness. В этом случае пользователь должен совершить типовые действия: система просит его повернуть голову, улыбнуться, моргнуть. Это надежный

метод: мошеннику сложно перебрать все варианты. Плюсом ко всему здесь ограничено время выполнения действий, что повышает безопасность. Но у этого метода есть минусы: он нередко доставляет пользователям неудобства — люди теряются в инструкциях, например не понимают, относительно чего определяется правая сторона (себя или телефона). Это приводит к ошибкам и потере клиентов.

Вторая технология — пассивный liveness — менее навязчива и более удобна для пользователя, так как не требует активных действий. Здесь ключевую роль играют нейросетевые алгоритмы, которые в последнее время научились определять живого человека по одному изображению с точностью более 99,9%.

Биометрия по ладони

Если говорить о новых направлениях, которые пока не стали таким стандартом, как распознавание лица, но уже активно исследуются, то особо стоит упомянуть технологии, связанные с ладонями.

Речь идет не только о работе с изображением ладони в видимом диапазоне — рисунком линий и складок между фалангами пальцев, который может использоваться вместе с распознаванием лиц на одном терминале, но и о венозном рисунке, считываемом с помощью инфракрасной камеры.

Венозная биометрия уже применялась на предприятиях с особыми требованиями к безопасности — там, где сотрудники носят каски или маски, затрудняющие распознавание лиц, а также в условиях, где травмы рук и мозоли мешают использовать классическое изображение ладони.

Поведенческая биометрия

Помимо распознавания по венам серьезные надежды связывают с поведенческой биометрией — оценкой движений тела. Пока она считается менее точной во многом потому, что в ее развитие заметно меньше инвестируют. Однако при целенаправленных усилиях компании вполне могли бы дообучить алгоритмы до приемлемого высокого уровня качества.

Примером может служить анализ движений для пропуска в здание: человек, заходя на предприятие, проходит через коридор, а система анализирует его походку. Ряд российских компаний уже пробовали подобные решения в пилотном режиме. Технологии анализа поведения и трекинга движения человека есть, например, у NtechLab и VisionLabs.

В других сценариях поведенческая биометрия также выглядит перспективно. Если речь идет не о точке прохода на предприятии, а, скажем, о ноутбуке, привычная связка "логин—пароль" создает множество неудобств: пароли забываются, их нужно регулярно менять, а при нарушении регламента пользователь может временно потерять доступ.

Здесь помимо распознавания лица возможен вариант с клавиатурным почерком — уникальной манерой набора текста. Эта технология хорошо описана и может использоваться как для аутентификации при входе, так и для контроля в процессе работы, чтобы исключить ситуацию, когда один сотрудник разблокировал устройство, а затем за него начинает работать другой под теми же учетными данными.

При этом поведенческая биометрия пока сложнее в использовании, поскольку сильно зависит от бытовых факторов. Неудобная обувь, новая пара ботинок, травмы ног — все это меняет походку. Аналогично и за ноутбуком: непривычная клавиатура, травмы рук, разговор по телефону во время набора текста — все влияет на стиль печати и снижает точность распознавания.

Тем не менее любой параметр, позволяющий достоверно отличить одного человека от другого, потенциально может стать биометрическим фактором. В разные годы пробовали использовать даже электроэнцефалограмму или электрокардиограмму, но такие методы оказались слишком неудобными. Нужно было специальное оборудование: аппарат ЭКГ, датчики и т. п.

Впереди планеты всей

В биометрических технологиях российские компании — одни из лучших в мире. Во многом стремительное развитие направления в России связано с участием отечественных компаний в международных тестированиях и высокой конкуренцией на рынке.

Многие российские разработчики регулярно участвуют в открытых конкурсах, например в международных испытаниях, проводимых американским институтом стандартов NIST, и занимают призовые места по разным базам данных. Эти базы учитывают различные условия съемки: кооперативный режим (пользователь смотрит в камеру) и некооперативный режим (человек не знает о распознавании, могут быть большие повороты головы, частичное попадание в кадр, плохое освещение). Успехи в таких испытаниях подтверждают качество алгоритмов и стимулируют их развитие.

Что касается разработок отечественных компаний, то большая часть алгоритмов и решений российские. Да, возможно использование отдельных open source библиотек, но в целом это собственные разработки отечественных команд, и по части программного обеспечения значительной зависимости от иностранных ресурсов нет.

Российские компании активно сотрудничают и с университетами: проводят обучающие семинары, берут студентов на стажировки, читают лекции, совместно работают в лабораториях. Среди вузов, уже имеющих образовательные программы в сфере биометрии,— МГТУ имени Баумана, ИТМО, МФТИ, СПбГУ, Центральный университет и др.

Вузы участвуют в исследованиях, а студенты в рамках научных работ разрабатывают новые алгоритмы, которые затем могут быть востребованы рынком. Такое взаимодействие дает приток талантов и способствует формированию новых компетенций.

Защита данных

Проблема защиты биометрических данных от взлома вызывает наибольшие страхи в обществе. Реальных оснований под этими страхами нет.

В России все данные хранятся централизованно и под контролем государства в Единой биометрической системе. Взламывать ее, во-первых, технически сложно, а во-вторых, бессмысленно. В системе не содержатся паспортные данные, а сами биометрические образцы хранятся в обезличенном зашифрованном виде.

Даже если бы мошенническая нейросеть смогла частично восстановить изображение по вектору признаков, она бы сделала это с потерями. Результат не был бы идентичен исходному снимку.

Помимо шифрования данных и защищенной передачи применяются алгоритмические методы защиты векторов признаков. Разработчики могут использовать дополнительные преобразования или вносимый шум, модификацию вектора и другие приемы, которые препятствуют точному восстановлению исходного изображения. Эти методы в некоторой мере аналогичны криптографическим приемам защиты.

В России при обработке биометрических данных действуют нормативные требования ФСБ и ФСТЭК к безопасности систем и к применяемым средствам информационной безопасности для хранения и передачи биометрических персональных данных.

Биометрические данные хранятся в зашифрованном виде и передаются по защищенным каналам. Компания, которая внедряет биометрический сервис, обязана обеспечить соответствующие меры информационной безопасности и приобрести необходимое оборудование.

Будущее биометрии

Судя по динамике рынка, главный прорыв еще впереди, и он будет связан не столько с появлением принципиально новых технологий, сколько с ростом числа пользователей.

Сейчас мы переживаем стадию "притирки". Похожую ситуацию мы наблюдали пару десятилетий назад, когда люди массово переходили на банковские карты: многие боялись, что их банковский счет украдут или внезапно заморозят. Биометрия проходит те же этапы, что и любое технологическое новшество. Здесь наибольший эффект даст увеличение количества людей, ежедневно использующих биометрические сервисы в бытовых ситуациях: для оплаты, доступа в помещения, удаленной идентификации на "Госуслугах" и в банках. Все это ждет нас в ближайшее время. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Совместимость как стратегия. "КоммерсантЪ". 11 декабря 2025

Почему внедрение интеграционной платформы становится условием успешной цифровизации

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 Bercut Андрей Богданов.

Этот подход отвечает на главный вызов для бизнеса — необходимость одновременно работать с разнородными IT-системами. В корпоративном ландшафте соседствуют продукты SAP, 1С, 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 продукта. 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.

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

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 типовые 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Устойчивость вместо скорости. "КоммерсантЪ". 11 декабря 2025

Как сервисные модели управления помогают компаниям сохранять предсказуемость процессов

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.

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 сильна 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 заказчиков — 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 промышленных 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 реальную бизнес-логику и обеспечивать предсказуемость процессов.

Поддержать такую трансформацию организациям помогают инструменты управления процессами: no-code 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 требования. 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Управление данными: выход из хаоса. "КоммерсантЪ". 11 декабря 2025

Почему компании переходят от накопления информации к системной работе с ней

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.

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 Роскомнадзора, 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 DataGovernance показывают достаточно высокий уровень зрелости, сопоставимый с зарубежными аналогами. В этом году международная биофармацевтическая компания AstraZeneca выбрала российского 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 обеспечивают 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Замедление неизбежно: какие IT-проекты выживут в 2026 году. "РБК.Отрасли". 12 декабря 2025

Рынок IT в 2026 году столкнется с самым заметным замедлением за последние годы. Деньги в отрасли есть, но вкладывать их стали осторожнее. О том, почему компании сворачивают проекты и какие направления "выживут", — Александр Семенов, "КОРУС Консалтинг"

Если в 2024 году рост российского IT-рынка оценивался в районе 18–20%, то по итогам 2025-го можно ожидать почти двукратное замедление роста в районе 10%. При этом существуют и более пессимистичные прогнозы, согласно которым в текущем году оборот IT-рынка вырастет только на 3%.

Основные факторы, влияющие на отрасль, очевидны — общая нестабильность экономической ситуации, высокая ключевая ставка и, соответственно, сокращение объемов инвестиций, в том числе в цифровизацию.

Кто сейчас покупает IT-проекты

Уровень спроса на IT-продукты и услуги остается неоднородным и зависит от отраслевых особенностей, потребностей и финансовых возможностей каждой компании. Например, если в 2025 году банки и страховые компании инвестировали в IT-системы и оборудование на 36,5% больше, чем в прошлом, то в таких сферах, как машиностроение, нефтегазохимия и транспорт, эти расходы сократились на 10–40%. Однако это скорее "средняя температура по больнице", поскольку в любой отрасли остаются как лидеры, которые продолжают активно вкладываться в цифровизацию, так и компании, замораживающие часть IT-проектов.

Тем не менее можно выделить два общих тренда, поддерживающих спрос на IT-продукты и услуги. Во-первых, многие продолжают IT-проекты, связанные с импортозамещением софта, причем это касается не только государственных компаний, но и частного бизнеса. Например, в этом направлении активно работают компании, иностранные владельцы которых ушли с рынка, а активы были выкуплены местным менеджментом. Материнские компании перестали поставлять и поддерживать иностранное ПО, поэтому новому руководству необходимо продолжать перестраивать и развивать IT-инфраструктуру.

Вторая история тоже связана с консолидацией бизнес-активов, например, в ретейле, e-commerce и других сферах. Крупные компании за последние два-три года начали скупать более мелких игроков. Среди этой категории спрос на проекты по повышению эффективности производственных и бизнес-процессов с помощью IT-инструментов или по управлению холдингом (планирование, бюджетирование, учет, документооборот и т.д.) тоже сохраняется. Рост

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

бизнеса по определению подразумевает переменку IT-инфраструктуры, миграцию данных, прозрачность управления и другие аспекты, связанные с цифровизацией.

"Кэптивные иллюзии" прошли

Еще три года назад на фоне ухода зарубежных вендоров с российского рынка, предоставления льгот IT-сектору и других причин многие крупные игроки начали создавать кэптивные IT-компании. Предполагалось, что они смогут работать не только на материнскую компанию, но и продавать свои продукты и услуги на внешнем рынке, генерировать выручку.

Но уже сейчас стало понятно, что такая экономическая модель во многом себя не оправдала. Когда у кэптивной IT-компании есть гарантированный внутренний заказ, ей не особо интересно работать на внешнем рынке с высокой конкуренцией. Кроме того, зачастую IT-решения "дочек" учитывали исключительно особенности и потребности своих материнских компаний. Соответственно, функциональность таких решений оказалась невостребованной среди других игроков рынка за редким исключением.

Поэтому в 2026 году можно с большой вероятностью ожидать реструктуризации ряда кэптивных IT-компаний, снижения инвестиций в этом направлении. Многие крупные игроки будут переосмыслить экономическую модель и стратегии своих IT-"дочек".

Кто вырастет в 2026 году

В целом спрос на IT-продукты и решения большинства классов останется стабильным, и большого всплеска по какому-то отдельному направлению ожидать не стоит. Однако есть три сферы, которые в следующем году будут расти быстрее других.

Первое — это продукты и услуги в сфере кибербезопасности. Даже при сокращении IT-бюджетов все понимают, что угрозы, связанные с ИБ, — это прямые риски остановки бизнес-процессов, поэтому инвестиции в этом направлении компании будут сокращать в последнюю очередь.

Второе — ИИ-решения. Мы полагаем, что во всех отраслях в ближайшие годы появятся новые компании, потенциальные лидеры рынка, которые изначально будут строить свои бизнес-процессы на базе ИИ-инструментов. Число ИИ-стартапов в стране к 2030 году может вырасти почти вдвое, а объем инвестиций достичь 300 млрд руб. Другой вопрос, что для внедрения ИИ-решений (которые сами по себе стоят не так много) нужна дорогая IT-архитектура, нужны изменения корпоративной культуры. Несмотря на возможные сложности, компании будут активно вкладываться во внедрение ИИ, так как это позволит им существенно повысить общую продуктивность организации. Среди наиболее распространенных задач, которые сегодня доверяют ИИ: анализ данных, поддержка клиентов и работа чат-ботов, формирование отчетов, презентаций, задачи дизайна. Это снижает нагрузку на сотрудников и повышает производительность труда.

Наконец, в 2026 году можно ожидать роста количества IT-проектов, связанных с повышением эффективности промышленной автоматизации. Многие предприятия будут продолжать замещать софт, и им потребуется альтернатива. Прежде всего речь идет об обеспечении бесперебойного производства, предиктивной аналитике в рамках технического обслуживания и ремонта и машинном обучении.

Международные перспективы

В 2025 году многие российские IT-компании хотели закрепиться на рынках Азии, Африки и Ближнего Востока. Пока нельзя однозначно говорить, что какой-либо отечественный вендор или интегратор заняли значительную часть рынка в той или иной стране. Скорее речь идет о локальных проектах.

В то же время в следующем году можно ожидать, что российские IT-компании будут предпринимать больше попыток выйти на международные рынки, работать с развивающимися странами с существенным потенциалом для экономического роста. Спрос на наши технологии есть. Более того, уже есть и удачные кейсы, когда компании, которые разработали прикладные продукты, успешно работают в Азии, несмотря на высокую конкуренцию.

Инвестиции в IT: деньги есть, вложений меньше

Пока индекс российского фондового рынка не будет расти, объемы инвестиций (в том числе и в IT), а также стоимость публичных компаний будут либо снижаться, либо оставаться на том же уровне. Что касается венчурных инвестиций, то в 2026 году они, скорее всего, тоже сократятся. По оценкам экспертов, доля IT-проектов в общем количестве венчурных сделок и стартапов ежегодно снижается на 5%.

Конечно, отдельные игроки продолжат инвестировать в IT-стартапы, строить свои экосистемы, но это крайне небольшая часть венчурных сделок. Следует также отметить, что значительного дефицита капитала у частных инвесторов нет, однако в текущей экономической ситуации большинство из них предпочитают не рисковать.

Чего ждать в 2026 году

В целом спрос на все классы решений и IT-продукты в 2026 году останется устойчивым, однако на рынке становится меньше денег, что приведет к дальнейшему снижению темпов роста. Также с учетом нововведений в налоговом законодательстве и инфляции цены на IT-продукты и услуги будут расти — в большинстве случаев IT-проекты станут дороже на 20%. Некоторые игроки рынка уже публично заявляли, что стоимость их продуктов вырастет на 35–40%, но здесь возникает риск, что многие клиенты просто не смогут покупать эти продукты по такой цене.

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

Дополнительным драйвером для рынка может послужить новая волна импортозамещения ПО в случае ужесточения требований, касающихся, например, КИИ или появления новых отраслевых стандартов. Также сохранится спрос на повышение эффективности производства и бизнеса с помощью IT-инструментов.
При этом продолжат расти требования к IT-проектам. По нашей оценке, все больше заказчиков ориентируются не просто на автоматизацию производственных и бизнес-процессов, а на бизнес-трансформацию, понятный ROI, измеряемый и быстрый результат. Количество проектов, где заказчик и IT-партнер отталкиваются от бизнес-целей, а уже затем разрабатывают IT-архитектуру, будет только расти. Бизнес будет более внимательно оценивать окупаемость вложений, уделять больше внимания эффективности всех операционных затрат. Это приведет к частичному оздоровлению рынка: повысится качество IT-продуктов и услуг, а подходы заказчиков к IT-проектам станут более зрелыми. (РБК.Отрасли 12.12.25)

К СОДЕРЖАНИЮ

Почему больше не стоит откладывать вопросы модернизации ИТ-инфраструктуры, и какие тренды будут влиять на рынок ЦОД в 2026. "IT Channel News". 15 декабря 2025

В реалиях современного ИТ-рынка инфраструктура ЦОД — это не только про "стройку", инженерные решения, поставку оборудования и ПО, но и различные интеграционные и сервисные проекты любого уровня сложности. В этой статье рассказываем, какие тренды существуют на российском и зарубежных рынках, как происходит взаимодействие с ключевыми российскими разработчиками программного и аппаратного обеспечения, а также представляем опыт, полученный в рамках реализованных проектов в ICL Services.

Современная "перестройка" рынка

С появлением первых санкций и ограничений ключевых зарубежных производителей оборудования, ОС, системного и прикладного ПО ИТ-рынок России не просто существенно перестроился. Самое главное — появилась возможность долгосрочного планирования развития давно не обновляемой ИТ-инфраструктуры компаний.
Еще несколько лет назад перед бизнесом стоял вопрос не обновления, а выживания и поддержания работоспособности имеющейся инфраструктуры, так как некоторое время еще была надежда на "возвращение" привычных вендоров. Действительно, большинство компаний заморозили все инвестиционные проекты с длинным циклом окупаемости. Но сегодня, по прошествии четырех лет, можно выделить большое число успешных проектов, реализованных как по перевыстроенным каналам "параллельного импорта", так и с использованием отечественных аппаратных и программных решений.
Стоит вспомнить, что тема импортозамещения для компаний с госучастием началась не 4, а примерно 10 лет назад — и сегодня нельзя не замечать основной тренд: независимо от геополитической ситуации в будущем государство продолжит быть главным регулятором ИТ-рынка в России. Во многом это означает, что возвращение иностранных вендоров будет осложнено как регулированием со стороны государства, так и технической интеграцией с массово внедряемыми отечественными продуктами и решениями. Это не только позволит поддержать российских разработчиков, но и дополнительно сместит фокус на технологический суверенитет и информационную безопасность.
Для государственных организаций актуальность вопросов импортозамещения останется до 2030 года: на основании обзоров российского рынка инфраструктурного ПО, именно к этому времени ожидается достижение порога замещения до 90% с текущих ~50-60%. По коммерческим структурам уровень проникновения отечественных решений будет скромнее — как ожидается, с 18% в 2026-м до 48% в 2030 году.

Полагаться исключительно на зарубежные решения может быть опасно

Как уже было сказано, не стоит ждать возвращения международных ИТ-компаний, а нужно рассматривать имеющиеся альтернативы здесь и сейчас. Но выбор здесь не всегда очевиден (особенно для нерегулируемых отраслей), совмещен с рядом компромиссов и часто сопровождается необходимостью привлечения серьезных своих или внешних компетенций, чтобы не наступить на "разбросанные грабли".
По данным отраслевой аналитики, объемы закупок серверов в России за 2 года снизились на 10–15%, при этом средняя стоимость выросла почти на треть. Так формируется отложенный спрос — бизнес вынужден будет обновлять инфраструктуру, даже если сейчас тянет до последнего. А таких примеров действительно много. И те, кто заранее подготовились к этой волне, смогут занять лидирующие позиции, когда спрос снова вспыхнет.
Продолжать работать на старом оборудовании становится опасно. На это есть несколько объективных причин:
технический риск: серверы и СХД теряют производительность относительно непрерывного развития технологий, становятся несовместимыми с современными системами и обновлениями, да и просто становятся экономически менее привлекательными в сравнении TCO обновленных решений;
риск безопасности: уязвимости "нулевого дня" в железе и прошивках остаются без патчей — а значит, критичные сервисы могут быть выведены из строя в любой момент;
риск бизнес-простоев: оборудование может отказать, когда найти замену или совместимый модуль уже либо невозможно, либо слишком долго.

Компетенции интеграторов и производителей только растут

К 2025 году в России сформировался собственный рынок производителей ИТ-оборудования. ICL Техно, Yadro, "Гравитон" и другие разработчики доказали, что отечественные решения могут конкурировать по производительности и надежности, а главное — обеспечивать технологическую независимость. Эти компании обеспечивают полный цикл производства — от проектирования плат до выпуска готовых систем, сертифицированных в реестре отечественного ПО и техники.

Конечно, корпоративный заказчик может собрать современный ЦОД на российских ИТ-решениях с качественным сервисом, поддержкой искусственного интеллекта, облачных технологий и гибридных нагрузок. Или же по каналам ПИ достать самые современные и технологичные зарубежные решения.

Но сделать это самостоятельно трудно: выбор решений огромен, а ответственность за интеграцию колоссальная. Без хорошей ориентации в реальных, а не маркетинговых спецификациях решений, без опыта обеспечения совместимости и знаний трендов в мировой ИТ-индустрии конфигурация может получиться заметно неоптимальной по цене в сравнении с альтернативами, а сроки доставки — неприлично долгими.

Несколько важных наблюдений:

Далеко не все российские серверные платформы протестированы на гарантированную совместимость работы с мощными NVidia-картами и GPU-вычислениями для работы с ИИ, взрывной рост которого наблюдается с 2024 года и продолжает набирать обороты. Часть функционала может быть лицензируемой и недоступной для приобретения по стандартным каналам.

Вслед за ограниченной доступностью чипов для памяти DDR5 наблюдается взрывной рост цены (более 200% в 2025 году, и ожидается продолжение этого тренда), что отражается на нестабильности цен на серверы на актуальных 4+ поколениях процессоров.

Топовые отечественные решения для хранения данных (СХД) только начинают приближаться к возможностям средних/крупных решений зарубежных аналогов.

TCO очень часто идет не в пользу отечественных решений.

К 2025 году российские производители ИТ-оборудования доказали, что отечественные платформы способны закрывать корпоративные требования по производительности и надежности, обеспечивая технологическую независимость. На фоне ограниченной доступности зарубежных компонентов ключевые элементы современных серверных систем будут продолжать дорожать и в следующем году, что только ускоряет переход бизнеса на локальные решения и делает вопрос грамотного выбора архитектуры критичным.

При этом импортозамещение касается не только "железа". В сегменте инфраструктурного ПО по мнению экспертов уже сложилась устойчивая тройка лидеров: "Группа Астра", "Ред Софт" и "Базальт СПО" — на них приходится около 98% рынка среди российских разработчиков ОС для серверов и рабочих станций. А вот оценка доли импортного ПО скорее невозможна из-за особенностей учета — по существу, публичных данных просто нет.

Но даже при таком росте локальных платформ остаются сложности в практической эксплуатации. Интеграция продуктов все еще требует глубоких компетенций, а стыковка с внешними сервисами нередко упирается в необходимость тонкой настройки, доработок и написания скриптов на Bash и Python.

Поэтому спрос на мультискилловых администраторов и опытные интеграционные команды будет только усиливаться: именно они обеспечивают полноценную замену и обновление зарубежных решений, а не просто формальное соответствие требованиям импортозамещения.

Хорошие ИТ-специалисты продолжат дорожать

Все это неминуемо приведет к перестройке и необходимости наращивания экспертиз собственных инсорс-команд. Количество технологий будет только разрастаться, и качественные специалисты станут еще дороже. А уже запланированное снижение льгот для ИТ компаний приведет к увеличению стоимости и привлекаемых специалистов из специализированных компаний.

Поэтому логичен и уже заметен повышенный фокус заказчиков на платформенные решения, способные облегчить жизнь ключевым специалистам. Здесь преобладают платформы контейнеризации (Dockers&Kubernetes), показывающие стабильный рост более 23% от года к году, а в 2024 году рынок решений для контейнеризации вырос на примерно 82% в связи с восстановлением после спада в 2022 г. и стадией активного развития технологий и DevOps практик. Если смотреть на мировой рынок контейнеризации, то уже в этом году он сравнялся с рынком виртуализации и продолжит обгонять его с двукратной интенсивностью.

Рынок решений для администрирования инфраструктуры вырос на 24% в 2024 году, показывая максимальный уровень роста с 2021. Рынок виртуализации стабильно растет до 13% в год и переходит к прямой конкуренции между ведущими российскими вендорами. Рынок СУБД опережает базовые прогнозы роста на 15% (рост на 35%) и т. д. И снова заметен повышенный интерес к экосистемным и глубоко интегрируемых между собой продуктов, которые имеют поддержку и находятся в постоянной доработке российскими вендорами — как в плане совместимости и безопасности, так и в части нового функционала и оптимизаций.

И здесь нет ничего удивительного: в мире все так быстро меняется, что скорость разработки и внедрения новых сервисов становится критическим фактором успеха, а использование всех возможностей применения автоматизации и помощи искусственного интеллекта — жизненной необходимостью.

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Платформенные решения исключают необходимость поиска совместимости продуктов между собой, так как уже являются готовой инфраструктурой, которую легко масштабировать под изменение размера бизнеса. Это позволяет компаниям сфокусироваться на стратегических бизнес-задачах, а не на технических нюансах.

Что нас ждет в ближайшее время

В 2026-2027 годах выигрывать будут те компании, которые уже сегодня осознанно перестраивают свои ИТ-ландшафты. Задержки в обновлении инфраструктуры больше не работают — слишком высоки риски, слишком быстро меняется рынок, растут требования к ИБ и производительности.

Российские производители создали зрелую экосистему решений, а рынок на фоне большого числа успешных проектов наконец получил возможность двигаться стратегически. Но даже при расширяющихся возможностях выбор "правильного" набора технологий становится все сложнее: цена ошибки растет вместе со стоимостью компонентов и скоростью изменений.

Поэтому грамотная модернизация сегодня — это не разовая закупка, а выверенная стратегия, в которой учитываются совместимость аппаратных платформ, специфика ПО, перспективы развития бизнеса, требования к ИБ и нагрузкам, а также реалии российского рынка. И как показывает практика, именно интеграционная экспертиза позволяет собрать из доступных решений оптимальную, устойчивую и экономически оправданную конфигурацию. (IT Channel News 15.12.25)

К СОДЕРЖАНИЮ

Региональные новости ИТ-компаний

ГД разрешит Москве использовать ИИ для выявления нарушений в благоустройстве.

В случае принятия поправки вступят в силу с 1 января 2026 года

Депутаты Госдумы приняли во втором чтении проект закона, который предусматривает проведение в Москве эксперимента по использованию средств автоматической фиксации, а также технологий искусственного интеллекта для выявления нарушений в сфере благоустройства и городского хозяйства.

Законопроект был внесен в Госдуму в апреле 2025 года Мосгордумой и принят в первом чтении 22 июля. Инициатива вносит изменения в закон о статусе столицы РФ. В проекте указано, что с 1 января 2026 года по 31 декабря 2028 года проводится эксперимент, в рамках которого власти Москвы смогут применять технические и программные средства для выявлений административных нарушений в сфере государственной охраны объектов культурного наследия, в строительном надзоре, экологическом и геологическом контроле, а также в надзоре на автотранспорте, городском наземном транспорте, в дорожном хозяйстве, в сфере защиты зеленых насаждений и благоустройства.

В пояснительной записке указано, что к таким средствам относятся камеры городской системы видеонаблюдения, камеры на автомобилях и беспилотных летательных аппаратах, а также иные виды средств, имеющих функции аудиозаписи, обнаружения, распознавания, анализа и идентификации объектов. К ним относятся в том числе комплексы нейронных сетей, сигнальные датчики, лазерная система измерения LIDAR, инфракрасная спектрометрия, контрольно-измерительные пункты массы.

В случае принятия поправки вступят в силу с 1 января 2026 года. (ТАСС 09.12.25)

К СОДЕРЖАНИЮ

Мэр Москвы Сергей Собянин: В Москве создана уникальная система поддержки для отрасли робототехники.

В числе мер поддержки — льготы по кредитованию, налогам и таможенным пошлинам, а также система грантов, стажировок и обучения специалистов.

Разработка и производство роботов — одна из самых перспективных отраслей, развитие которой во многом определит облик московской промышленности в ближайшие десятилетия. Сегодня в этой сфере работают около 25 компаний, которые производят роботов, занятых в промышленности, сельском хозяйстве, в складских и спасательных операциях и на других работах. О том, как город помогает развитию отрасли, Сергей Собянин рассказал в своем блоге.

"Правительство Москвы предлагает компаниям-разработчикам комплексную систему поддержки, включающую как финансовые, так и нефинансовые инструменты. В частности, Московский фонд поддержки промышленности и предпринимательства компенсирует до 50 процентов ключевой ставки Центрального банка по инвестиционным кредитам на сумму до пяти миллиардов рублей", — написал Мэр Москвы.

Кроме того, до 70 процентов кредитных средств компенсирует Московский гарантийный фонд. А на платформе Московского инновационного кластера i.moscow можно получить грант до 30 миллионов рублей на приобретение оборудования, лизинг или компенсацию уплаченных процентов.

Важную роль в развитии отрасли робототехники играет особая экономическая зона (ОЭЗ) "Технополис Москва".

Компании-резиденты могут существенно снизить налоговую нагрузку. Так, они на 10 лет освобождаются от уплаты налога на имущество, землю и транспорт, платят всего два процента налога на прибыль вместо 25 процентов, а также освобождены от таможенных пошлин и НДС при ввозе оборудования.

Кроме того, ОЭЗ "Технополис Москва" — площадка для подготовки кадров. С прошлого года на площадке "Руднево" работает флагманский центр практической подготовки колледжей, где по промышленным специальностям обучаются более трех тысяч студентов ежегодно.

Осенью в "Печатниках" начал работу центр практического обучения "Профессии будущего", где взрослые могут освоить востребованную профессию, а студенты колледжей — пройти учебную и производственную практику. Ежегодно центр будет выпускать 15 тысяч квалифицированных специалистов.

Молодые специалисты также могут пройти практику на ведущих предприятиях в рамках проекта "Техностажировка" — получить реальные навыки в высокотехнологичных отраслях промышленности, в том числе разработке и производстве роботов. С 2022 года в программе приняли участие 3,2 тысячи человек.

В мае этого года в ОЭЗ "Технополис Москва" открылся робоцентр компании "Технорэд". Предприятие выпускает промышленных роботов, роботизированные системы и соответствующее программное обеспечение. Решения используют для автоматизации ряда основных производственных операций, среди которых сварка, палетирование, укладка, загрузка станков и другие. К 2030 году резидент планирует выпустить не менее 25 тысяч роботов. Устройства уже поставляются на предприятия Москвы и десятков других городов по всей России.

Недавно компания запатентовала устройство, которое автоматизирует нажатие кнопок на панели управления. Это решение позволяет клиентам компании повысить эффективность производства, снизить влияние человеческого фактора, а также выполнять монотонные и повторяющиеся операции без участия персонала.

Технопарки: современные производства и разработка роботов

Для масштабирования производства в столице создана сеть технопарков. Они предоставляют компаниям современную инфраструктуру и доступ к мерам поддержки: налоговым льготам, грантам, субсидиям, а также консультациям и обучающим программам.

Сегодня в Москве работает 49 технопарков. Их резиденты могут воспользоваться мерами поддержки Московского инновационного кластера. Управляющие компании и якорные резиденты имеют право на инвестиционный налоговый вычет. Им возмещается до 90 процентов расходов на оснащение производственной площадки оборудованием за счет региональной части налога на прибыль (13,5 процента).

Недавно в технопарке "Мосгормаш" компания "Робопро" освоила выпуск коллаборативных роботов, которые используются для автоматизации рутинных производственных задач. Ежегодно планируется выпускать более тысячи единиц оборудования, а к 2030-му — до пяти тысяч роботов в год.

Еще один резидент технопарка "Мосгормаш", компания "Арипикс Роботикс", специализируется на создании роботизированных технических комплексов и программного обеспечения, сокращающих долю ручного труда. Например, по заказу холдинга "Объединенные кондитеры" был создан роботизированный комплекс для укладки печенья. За одну смену он упаковывает до 42 тысяч изделий — почти вдвое больше, чем может сделать бригада из 12 человек.

На пищевых производствах успешно используют и другие разработки этой компании, в том числе автоматическую линию для укладки чайных пакетиков. Ее важное преимущество в том, что система справляется с большим ассортиментом. Например, она может раскладывать до 15 разных видов чая.

Предприятие "Битроботикс", резидент технопарка "Элма-Семеновский", создает высокотехнологичное оборудование и комплексные решения для автоматизации процессов в пищевой промышленности. Среди разработок — ватрушкомат — роботизированный комплекс для производства ватрушек. Робот-манипулятор фотографирует заготовки теста на противне, точно определяет центр (с погрешностью не больше миллиметра), формирует ватрушку, наносит яичную смесь и добавляет творожную начинку — дозировка при этом контролируется с точностью до грамма. Скорость работы — 18 ватрушек в минуту. Сейчас этот робот трудится на кондитерско-булочном комбинате "Черемушки".

Резидент "Сколкова" компания "Невлабс" также производит роботов для пищевой промышленности. Предприятие реализовало поставку около 50 единиц этого оборудования. Среди покупателей — крупнейший производитель продукции из рыбы и морепродуктов "Меридиан". Роботы помогают укладывать продукцию в первичную и вторичную упаковку. Производительность достигает 150 укладываемых объектов в минуту. Один робот может заменить до четырех человек.

Компания Ronavi Robotics, входящая в группу "Роснано", внедряет свои роботизированные решения в разных отраслях — от складской логистики до автопрома. На своем складе "Восток-Сервис" в Раменском предприятие запустило флот из 48 мобильных роботов, объединенных интеллектуальной системой управления. В результате комплектация штучных заказов стала в пять раз быстрее.

В автомобильной промышленности решения компании помогли автоматизировать перевозку деталей между сборочным конвейером и покрасочным цехом. При этом не потребовалось перестраивать инфраструктуру: робот сам прокладывает маршрут, объезжает препятствия и возвращается на базу после выполнения задания.

Роботы компании Robotic Management Systems (также входит в группу "Роснано") берут на себя рутинные задачи по транспортировке грузов, а интеллектуальное программное обеспечение оптимизирует маршрут. Командой было реализовано более 10 масштабных проектов, свыше 100 роботов различных моделей уже работают на складах заказчиков.

Компания стала призером престижного конкурса "Новатор Москвы", ежегодной награды для тех, кто придумывает и внедряет новые технологии, создает новую технику, приборы, оборудование или материалы для самых различных отраслей городской экономики

Компания "Деморобот" разрабатывает и производит демонтажных роботов. Техника зарекомендовала себя при строительстве метро, реконструкции школ, поликлиник, больниц, гостиниц, спортивных объектов и торговых центров. Главные преимущества роботов — электропривод, небольшой вес и компактные размеры. Благодаря этим характеристикам их удобно использовать для демонтажа внутри зданий. Один робот способен заменить одну или несколько бригад рабочих, которые обычно используют ручные перфораторы и отбойные молотки.

От метростроения до подводных исследований

Группа компаний "Прикладная робототехника" создает и поставляет манипуляционных роботов на различные предприятия — от автопрома и производства электроники до фармацевтической и химической отраслей.

Например, столичная компания "Станкин-инновация" использует манипуляторы в составе многофункциональных роботизированных комплексов для судостроения и ряда других отраслей промышленности. Решения

INFOLine информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

продемонстрировали высокую эффективность, например окрасочных операций, и позволят значительно сократить сроки и стоимость работ, а также получить высокое качество при строительстве судов.
Разработки компании находят применение и в пищевой промышленности. Одно из предприятий отрасли — компания "Айскейк-эко" — закупило робота-упаковщика для мороженого. Аппарат справляется с работой, которую раньше выполняли четыре специалиста.
Разработка компании "Прометей" представляет собой универсальный робототехнический комплекс для проведения подводных исследований. Аппарат имеет модульную конструкцию, адаптируемую под любые задачи — от обследований дна водоемов, подводных газо- и нефтепроводов до мониторинга работы гидроэлектростанций. Он также может использоваться при строительстве подводных объектов. Разработка аппарата была проведена при поддержке "Академии инноваторов — флагманской программы АНО "Развитие человеческого капитала" по развитию молодежного предпринимательства и запуску стартапов. В ходе акселерации команда проекта оформила три патента и провела успешные пилотные испытания продукции в Московской области и Волгограде.
Разработчики из компании ABA Robotics создали роботизированный киоск, который готовит до 140 бургеров в час, занимая всего один квадратный метр. Команда прошла акселерацию, готовится к пилотным испытаниям и ведет переговоры с крупными ретейлерами.
В числе решений, созданных командой Astramis, — робот для лазерного выжигания сорняков, дрон для мойки фасадов и автономный уборщик производств. Сейчас команда проходит акселерацию в рамках седьмого потока "Академии инноваторов", а дрон для мойки фасадов готовится к пилотному тестированию.
Среди участников Московского инновационного кластера — ООО "Управление демонтажных роботов". Роботы, разработанные компанией, приходят на помощь специалистам при строительстве технических помещений, коллекторов и вентиляционных тоннелей, а также способны выдерживать высокие нагрузки и функционировать в тяжелых условиях без поломок и деформаций при проведении буровых работ. Решения успешно применяются на цементных и металлургических заводах, строительных площадках, подходят для целей атомной промышленности и горной добычи. Благодаря своей компактности они незаменимы при строительстве линий метрополитена, а ювелирная точность работы позволяет использовать их в процессе реконструкции исторически значимых объектов.
"Роботы "Сделано в Москве" помогают компаниям идти наравне и даже опережать конкурентов", — отметил Сергей Собянин.

Для справки: Название компании: *Особая экономическая зона Технополис Москва, АО (ОЭЗ Технополис Москва, ИНН 7735143008)* Адрес: *109316, Россия, Москва, Волгоградский пр-т, 42, к. 13* Телефоны: *+74956470818* E-Mail: *office@technomoscow.ru* Web: *https://technomoscow.ru* Руководитель: *Дегтев Геннадий Валентинович, генеральный директор*

Для справки: Название компании: *Технорэд, ООО (TECHNORED)* Адрес: *123007, Россия, Москва, 2-й Хорошёвский проезд, 7 стр. 1* Телефоны: *+7(800)7755271* E-Mail: *sales@technored.ru* Web: *https://technored.ru/* Руководитель: *Лукин Артём Владимирович, генеральный директор*

Для справки: Название компании: *Технопарк Мосгормаш (УК-НПО Мосгормаш, ГУП)* Адрес: *115201, Россия, Москва, Каширский проезд, 13* Телефоны: *+7(499)9515059* E-Mail: *info@tpmgm.ru; office@tpmgm.ru* Web: *http://tpmgm.ru* Руководитель: *Морозов Юрий Александрович, генеральный директор* (Сайт правительства Москвы 12.12.25)

К СОДЕРЖАНИЮ

ИТ-компании Краснодарского края за пять лет увеличили выручку почти в 4 раза.

Проблемы и перспективы развития отрасли обсудили на встрече с ИТ-сообществом, которую провел вице-губернатор Александр Руппель.
Участие в мероприятии также приняли специалисты краевых департаментамента информатизации и связи, департамента развития бизнеса и внешнеэкономической деятельности, сотрудники местных ИТ-компаний, представители Ассоциации цифрового развития региона, ведущих вузов и организаций поддержки бизнеса.
– Краснодарский край – один из регионов-лидеров по темпам цифровой трансформации. Сегодня у нас работают больше двух тысяч организаций, где трудятся свыше 18,5 тысячи человек – это практически вдвое больше, по сравнению с 2019 годом. На Кубани развернута обширная инфраструктура содействия бизнесу, реализован комплекс федеральных и региональных мер поддержки. Однако развитие реального сектора экономики невозможно без инноваций. Уверен, что объединение усилий государства, бизнеса и научного сообщества позволит нам достичь самых амбициозных целей и вывести цифровизацию всех отраслей экономики Кубани на новый уровень, – отметил Александр Руппель.
Одним из ключевых вопросов встречи стали меры государственной поддержки ИТ-отрасли Кубани.
– О том, насколько продукция наших ИТ-компаний востребована на рынке, говорит их выручка. За пять лет она выросла почти в 4 раза. Так рост налоговых поступлений от сферы информатизации и связи за 2019-2024 годы

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

составил 60 процентов, а объем инвестиций увеличился в 1,2 раза. Это стало возможным благодаря, в том числе, реализуемым федеральным и региональным мерам поддержки, – отметил и. о. руководителя департамента информатизации и связи Краснодарского края Станислав Завальный.

На Кубани с 2022 года ввели инвестиционный налоговый вычет в размере 70%, благодаря которому ИТ-бизнес смог сэкономить 621,2 млн рублей за три года. Эти средства направят на развитие компаний, включая расширение и модернизацию.

С 2025 года на Кубани запустили новую кадровую меру поддержки: для аккредитованных предприятий ИТ-сферы предусмотрена субсидия на возмещение половины НДФЛ за своих сотрудников. Выделенные средства можно использовать как на поощрение работников и улучшение условий труда, так и на общее развитие компании.

Для успешного развития отрасли необходима и адаптация образовательной системы к современным требованиям. В ходе дискуссии участники подробно рассмотрели взаимодействие образовательных учреждений с потенциальными работодателями. Совместные проекты позволят студентам приобретать востребованные практические навыки и станут залогом их конкурентоспособности на рынке труда.

– В 2026 году Центр искусственного интеллекта КубГУ примет порядка 160 студентов. Мы заинтересованы в привлечении ИТ-организаций региона в качестве индустриальных партнеров, которые будут участвовать в образовательном процессе, предоставлять практические задачи и служить базой для стажировок. В дальнейшем мы надеемся на их помощь нашим выпускникам в трудоустройстве, – отметил ведущий научный сотрудник Института математики, механики и информатики Кубанского государственного университета Артем Еремин. (INFOLine, ИА (по материалам Администрации Краснодарского края) 10.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Отраслевые мероприятия

В Ульяновске открылся технологический форум по развитию станкостроения и робототехники.

Мероприятие, посвященное развитию станкоинструментальной отрасли и промышленной робототехники, состоялось 10 декабря на площадке Ульяновского станкостроительного завода.

Событие собрало более 130 участников, включая представителей органов власти, ведущих промышленных предприятий, научного сообщества и отраслевых объединений из 19 регионов России. Ключевыми темами обсуждения стали импортонезависимость, технологический суверенитет и практические инструменты модернизации производства.

"Сегодня станкостроение и робототехника – это основа технологического суверенитета страны, залог устойчивого развития реального сектора экономики. Мы инициировали создание станкостроительного кластера в нашем регионе и делаем серьезную ставку на его развитие. Объединение усилий ведущих предприятий – это необходимая нам синергия между наукой, образованием и производством. Наш регион обладает богатейшей историей и традициями в станкостроении. И ключевая задача сегодняшнего дня – увеличить долю отечественной продукции и обеспечить технологическую независимость. Это амбициозная, но достижимая цель, и мы работаем над её реализацией. Уверен, что форум станет продуктивной площадкой для диалога, обмена опытом и формирования конкретных проектов в области автоматизации и модернизации производства", — сказал губернатор Ульяновской области Алексей Русских.

Форум стал площадкой для диалога между производителями станков и инструментов, интеграторами робототехники, разработчиками цифровых решений и представителями власти. В фокусе обсуждения — практические технологии, обмен опытом и формирование совместных проектов в области модернизации и автоматизации производства. Участники обсудили задачи в рамках национального проекта "Средства производства и автоматизации", в частности увеличение доли отечественной станкоинструментальной продукции на внутреннем рынке до 60% к 2030 году и достижение технологической независимости в производстве высокотехнологичных станков на уровне 95%.

Одним из ключевых результатов развития отрасли в регионе стало создание промышленного станкостроительного кластера, в который вошли пять предприятий: ООО "Ульяновский станкостроительный завод", ООО "Завод тяжелых станков Ульяновск", АО "ФРЕСТ", ООО "ТПК Легато" и ООО "ПасКом".

Предприятия кластера демонстрируют уверенный рост: на базе Ульяновского станкостроительного завода активно развивается инженерная школа, внедряются современные системы ЧПУ, включая отечественные разработки. К 2030 году завод планирует выпускать до 250 станков в год. Предприятия ООО "Завод тяжелых станков Ульяновск", АО "ФРЕСТ" и ООО СК "УЗТС" переходят от ремонта и модернизации тяжелых станков к производству современных станков собственной разработки.

Развитие отрасли в Ульяновской области поддерживается в том числе и льготными кредитными программами от Фонда развития промышленности, что дает предприятиям необходимые инструменты для технологического рывка и укрепления промышленного потенциала страны.

Для справки: Название компании: *Ульяновский станкостроительный завод, ООО* Адрес: *433400, Россия, Ульяновская область, Ульяновск, ул. ДМГ МОРИ, 1* Телефоны: *+7(8422)590650; +7(800)7007409* Факсы: *+7(8422)590651* E-Mail: *service.russia@dmgmori.com; info@dmgmori.com* Web: *http://ru.dmgmori.com* Руководитель: *Антипин Алексей Павлович, генеральный директор* (Газета Ульяновская правда 10.12.25)

К СОДЕРЖАНИЮ

Конференция Data Fusion 2026 состоится 8–9 апреля в Москве.

Шестая ежегодная конференция Data Fusion пройдет в Москве 8–9 апреля 2026 года. Мероприятие станет кросс-индустриальной площадкой для диалога бизнеса, науки и государства в области работы с данными и развития технологий ИИ."Технологии искусственного интеллекта сегодня определяют динамику развития многих отраслей. Это предъявляет новые требования к специалистам, компаниям и государственным структурам: критически важной становится скорость внедрения и масштабирования решений. От того, насколько эффективно мы будем развивать компетенции и инфраструктуру, зависят позиции страны на глобальной технологической карте. Именно этому мы посвятим обсуждения на Data Fusion — бизнесу, научному сообществу и государству предстоит выработать наиболее продуктивный подход к развитию ИИ и технологий работы с данными", — сообщил Вадим Кулик, заместитель президента — председателя правления ВТБ.

Программа конференции включает более 60 сессий, посвященных экономике данных, внедрению и масштабированию ИИ-решений в разных индустриях, обсуждению лучших международных практик в области искусственного интеллекта, а также совершенствованию наукоемких технологий.

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

В дни конференции также состоится церемония вручения премии Data Fusion Awards, направленной на продвижение технологий работы с данными и ИИ. Коммерческие компании, научные и образовательные учреждения, государственные организации, а также авторы научных исследований могут подать заявки до 20 января 2026 года на сайте премии.

Научная повестка традиционно занимает важное место на Data Fusion. В 2025 году исследователи и эксперты обсуждали развитие современных моделей машинного обучения, задачи масштабирования ИИ-систем, новые подходы к работе с данными. Участники рассматривали как фундаментальные научные исследования, так и практические кейсы внедрения технологий. В рамках конференции на церемонии Data Fusion Awards впервые были вручены награды в номинации "Научный прорыв года в искусственном интеллекте", общий призовой фонд составил 3 млн рублей. Награды присуждались за научные статьи российских ученых в области искусственного интеллекта, опубликованные в журналах или материалах конференций в 2024 году.

В 2026 году внимание к научным вопросам сохранится — в программу войдут дискуссии о ключевых направлениях развития ИИ и инфраструктуры данных.

В 2025 году конференцию Data Fusion посетили свыше 2700 человек. На сессиях выступили более 300 спикеров, среди которых Председатель Правительства России Михаил Мишустин, заместитель Председателя Правительства РФ Дмитрий Григоренко, председатель Центрального Банка РФ Эльвира Набиуллина, министр цифрового развития, связи и массовых коммуникаций РФ Максут Шадаев.

Конференция состоится в Инновационном кластере "Ломоносов". О старте регистрации участников будет объявлено дополнительно. (Волга Ньюс 12.12.25)

К СОДЕРЖАНИЮ

Информационно-аналитические системы

В опережающем темпе и своим путем: развитие российских платформ low-code. "ItWeek". 15 декабря 2025

Low-code стала одной из немногих продуктовых ниш информационных технологий, где Россия не догоняет, а формирует собственные стандарты. Low-code продукты появились в ответ на потребность бизнеса быстро создавать цифровые решения без сложной разработки. Рассмотрим, почему так происходит, в чем преимущества и недостатки российского low-code по сравнению с западным.

Созревание бизнеса

По данным Высшей школы бизнеса НИУ ВШЭ, 21,6% российских компаний уже используют low-code и no-code продукты. Еще 42,3% из них планируют внедрение, 36% изучают возможности. В данных цифрах видится не просто рост интереса со стороны заказчиков, но и перспектива смены подхода к ИТ. С одной стороны, компании ищут способ работать быстрее и дешевле, с другой — дефицит разработчиков и уход зарубежных поставщиков усиливают спрос на локальные инструменты.

В 2021 году доля иностранных решений low-code превышала 60%. Сегодня она не выше 5%. За три года отечественные игроки вывели зрелые продукты и заняли рынок, сделав ставку на практику, а не на копирование зарубежных решений. Отечественные разработчики тесно работают с заказчиками, собирают обратную связь, быстро исправляют слабые места.

В итоге отечественные low-code продукты стали гибче, получили шаблоны, встроенную аналитику и поддержку ИИ. Многие продукты поддерживают как облачное, так и локальное развертывание на инфраструктуре заказчика, что важно для критических отраслей, промышленности и госсектора. В некоторых случаях из отдельных no-code продуктов начали развиваться no-code платформы и экосистемы.

Зарождение платформ

Большинство российских решений выросло из проектов кастомной разработки. Компаниям необходимо было быстро автоматизировать процесс — например, документооборот или обработку заявок, а готового решения на рынке не было, либо оно не устраивало по важным критериям. Так появлялись внутренние инструменты, которые в некоторых случаях позже превращались в продукты и выходили на рынок.

Такая логика развития во многом и определила сегодняшний рынок. Важно понимать, что для работы с документами и таблицами выбирается одна архитектура, для клиентских сервисов — другая. Low-code продукты изначально создавались под конкретные бизнес-процессы, а не как универсальные конструкторы. Поэтому low-code продукты в России с одной стороны отличаются определённым разнообразием, а с другой стороны — несут в себе специфику и ограничения первоначально решаемой задачи. Например, некоторые продукты унаследовали тяжеловесную архитектуру от BPM- и СЭД-систем, и таких продуктов на рынке большинство.

Универсальные low-code платформы-конструкторы, создававшиеся такими изначально, находятся на рынке в абсолютном меньшинстве.

Выгоды и пробелы

Российские low-code платформы, в отличие от разрозненных продуктов, ускоряют автоматизацию и объединяют системы без необходимости поддерживать сложные интеграции и разрозненные процессы обслуживания. Появились платформы, позволяющие собирать полноценные корпоративные решения — от MVP до готового продукта. При этом на их основе создаётся всё та же функциональность, что и в случае использования изолированных продуктов: CRM, сервисы поддержки, корпоративные порталы и документооборот. Для многих компаний возможностей перечисленных решений вполне достаточно. Бонусом это дает бизнесу два ключевых преимущества — гибкость и скорость.

Есть и ограничения. Для задач с глубокой аналитикой и ИИ российские решения уступают западным. Массовых примеров промышленного применения ML пока мало. При высоких нагрузках часть систем теряет стабильность. Слабо развиты мобильные инструменты и автоматическое тестирование. Недостаток готовых модулей заставляет отечественных вендоров дорабатывать их вручную. Осложнена и прямая миграция с зарубежных решений, так как готовых отечественных решений нет в большинстве случаев. Зачастую миграция требует написания кастомного решения со стороны российского вендора.

Другие преимущества

Российские low-code продукты платформы выигрывают за счет локализации — они изначально создавались для отечественной инфраструктуры и российского законодательства. Отечественные платформы как правило соответствуют базовым требованиям 152-ФЗ, 44-ФЗ и 223-ФЗ, обеспечивают хранение данных внутри страны и зачастую внутри инфраструктуры компании, а также способны интегрироваться с государственными системами.

Независимость от санкций и зарубежных сервисов делает отечественные решения предсказуемыми по стоимости владения и распределению этой стоимости во времени. Поддержка продукта на русском языке, гибкие модели лицензирования и быстрые внедрения усиливают конкурентоспособность.

Информационная безопасность — еще один плюс. Вендоры встраивают многоуровневую защиту и контроль доступа, потому что заказчики работают с чувствительными данными. В данном случае это реальный запрос рынка, усилившийся многократно из-за влияния внешних факторов. Поскольку большинство решений применяются в госсекторе, промышленности и финансовых структурах — уровень доверия напрямую зависит от того, как выстроены процессы контроля, аудита и защиты данных.

На первом уровне действуют внутренние стандарты безопасности разработки от практик код-ревью до регулярного сканирования кода на уязвимости. Второй уровень включает внешний аудит или проведение исследований тестов на проникновение (пентестов). Второй уровень чаще всего является добровольно-сертификационным, либо чаще всего выполняется по требованию заказчика (организаций госсектора и компаний, эксплуатирующих элементы критической инфраструктуры). Третий уровень — сертификация по требованиям ФСТЭК и ФСБ и обязательное лицензирование как ключевое условие для работы в госсекторе и компаний с элементами КИ.

Контроль использования в составе решений open-source компонентов становится отдельным направлением контроля для компаний, разрабатывающих low-code продукты. Поскольку значительная часть этих продуктов опирается на открытые библиотеки и фреймворки, то вендоры внедряют собственные механизмы регулярного сканирования уязвимостей в open-source компонентах. Для этого применяются решения, интегрированные в процесс CI/CD, например, модули GitLab Security, Sonatype или SonarQube. Некоторые вендоры создают собственные разрешенные реестры open-source библиотек, что снижает риск появления неподдерживаемых или скомпрометированных компонентов.

Если стоит задача развернуть low-code решение в облачной среде, то комплекс мер защиты информации усиливается. Например, применяется дополнительное шифрование данных на всех уровнях от транспортного трафика с использованием протоколов TLS 1.2, 1.3 и до шифрования информации непосредственно в базах данных. Аутентификация реализуется через корпоративные SSO-системы с применением фильтров по IP или геолокации пользователя, а также механизмов 2FA. Многие российские low-code сервисы разворачиваются в отечественных облаках или защищенных центрах обработки данных, уже прошедших сертификацию на соответствие требованиями 152-ФЗ.

Следующий этап развития безопасности решения заключается в появлении встроенных в само решение инструментов мониторинга и анализа уязвимостей. Российские производители low-code интегрируют свои решения с SIEM-системами заказчиков, а также создают собственные ИБ-дашборды, которые позволяют отслеживать аномалии и подозрительную активность прямо в административных панелях поставляемых low-code решений. Подобная внутренняя аналитика превращает low-code не только в инструмент быстрого решения бизнес-задач, но и в элемент корпоративной системы киберзащиты.

Обеспечение высоких стандартов безопасности в отечественных low-code платформах постепенно перестает быть результатом воздействия внешних факторов и становится естественной частью жизненного цикла отечественного продукта.

Слабые места и вызовы

С 2010-х на российском рынке low-code появились десятки новых игроков. Уровень зрелости их продуктов сильно различается. Одни решения стабильно работают в Enterprise-сегменте, другие остаются нишевыми. Это препятствует стандартизации рынка.

Сохраняются архитектурные ограничения. Старые BPM- и СЭД-подходы снижают производительность и гибкость интерфейсов. При работе с большими объемами данных отечественные low-code продукты зачастую требуют дополнительных оптимизаций. Внешний аудит ИБ часто выявляет устаревшие, уже не поддерживаемые open-source компоненты в составе этих продуктов.

Однако в целом, несмотря на это, российский рынок low-code и основные отечественные его игроки постепенно движутся к системному контролю кода и внедрению единых стандартов безопасности.

Все понимают, что с одной стороны переход на отечественные low code-платформы потребует значительных усилий со стороны заказчиков. Необходимо обучать сотрудников работе с новым решением, где-то перестраивать и систематизировать бизнес-процессы. С другой стороны, данный этап неизбежно проходят компании при внедрении любого решения, как отечественного, так и зарубежного.

*** * ***

Отечественные разработчики low-code продуктов, и особенно — полноценных платформ, перестали играть роль догоняющих. На основе отечественных решений выстраиваются целые экосистемы, формируются партнерские сети. Вендоры не отстают в зрелости ИИ-инструментария, начинают формировать собственные технологические стандарты. Low-code как подход перестает быть способом просто ускорить внутреннюю разработку и становится элементом зрелого цифрового рынка, на котором главным критерием выбора становится не происхождение платформы, а способность превращать технологию в ощутимое и измеримое конкурентное преимущество. (ItWeek 15.12.25)

К СОДЕРЖАНИЮ

Облачные решения

Как российские компании перестраивают инфраструктуру под новые требования. "РосБизнесКонсалтинг". 10 декабря 2025

Директор по продукту "ТТК.Облако" Андрей Малов — о том, почему цифровизация ускорила переход бизнеса на защищенные облачные решения и как перезагрузка рынка повысила спрос на сегмент частных облаков

Уход западных вендоров, санкции и новые регуляторные требования превратились в мощный катализатор развития новых стратегий по цифровизации российских компаний. Бизнес прошел важный путь: от идеи цифровой трансформации ради эффективности к осознанию, что цифровая устойчивость — это вопрос выживания.

Сегодня компании ориентируются не на абстрактные выгоды, а на конкретные потребности защиты от реальных угроз. В первую очередь бизнес старается минимизировать операционные риски — например, остановку систем из-за недостаточно эффективной техподдержки, репутационные и финансовые потери — крупные штрафы за несоответствие требованиям регуляторов. Также важно учитывать стратегические риски, такие как технологическая зависимость от иностранного вендора.

В этих условиях изменения в IT-инфраструктуре и переход на облачные решения становятся основными инструментами управления этими угрозами. Российский рынок облаков переживает бурный рост. После 2022 года мы наблюдаем увеличение спроса на облачные сервисы, особенно на отечественные решения в этом сегменте. В 2024 году объем рынка увеличился на 32,8% к предыдущему году — до 322,3 млрд руб., по данным отчета iKS-Consulting. Согласно прогнозам экспертов, в 2025 году объем рынка увеличится на 29,2%, до 416,5 млрд руб., а к 2030 году достигнет отметки в 1,2 трлн руб. при среднегодовых темпах роста в 24,4%.

Основные игроки рынка — это национальные провайдеры на базе телеком-холдингов. Наибольший интерес к их услугам проявляют отрасли с высоким уровнем регулирования — финансовый рынок и госсектор. Их приоритетная задача — соответствие требованиям Центробанка (ЦБ) и Федеральной службы по техническому и экспортному контролю (ФСТЭК), так как они работают с критическими данными. Их утечка влечет не только репутационные риски, но и финансовые санкции от регуляторов. Также облачные сервисы востребованы для компаний в ретейле и промышленности, для которых важна бесперебойность работы и импортозамещение устаревших систем.

Один из наиболее динамичных сегментов рынка в России — инфраструктура в публичном облаке, согласно данным Apple Hills Digital. С 2022 по 2024 год его среднегодовой рост составил 29%, а спрос на услуги высокопроизводительных виртуальных машин с GPU-ускорителями (от англ. Graphics Processing Unit — графический процессор. — "РБК Отрасли") в среднем увеличивается на 39% в год. Это связано с возрастающим количеством задач в области машинного обучения, аналитики и обработки больших данных.

Также аналитики отмечают развитие частных облаков: объем их сегмента в 2024 году превысил 40 млрд руб. и составил около 12% всех типов облачных решений в России. В отличие от публичного облака, где провайдер управляет общей инфраструктурой и клиенты арендуют виртуальные мощности по принципу оплаты за потребление, частное облако предоставляет выделенные ресурсы только одной организации, в собственном или дата-центре провайдера. Это дает полный контроль над настройками, политиками безопасности и производительностью, но требует больших первоначальных инвестиций и операционных усилий.

Критериями выбора между тем или иным форматом облака сейчас прежде всего являются вопросы безопасности и соответствия нормативам регулятора. Возможность локализовать данные и пройти аудит ФСТЭК — весомое преимущество. Мы, например, руководствуемся всеми текущими требованиями российского законодательства в области обеспечения физической и информационной безопасности для облачных решений, в том числе по их криптозащите и сертификации, а также локализации персональных данных. Кроме того, мы ориентируемся на отраслевые требования, например, закона о коммерческой тайне, обработке медицинских данных и требованиях Центробанка России.

На втором месте при выборе облаков возможность контроля над инфраструктурой и ее суверенитет: гибкость и масштабируемость по-прежнему важны, но бизнес теперь ищет их в предсказуемой, контролируемой среде. Поэтому гибридная архитектура, при которой критические нагрузки остаются в частном облаке, а менее чувствительные — в отечественном публичном, постепенно становится стандартом.

Стереотип о том, что on-premise инфраструктура (модель локального развертывания программного обеспечения — "РБК Отрасли") негибка и медленна, устарел. Современные частные облака на базе российских платформ или открытых технологий, например платформ Kubernetes, Terraform, OpenStack — в связке с автоматизацией через IaC (от англ. Infrastructure as Code — подход к автоматизации и управлению инфраструктурой через использование кода, а не ручную настройку. — "РБК Отрасли") дают гибкость, сопоставимую с публичными облаками.

Ключевые метрики подтверждают это: время развертывания нового сервера сокращается до минут, а скорость "выкатки" приложений заметно увеличивается. Опыт одного из наших клиентов, крупной компании в здравоохранении, показал, что переход в частное облако с поддержкой IaC позволяет быстро перенести и развернуть критичные бизнес-приложения в безопасной инфраструктуре без потери скорости разработки и сопровождения.

Разместить частное облако "под ключ" — от инфраструктуры до безопасности, с гибкими условиями и экспертной поддержкой, можно как локально у заказчика, так и в наших ЦОД. Причем при наличии зрелых DevOps-практик и IaC миграция на защищенное частное облако проходит почти бесшовно — разработчики продолжают работать с теми же Terraform и Kubernetes и пользоваться облаком, меняется лишь бэкенд (от англ. backend — внутренний интерфейс. —"РБК Отрасли"). Основная нагрузка ложится на поставщика, который должен обеспечить соответствие требованиям безопасности и операционную надежность.

При выборе провайдера можно выделить три ключевых критерия: опыт аттестации по ФСТЭК, то есть готовое аттестованное решение с полным пакетом документов, глубокая экспертиза в информационной безопасности и портфолио референсов в определенной отрасли, а также прозрачность — готовность к внешним аудитам и детализированные SLA (от англ. Service Level Agreement — соглашение об уровне обслуживания. — "РБК Отрасли"). По сути, компания покупает не просто услугу, а партнерство в области безопасной IT-инфраструктуры.

В перспективе трех-пяти лет развитие частных и гибридных облаков сформирует прочный фундамент для новой цифровой независимости: компании получат контроль над цифровой судьбой, снизят уязвимость к внешним угрозам и смогут выстраивать собственные технологические экосистемы, повышая общую зрелость IT. Но одновременно с этим есть риск — закрытость национальных экосистем может привести к технологическому отставанию, если темпы развития внутренних решений замедлятся.

Поэтому бизнесу нужно не просто импортозамещение, а технологическое опережение — создание конкурентоспособных на мировом уровне облачных платформ, которые дадут не только защиту и суверенитет, но и инновационное преимущество. (РосБизнесКонсалтинг 10.12.25)

К СОДЕРЖАНИЮ

Как импортозамещение влияет на облачную стратегию финансового сектора. "РосБизнесКонсалтинг". 10 декабря 2025

О том, как цифровая трансформация влияет на IT-инфраструктуру финансовых компаний и какие факторы стимулируют их переходить на отечественные облачные платформы, рассказал IT-директор "Ренессанс Брокера" Азат Вафин

— Насколько цифровизация и рост спроса на IT-услуги влияют на бизнес-стратегию финансовых компаний сегодня?

— Цифровая трансформация и стремительное повышение спроса на IT-услуги уже давно перестали быть фоном — это ключевой драйвер стратегии любой финансовой организации. Сегодня практически каждый финансовый продукт, по сути, IT-услуга. Без надежной, масштабируемой и безопасной технологической платформы невозможно выпустить конкурентоспособный продукт, запустить сервис мгновенных платежей или предложить удобный инвестиционный инструмент.

Скорость и гибкость стали базовыми конкурентными преимуществами: те, кто быстрее выводит на рынок новые цифровые продукты и умеет быстро тестировать гипотезы, выигрывают. Облачные платформы в этом смысле становятся стратегическим активом: они дают возможность экспериментировать и масштабировать решения за недели, а не за месяцы.

Также сами данные превратились в стратегический актив. Финансовые компании всегда работали с массивами информации, но сегодня они стали основой для принятия всех ключевых решений — от скоринга, автоматизированной системы оценки платежеспособности заемщика и персональных предложений до управления рисками и выявления мошенничества. Стратегия компании теперь должна быть data-driven (управляемая данными. — "РБК Отрасли"), когда решения принимаются на основе данных, а не интуиции и мнений. Это требует внедрения мощных аналитических платформ и инструментов искусственного интеллекта (ИИ), которые могут работать с огромными объемами информации в реальном времени.

Наконец, цифровизация многократно увеличила уровень киберрисков, поэтому безопасность и соответствие требованиям регуляторов сегодня являются неотъемлемой частью бизнес-стратегии. Выбор партнеров, архитектура решений и управление доступом рассматриваются через призму защиты данных клиентов — доверие к компании напрямую зависит от технологической надежности.

— Как вы оцениваете текущий уровень спроса на облачные услуги для финансового сектора — какие главные изменения и тренды заметны за последние два-три года?

— После 2022 года спрос на облачные услуги в финансовом секторе претерпел качественные изменения: облако из инструмента для тестирования и вспомогательных задач превратилось в стратегический фундамент цифровой трансформации.

Сейчас мы видим несколько ключевых трендов на рынке. Первый — "суверенизация" и стремление к импортонезависимости. Соблюдение регуляторных требований по локализации данных и поддержка отечественного программного обеспечения (ПО) послужили основой для становления зрелого рынка доверенных облачных платформ.

Второй тренд — переход к датацентричным сервисам. Банки и брокеры осознали, что главный актив — это данные, поэтому растет спрос не просто на виртуальные машины, а на управляемые сервисы для хранения и обработки данных.

Третий — интеграция искусственного интеллекта и машинного обучения (ML) в продуктовую воронку. Облако стало полигоном для перехода от экспериментов к промышленному использованию ИИ/ ML для конкретных задач — от автоматизации call-центров с помощью NLP (от англ. Natural Language Processing — обработка естественного языка. —"РБК Отрасли") до предиктивной аналитики оттока и внутренних ИИ-ассистентов.

Помимо этого безопасность стала частью архитектуры by design, когда защита встраивается в архитектуру ПО с нуля и является неотъемлемой частью процесса разработки. Финансовые компании требуют от провайдеров встроенных механизмов защиты — шифрования данных на всех этапах, продвинутого управления доступом и готовых инструментов для соответствия отраслевым стандартам.

— В 2023 году вы перевели бэк-офис с облачной платформы Azure на Cloud.ru Advanced. Почему был выбран отечественный провайдер и какие факторы на это повлияли?

— Решение о миграции было продиктовано стратегией технологического суверенитета и необходимостью полного соответствия регуляторным требованиям. При выборе платформы мы ориентировались на четыре ключевых фактора: соответствие российскому законодательству, обеспечение бизнес-непрерывности и безопасности, технологическую зрелость платформы и экономическую эффективность.

В итоге Cloud.ru Advanced показал готовность работать с нагрузками уровня enterprise в финансовом секторе и позволил нам сохранить привычный уровень сервиса для сотрудников, одновременно гарантируя соответствие регуляторным требованиям и стратегическую независимость.

— Как изменились бизнес-процессы после перехода на облачную инфраструктуру?

— Переход на облако дал не просто технологические инструменты — он изменил сам темп принятия решений и способы работы. Мы получили принципиально другую скорость вывода продуктов на рынок: эксперименты и пилоты превращаются в рабочие решения за недели, а не месяцы.

Ключевым фактором успешной миграции стала безупречная квалификация и слаженная работа нашей команды. Это позволило реализовать переход без перестановок в команде и без обращения к внешним ресурсам на постоянной основе — основные задачи были решены силами внутренних специалистов.

— Как формируется конкурентоспособность у финансовых компаний, активно использующих облака, по сравнению с традиционными игроками?

— Конкурентное преимущество складывается из нескольких взаимосвязанных факторов. Скорость стала новым стандартом — облако позволяет сокращать TTM (от англ. time-to-market—время от идеи продукта до его выхода на рынок. —"РБК Отрасли") и быстро тестировать и масштабировать успешные решения.

Также важна экономическая эффективность: переход к OPEX (от англ. Operating Expenditure — операционные затраты компании. — "РБК Отрасли") вместо масштабных CAPEX-вложений (от англ. Capital Expenditure — капитальные затраты компании. — "РБК Отрасли"). Оплата только за фактическое потребление и эластичность ресурсов дает значительную экономию и управляемость затрат. Это снижает совокупную стоимость владения инфраструктурой и при грамотном подходе позволяет экономить до 30–40% на инфраструктурных расходах.

Кроме того, с помощью них поддерживается клиентоцентричность: облако обеспечивает бесперебойную доступность цифровых каналов и возможности для глубокой персонализации, что повышает уровень удовлетворенности клиентов.

Таким образом, финансовые организации получают не просто технологическое преимущество, а принципиально другую бизнес-модель — более гибкую, клиентоориентированную и способную к постоянной эволюции.

— Какой практический эффект вы увидели после миграции в Cloud.ru? Были ли положительные результаты?

— Для нас этот переход был стратегическим шагом, который принес конкретные результаты в трех ключевых направлениях.

Первое — это формирование стабильного и предсказуемого IT-фундамента. Провайдер Cloud.ru проявил себя как надежный партнер, предоставив отказоустойчивую инфраструктуру с понятным SLA (от англ. Service Level Agreement — соглашение об уровне обслуживания между поставщиком услуг и заказчиком. — "РБК Отрасли").

Второе — доступ к инструментам для технологического лидерства. Важно, что партнер не просто предоставляет ресурсы, а активно развивает сервисы. Третье — это, разумеется, суверенность.

— Есть ли планы по дальнейшему использованию облаков?

— Да, это одно из важных направлений развития. Мы придерживаемся стратегии использования облачных технологий там, где это дает максимальный эффект для бизнеса.

Постоянно анализируем рынок и оцениваем предложения таких партнеров на предмет новых сервисов, которые могут повысить нашу операционную эффективность или создать новое конкурентное преимущество. Проще говоря, мы открыты для всего, что делает наш бизнес более технологичным и гибким. (РосБизнесКонсалтинг 10.12.25)

К СОДЕРЖАНИЮ

В России замедлился рост рынка облачных технологий. "Деловой Петербург". 10 декабря 2025

Рост отечественного облачного рынка замедлился. Ожидается, что в 2025 году он составит 29%, тогда как в 2024 году показатель был 39%.

В конце 2024 года прогнозировался активный переход компаний к монетизации частных облаков, однако экономическая ситуация скорректировала планы, отмечают аналитики ИТ–холдинга Т1. Впрочем, даже с учётом этого замедления облака остаются одним из самых быстрорастущих ИТ–сегментов. В 2026 году, как предполагают аналитики, рост рынка продолжит замедляться и составит +27%.

Как прогнозировалось ранее консалтинговым агентством iKS–Consulting, объём российского рынка облачных услуг достигнет отметки 416,5 млрд рублей в 2025 году.

Директор по стратегии Cloud.ru Илья Королёв подчёркивает, что замедление роста рынка во многом связано с общим охлаждением экономики.

"В облаке можно быстро стартовать с новыми проектами и наращивать объёмы потребления ресурсов, поэтому экономическая активность клиентов довольно быстро отражается на спросе. Однако падения рынка мы не ожидаем, так как уровень проникновения облаков в РФ всё ещё сильно отстаёт от среднемирового уровня", — говорит он.

По словам продакт–оунера UserGate uFactor Александра Луганского, замедление роста также связано с критически высокой стоимостью денег для бизнеса. Это касается в том числе компаний уровня Enterprise, где многие инвестиционные проекты были поставлены на паузу.

Сокращения потребления инфраструктуры пока не заметно, речь именно о сокращении темпов наращивания мощностей, подчёркивает заместитель генерального директора по разработке и эксплуатации продуктов Selectel Сергей Пимков. Компании из некоторых отраслей даже значительно выросли в потреблении ресурсов за 3 квартала 2025 года. Наиболее активный рост пришёлся на клиентов Selectel из финансовой отрасли (в 2,2 раза год к году), а также медиа (в 1,8 раза год к году) и транспортного сектора (в 1,6 раза год к году).

Как отмечает CEO K2 Cloud Сергей Зинкевич, облачный рынок в России вступает в стадию естественного созревания. Первая волна массовой миграции в облако завершена. Рынок переходит от количественного расширения к этапу качественного развития с фокусом на реальную бизнес–ценность.

"Поэтому теперь компании ищут не просто инфраструктуру, а экспертизу провайдера в различных продуктовых направлениях и готовые отраслевые кейсы. Говорить о спаде не совсем корректно. Скорее происходит смена драйверов: будущий рост облаков обеспечат специализированные решения — GPU–as–a–Service, гибридные среды, кибербезопасность как сервис", — рассказывает эксперт.

С учётом многократного роста облачного рынка за последние годы со временем будет наблюдаться насыщение, что переведёт облака из быстро и бурно растущего сегмента в область стабильно растущего и зрелого бизнеса, резюмирует директор департамента облачных решений "Софтлайн Решения" (ГК Softline) Александр Андреев. (Деловой Петербург 10.12.25)

К СОДЕРЖАНИЮ

Перестройка облачного будущего. "КоммерсантЪ". 11 декабря 2025

Почему переход к гибридным архитектурам стал трендом облачного рынка

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.

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 закрепилась 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 утроится, 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 платформы 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.

"Турбо Облако" для хоккейного клуба

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 площадках 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.

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 зависеть 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 перебоями, ограничениями доступа или изменением регуляторики. Такой

подход возвращает управляемость: критичные 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 позволяют 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: критичные сервисы остаются в защищенных контурах, а аналитика, тестовые и рабочие пространства для разработки переносятся 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Минцифры и Минстрой создадут типовые IT-решения для строительства и ЖКХ. "Ведомости". 12 декабря 2025

Это поможет регионам сэкономить на закупках и в создании собственных IT-продуктов

В 2026 г. Минцифры и Минстрой планируют запустить типовые облачные решения в строительстве и ЖКХ. Об этом на парламентских слушаниях в Совете Федерации сообщил директор департамента развития сервисов и клиентского опыта Минцифры Андрей Ульянов. Речь идет о трех решениях: типовое облачное решение строительства, типовое облачное решение государственной информсистемы (ГИС) по управлению коммунальной инфраструктурой и типовое облачное решение "Умный город". Они позволят уравнять доступ регионов к современным технологиям в области строительства и ЖКХ.

"По всем трем направлениям формализуется образ целевого результата. Ожидаем старт по данным проектам в начале 2026 г.", - сообщил Ульянов. По его словам, старт проектов запланирован на следующий год.

Типовое облачное решение для строительства позволит объединить все процессы жизненного цикла проекта, пояснил Ульянов. Решение для "Умного города" позволит контролировать расходование денежных средств и получать обратную связь от населения. Решение для управления коммунальным хозяйством необходимо, чтобы организовать подготовку к отопительному сезону и наблюдать за состоянием многоквартирных домов.

Регионам типовые облачные решения позволят организовать "одинаковый подход к выполнению задач в области стройки и ЖКХ", уверен директор департамента цифрового развития Минстроя Николай Парфентьев. Сегодня цифровизация ЖКХ и строительства в регионах идет неравномерно, в основном это связано с разницей в ресурсах,

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

отметил он. "Формирование типовых облачных решений сможет снизить цифровое неравенство", - заверил чиновник. "Задача в том, чтобы тех, кто по цифровой зрелости находится чуть ниже, дотянуть до тех, кто уже такие решения реализует, не привлекая от них дополнительных средств", - подтвердил Ульянов. Он подчеркнул, что решения будут бесплатными для регионов.

Минцифры в подготовке типовых облачных решений выступает в качестве технического заказчика решения, пояснил Ульянов. Типовые облачные решения будут базироваться на Гостехе (единой цифровой платформе-конструкторе для создания ГИС). При этом сам субъект Федерации будет принимать решение о переходе на новый софт, сейчас для регионов нет обязательства использовать рекомендуемый Минцифры и Минстроем программный продукт, заверил Ульянов. Но у регионов есть запрос на это и Минцифры проводило пилотные проекты, связанные с внедрением типовых облачных решений для нужд местных властей, добавил он.

Создание типовых отраслевых решений (ТОР) "Умный город" и "Управление строительством" с тиражированием функциональности на все субъекты России планируется в 2026-2030 гг., уточнил "Ведомостям" представитель Минцифры. Благодаря ТОР "Умный город" органы местного самоуправления получат инструмент анализа текущих инцидентов городской инфраструктуры и прогнозирования потребности включения мероприятий в планы работ на основе данных (проблемы, жалобы, износ), говорит он. ТОР "Управление строительством" позволит обеспечить прозрачность процессов строительства, создать мастер-базу цифровых данных строительной отрасли и сократить длительность инвестиционно-строительного цикла.

По ФГИС "Объекты коммунальной инфраструктуры" на данный момент разрабатывается дорожная карта, заметил представитель Минцифры. ФГИС позволит повысить эффективность управления коммунальной инфраструктурой, обеспечить более прозрачное распределение средств на ее развитие и модернизацию, а также улучшить взаимодействие между всеми участниками процесса, указал он.

"Ведомости" направили запрос в Минстрой.

Сейчас в строительстве используют персональные компьютеры и ноутбуки с большими объемами вычислительных ресурсов, включая видеокарты (GPU), для задач проектирования, дизайна, рендеринга и расчетов, говорит руководитель направления продуктов и архитектурных решений Linx Cloud Алексей Корулин. В качестве альтернативы применяется виртуализация рабочих мест (VDI) с графическими ускорителями внутри облака, позволяющая подключаться к мощным ресурсам из любой точки мира. Для инженеров, проектировщиков и архитекторов, работающих в ресурсоемких приложениях, стоимость таких рабочих мест может варьироваться от 6000 до 30 000 руб. в месяц в зависимости от задач.

Чаще всего каждый региональный застройщик формирует IT-инфраструктуру индивидуально, отмечает архитектор MONS (входит в ГК "Корус консалтинг") Семен Назаров. Чаще всего она основана на локальных дата-центрах и системах, унаследованных от предыдущих проектов, добавляет он. К тому же в строительстве регионы используют несогласованные BIM-платформы (Building Information Model - информационная модель здания) и локальные базы, что мешает формированию полноценных цифровых двойников, добавляет руководитель комитета иммерсивных технологий АРПП "Отечественный софт" Дмитрий Александров.

Заявленные типовые облачные решения имеют разную природу и применимость, замечает заместитель генерального директора по науке АО "Сисофт девелопмент" (входит в ГК "Сисофт") Михаил Бочаров. "Если говорить о типовых проектных решениях, т. е. об облачной библиотеке проектной документации, - это действительно важно. Можно выбрать типовое решение, уже прошедшее экспертизу, с привязкой к ценам и поставкам строительных материалов, и проектная организация сможет эффективно с ним работать", - рассуждает топ-менеджер. Типовые решения по принципу "Умного города" вызывают скепсис, продолжает Бочаров. Информационная модель объекта должна храниться у него на сервере, а в облаке может быть только копия, объясняет он.

Идея регуляторов понятна - стандартизация проектной деятельности ведет к удешевлению, рассуждает заместитель директора департамента "Облака и данные" компании "Рексофт" Иван Шумовский. Централизованная типовая закупка, строительство, а также унифицированная эксплуатация в несколько раз дешевле стихийно созданных облаков, согласен руководитель направления MSSP (Managed Security Service Provider - провайдер управляемых служб безопасности) UserGate Артур Салахутдинов.

С технологической точки зрения унификация или изоляция решений (включая облачные сервисы) несет существенные риски, связанные с информационной безопасностью (ИБ), предупреждает Назаров. Менее оперативно будут выходить обновления, связанные с ИБ и закрытием уязвимостей. Пример Южной Кореи, где полностью сгорел крупный серверный центр и данные многих облачных систем оказались безвозвратно утеряны, показывает: не все можно и нужно переносить в облако, категоричен Бочаров. Помимо этого есть риски искажений или устаревания информации, добавляет он. Когда ключевые данные находятся у владельца, а облако используется только как вспомогательный инструмент, риски минимальны, полагает он.

Для справки: Название компании: *Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России, ранее Минкомсвязь)* Адрес: *123112, Россия, Москва, Пресненская наб.,*

10, стр.2 Телефоны: *+7(495)7718000; +74957718100* E-Mail: *office@digital.gov.ru* Web: *https://digital.gov.ru/ru/* Руководитель: *Шадаев Максут Игоревич, министр*

Для справки: Название компании: *Министерство строительства и жилищно-коммунального хозяйства Российской Федерации (Минстрой России)* Адрес: *127994, Россия, Москва, ул. Садовая-Самотечная, 10/23, стр. 1* Телефоны: *+74956471580; +7(495)5321380#50811; +7(495)7348580#50701* E-Mail: *sekr_gosstroy@minregion.ru; pressa@minstroyrf.ru* Web: *http://www.minstroyrf.ru* Руководитель: *Файзуллин Ирек Энварович, министр* (Ведомости 12.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Цифровизация

Вице-премьер Дмитрий Григоренко: Цифровизация – это основа для эффективного государственного управления.

Правительство применяет цифровую модель управления во всех ключевых направлениях своей работы. Об этом заявил Заместитель Председателя Правительства – Руководитель Аппарата Правительства России Дмитрий Григоренко во время своего выступления на общероссийском совещании Банка России с участием главы регулятора Эльвиры Набиуллиной.

Вице-премьер подчеркнул, что переход к управлению на основе данных стал фундаментом для повышения эффективности всей системы государственного управления – от работы с документами до реализации национальных проектов и других государственных инициатив.

"Цифровая модель управления позволила существенно структурировать работу госаппарата. Сегодня каждое наше мероприятие имеет измеримые результаты и контрольные точки. Они позволяют отслеживать прогресс исполнения и контролировать риски срыва сроков. Причём система автоматически собирает всю информацию и предупреждает о возможном неисполнении. Это в разы ускорило процессы согласования, повысило исполнительскую дисциплину и сократило уровень бюрократии. Для нас цифровизация стала фундаментальным изменением управленческой культуры, и мы готовы делиться этим опытом с федеральными органами власти и регионами", – подчеркнул Дмитрий Григоренко.

Он напомнил, что ежегодно через площадку Аппарата Правительства проходит порядка 2 млн документов, в том числе нормативных актов, проектов федеральных законов, отзывов и заключений на депутатские инициативы. Такой объём требует высокой точности работы, скорости и строгого соблюдения сроков, обеспечить которые позволяет цифровая модель управления.

Для её запуска Правительство полностью оцифровало процесс работы с документами. Так, была запущена новая система электронного документооборота (СЭД).

В результате сегодня свыше 90% документов на площадке Аппарата Правительства представлены в электронном виде. В 2020 году этот показатель не превышал 35%, при этом такие документы в основном представляли собой лишь скан-копии бумажного оригинала, визуальное отображение. Следовательно, эти скан-копии не содержали структурированных данных, что не позволяло системе извлекать и анализировать информацию.

В свою очередь за счёт внедрения новой СЭД документы сразу создаются в цифровом виде без дублирования на бумаге. Они также содержат структурированные данные, что даёт возможность государственным органам работать с электронными документами, в частности, систематизировать их по дате, номеру и виду документа, подразделению и содержанию, отслеживать историю согласования и исполнителей.

За счёт внедрения цифровых инструментов существенно выросли скорость и качество работы с документами. В три раза – до одного дня сократилось среднее время согласования документов за последние пять лет. При этом в 48 раз – до 15 минут уменьшилось время выпуска нормативных актов за аналогичный период. (INFOLine, ИА (по материалам Правительства РФ) 10.12.25)

К СОДЕРЖАНИЮ

Северная верфь ОСК внедряет цифровое управление сменно-суточными заданиями в цехах.

На судостроительном заводе ОСК "Северная верфь" началось внедрение корпоративного программного приложения для формирования и оперативной корректировки сменно-суточных заданий (ССЗ).

Новое решение предназначено для линейного персонала – мастеров и начальников участков судостроительных цехов. Планируется, что оно поможет повысить оперативность реагирования на происходящие изменения. Ранее процесс постановки и изменения задач часто был связан с бумажным документооборотом или требовал личного присутствия у стационарных компьютеров.

Ключевые задачи нового инструмента – повышение скорости и гибкости управления. Теперь мастер может сформировать, отправить или скорректировать задание для бригады непосредственно из цеха в режиме реального времени. В производственных помещениях приступили к установке специальных защищённых сенсорных киосков с интуитивно понятным интерфейсом, адаптированным для работы в условиях цеха.

Внедрение приложения ведёт к значительному сокращению бумажного документооборота, повышает прозрачность и управляемость на участках. Все изменения фиксируются в цифровой системе, обеспечивая актуальность информации о задачах для каждого сотрудника. Важным аспектом является именно локальная разработка, которая гарантирует идеальное соответствие решения внутренним бизнес-процессам и позволяет быстро вносить доработки по запросам конечных пользователей.

"Это не просто цифровизация ради галочки. Это решение, которое рождается внутри завода, чтобы закрыть конкретную производственную боль. Наши программисты, работая в тесном контакте с цехами, создали инструмент, который экономит время линейного персонала, повышает гибкость планирования и является важным шагом к созданию цифрового контура управления производством", – рассказал и.о. директора Северной верфи по информационным технологиям и цифровой трансформации Евгений Горелов.
Приложение создано внутренней IT-службой завода. В процессе внедрения оно будет доработана, чтобы максимально соответствовать потребностям конечных пользователей.

Для справки: Название компании: *Судостроительный завод Северная верфь, ПАО (СЗ Северная Верфь, ИНН 7805034277)* Адрес: *198096, Россия, Санкт-Петербург, ул. Корабельная, 6* Телефоны: *+78126005260* Факсы: *+78127877678* E-Mail: *info@nordsy.spb.ru* Web: *https://www.aoosk.ru/companies/oao-sudostroitelnyy-zavod-severnaya-verf/* Руководитель: *Волегов Василий Михайлович, временно исполняющий обязанности генерального директора* (Sudostroenie.info 12.12.25)

К СОДЕРЖАНИЮ

"Банки становятся интеллектуальным партнером промышленности". "КоммерсантЪ". 11 декабря 2025

Руководитель блока развития и цифровизации ОПК ПСБ Алексей Захаров о внедрении IT в передовых отраслях

Российские банки продолжают совершенствовать цифровые технологии в конкурентной борьбе за корпоративных клиентов. Какие стратегии они выбирают для развития цифровых решений для предприятий, применимы 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**.

— 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 следуете 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 рутиной. И, конечно, подстраиваем цифровые сервисы под процессы клиента, а не наоборот. Сначала наши клиентские и продуктовые менеджеры, IT-специалисты глубоко погружаются в клиентский бизнес, в специфику производственных процессов предприятий, их методологию и культуру работы. То есть начинаем не с "кода", а с контекста. Уверен: только так можно создать продукт, который станет частью эффективной бизнес-логики предприятия.
К примеру, по обращению одной из крупнейших строительных компаний мы внедрили в системе "Банк-клиент" дополнительный функционал по мониторингу платежей подрядчиков клиента и формированию детализированной аналитики. Для государственных корпораций разработали решение по интеграции их казначейских систем с системами банка на принципах открытых протоколов. Наше решение позволило клиентам упростить управление финансами и оптимизировать действия, обеспечив единую точку входа для всех финансовых потоков и сократив время обработки операций. Или другой пример: реализовали электронное подписание кредитно-обеспечительной документации для такой защищаемой категории клиентов, как предприятия ОПК, в системе ДБО PSB Corporate, что позволило упростить и значительно ускорить процедуры в рамках кредитного процесса.

— Во всем мире продолжается гонка искусственного интеллекта (ИИ). Как вы его используете в решениях для предприятий?

— При встраивании новых технологий и ИИ в наши продукты мы сначала проводим тщательную проверку гипотез на внутренних процессах на предмет их экономической целесообразности и эффективности, чтобы в наши сервисы попадали только зрелые решения. Собрали в банке команду для развития направления ИИ для крупного бизнеса, которая тестирует во внутрибанковских процессах AI-решения для проверки экономического и операционного эффекта. Одна из целей — освободить сотрудников от рутины и повысить скорость принятия решений. После

успешного завершения тестирования этих процессов перейдем к масштабированию технологий и их внедрению для оптимизации клиентского пути.

На мой взгляд, наиболее перспективно внедрение ИИ в контактные центры, системы дистанционного банковского обслуживания, кросс-продажи и андеррайтинг. При этом внедрение новых решений должно происходить при соблюдении жестких требований к защите данных — обязательна 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 темпы внедрения таких решений с учетом объективно возросшего спроса на продукцию оборонки как в рамках гособоронзаказа, так и задач импортозамещения.

— Насколько сложнее разрабатывать и внедрять цифровые решения для оборонного комплекса?

— При реализации крупных проектов по внедрению цифровых решений для ОПК наработанная отраслевая экспертиза позволяет нам предвидеть возможные сложности и заранее выстраивать процесс соответствующим образом. Объективные факторы, повторюсь, жесткие требования к информационной безопасности и необходимость использования импортозамещенных 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 разработали 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 импортозамещения в последней.

— 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 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 позволят оптимизировать характеристики изделия еще на этапе проектирования и повысить скорость выпуска новых образцов техники, а роботизированные комплексы уменьшат 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 потери в качестве изделия.

Текущие темпы развития агентных систем на основе искусственного интеллекта позволяют прогнозировать появление автономных цифровых "сотрудников", которые самостоятельно выполняют задачи, взаимодействуют 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 выявить 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, переосмыслят роль интеллектуальных партнеров промышленности за счет поставки ИИ-агентов, которые позволят предприятиям максимально сфокусироваться на индустриальных задачах. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Российские судостроители столкнулись с проблемой цифровизации. "Деловой Петербург". 12 декабря 2025

Судостроительная отрасль пока что не готова к переходу на классификацию с использованием цифровых моделей. Хотя пилотные проекты уже существуют.

Ключевые ограничения связаны с отсутствием единых требований к формату и структуре 3D–моделей, слабой стандартизацией и необходимостью юридически закрепить статус цифровой модели, объяснили "ДП" в Российском морском регистре судоходства (РС).

Напомним, ранее конструкторское бюро ОСК "Алмаз" представило пилотную программу цифрового взаимодействия с РС. В рамках проекта Регистр получил доступ к информационной 3D–модели судна, разработанной бюро в собственном программном обеспечении "Алмаз.Портал". Специалисты Регистра прошли обучение работе с системой.

"Цель проекта — используя достижения технологии информационного моделирования, перейти к согласованию результатов конструкторских работ в форме информационной 3D–модели, без использования традиционной конструкторской 2D–документации", — подтвердили "ДП" в пресс–службе КБ "Алмаз".

Однако, как уточняют в РС, задачей пилотного проекта является не переход на новую схему согласования, а оценка принципиальной возможности работы с 3D–моделью для целей классификации. Он должен показать, позволяет ли 3D–модель оценить соответствие проекта судна требованиям правил Российского морского регистра судоходства и международным конвенциям, а также каким образом будут фиксироваться результаты такого рассмотрения.

В РС отмечают, что пока вопросов больше, чем ответов. Основной проблемой является отсутствие единого подхода к формату и уровню детализации цифровых моделей. В отрасли одновременно сосуществуют технология BIM (Building information modeling) и её судостроительный аналог SBIM, внутренние закрытые форматы предприятий и попытки адаптации международного формата ОСХ (Open class 3D exchange format), который активно развивается зарубежными классификационными обществами.

При этом глубина проработки разных форматов неравномерна. По оценке специалистов Регистра, в ОСХ "достаточно детально описаны элементы корпусных конструкций", но данные по механическим системам и другим группам оборудования ограничены. Отечественные решения испытывают те же проблемы.

"Пока говорить об изменениях процедуры преждевременно", — указывают в связи с этим в организации. Ни один из пилотов, включая проект "Алмаза", ещё не позволил полностью пройти весь процесс проверки соответствия в цифровом виде.

Отдельной нерешённой задачей остаётся придание 3D–модели юридического статуса, сопоставимого с традиционной конструкторской документацией. В Регистре признают, что "в перспективе это, конечно же, случится", но сроки перехода не называются. Кроме того, необходимо определить механизмы защиты ноу–хау конструкторов при передаче цифровой модели третьим сторонам.

Так что пока дальнейшее взаимодействие с бюро и верфями будет вестись "в формате тестирования и освоения этой технологии", с параллельным рассмотрением традиционной документации.

Для справки: Название компании: *Центральное морское конструкторское бюро Алмаз, АО* Адрес: *196128, Россия, Санкт-Петербург, ул. Варшавская, 50* Телефоны: *+7(812)3738300; +78123737053* Факсы: *+7(812)3695925* E-Mail: *office@almaz-kb.ru* Web: *http://www.almaz-kb.ru/* Руководитель: *Голубев Константин Геннадьевич, Генеральный директор* (Деловой Петербург 12.12.25)

К СОДЕРЖАНИЮ

Как "Норникель", НЛМК, "Сибур" учатся предвидеть аварии на производстве. "РБК.Отрасли". 15 декабря 2025

Парадокс прогресса и тревожная статистика

Российские предприятия сталкиваются с системным парадоксом: несмотря на технологическое развитие, уровень производственного травматизма демонстрирует негативную динамику. По данным Социального фонда России (СФР), в 2024 году число несчастных случаев на производстве выросло на 7,4% по сравнению с 2023 годом.

Среди основных причин — неудовлетворительная организация работ (22,6%), нарушение технологического процесса (8,2%) и недостаточный контроль со стороны руководителей.

Проблема усугубляется экономическими факторами, такими как ужесточение условий труда и рост продолжительности рабочего времени в условиях дефицита кадров.

Традиционные, реактивные подходы к охране труда, основанные на разборе уже случившихся инцидентов, исчерпали себя. Они не справляются с вызовами цифровой эпохи, растущими требованиями регуляторов и

INFOLine информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

давлением ESG-повестки. Единственный адекватный ответ — цифровая трансформация, позволяющая прогнозировать и предотвращать нарушения.

Термин "цифровой иммунитет" в контексте охраны труда используется как метафора для обозначения устойчивой, проактивной системы управления рисками, основанной на данных и технологиях искусственного интеллекта для прогнозирования и нейтрализации угроз до их реализации.

Суть трансформации: от реагирования к предвидению

Цифровая трансформация охраны труда — это не про электронные журналы и умные браслеты. Это фундаментальное изменение философии управления безопасностью: переход от реагирования к предвидению.

Суть подхода заключается в создании целостной экосистемы, где данные из разрозненных источников (видеокамер, IoT-датчиков, ERP- и HR-систем) интегрируются и анализируются в режиме реального времени. Формируется сквозной процесс: данные последовательно проходят этапы сбора, аналитической обработки с прогнозированием, автоматизированного реагирования и используются для постоянного обучения и адаптации системы.

Что это дает на практике?

Снижение трудозатрат: в "Газпром нефти" автоматизация рутинных операций сократила трудозатраты специалистов на 35%.

Ускорение процессов: время согласования электронных наряд-допусков в той же компании снизилось на 90%, а формирование части управленческой отчетности ускорилось на 80%.

Упреждающее выявление рисков: в "Северстали" после внедрения комплексной системы потенциально смертельные риски стали выявляться почти в два раза чаще, а некоторые подразделения отработали месяцы без единой травмы.

Цифровой щит: обзор технологий, меняющих подход к безопасности труда

Подходы к охране труда кардинально меняются: эпоха простого реагирования на инциденты уходит в прошлое, уступая место стратегии их предупреждения. Трансформация, движимая цифровыми технологиями, уже набирает обороты: пока лидеры рынка активно ее реализуют, другим компаниям лишь предстоит к ней присоединиться.

Искусственный интеллект и машинное обучение. Это "мозг" современной системы безопасности. Алгоритмы анализируют видеопоток в реальном времени, выявляя нарушения правил ношения средств индивидуальной защиты (СИЗ) или рискованного поведения. Более того, ИИ способен обрабатывать исторические данные о происшествиях, параметрах оборудования и даже метеоусловиях, чтобы строить предиктивные модели и предсказывать вероятность аварий. Это позволяет перейти от расследования уже случившегося к его предотвращению.

Интернет вещей (IoT) и носимые устройства. Технология создает "цифровую кожу" предприятия. Сеть взаимосвязанных датчиков непрерывно мониторит состояние окружающей среды (загазованность, уровень шума, радиации) и самого оборудования (вибрация, температура). Носимые устройства для работников (например, умные каски или жилеты) могут автоматически регистрировать падение, перегрев или потерю сознания, отправляя сигнал тревоги за секунды. Это обеспечивает немедленную реакцию на угрозу, часто еще до того, как человек успевает осознать опасность.

Большие данные (big data) и цифровые двойники. Мощность технологий — в интеграции и анализе. Они объединяют разрозненные данные из систем охраны труда, кадрового учета (HR) и планирования ресурсов предприятия (ERP). На основе этой информации строится цифровой двойник — виртуальная копия производственного процесса, которая позволяет моделировать различные сценарии, выявлять скрытые корреляции рисков и принимать управленческие решения, основанные на данных, а не на интуиции.

Виртуальная и дополненная реальность (VR/AR). Инструменты кардинально меняют подход к обучению. VR-тренажеры позволяют сотрудникам в полной безопасности отрабатывать действия в смоделированных чрезвычайных ситуациях, что резко снижает количество ошибок новичков при столкновении с реальной угрозой. AR-очки могут проецировать цифровые инструкции и подсказки непосредственно в поле зрения работника, направляя его действия при выполнении сложных или опасных операций.

Важно понимать, что внедрение передовых решений было бы невозможно без уже ставших стандартом базовых систем, таких как ERP, программное обеспечение для системы управления охраной труда (СУОТ) и электронный документооборот (ЭДО). Сегодня это не конкурентное преимущество, а "цифровой хребет" организации, обеспечивающий операционную эффективность, прозрачность и управляемость. Именно на этот надежный фундамент в дальнейшем наращиваются более сложные технологии, такие как ИИ и big data.

При внедрении важно обратить внимание на следующее:

Качество данных. Эффективность систем на основе ИИ на 90% зависит от качества и объема входных данных. Начинать внедрение стоит с участков с максимальным числом инцидентов и историей данных не менее двух лет.

Кибербезопасность. Любое IoT-устройство — потенциальная точка входа для злоумышленников. Необходим строгий регулярный аудит уязвимостей и неукоснительное соблюдение требований законодательства (ФЗ-152 "О персональных данных", ФЗ-187 "О безопасности критической информационной инфраструктуры").

Результаты: когда проценты значат больше, чем слова

"Цифровой иммунитет" не теоретическая концепция, а практический инструмент, который демонстрирует значимые результаты в снижении травматизма и повышении безопасности на производстве.

Примеры внедрения:

Система машинного зрения от "Регенератора" на Кольской АЭС, применяемая с 2020 года, по данным компании, позволила в десять раз сократить число нарушений (с 80 до восьми случаев в неделю), полностью исключить несчастные случаи, связанные с неправильным использованием средств индивидуальной защиты (СИЗ) в контролируемых зонах, а также обеспечить распознавание 26 видов нарушений в режиме реального времени.

На Быстринском горно-обогатительном комбинате ("Норникель") внедрены ИИ-системы контроля использования СИЗ на ключевых производственных участках; в перспективе планируется обучение нейросети для распознавания применения страховочной привязи при выполнении работ на высоте.

В группе НЛМК действует комплексная цифровая платформа с модулем "Заявление об опасностях", благодаря которой за год сотрудники выявили 200 тыс. рисков, из которых 85% были оперативно устранены; кроме того, интеграция электронных нарядов-допусков с видеоаналитикой обеспечивает контроль безопасности — система блокирует начало огневых работ, если на фото с места их проведения отсутствует огнетушитель.

Анализ рыночных лидеров, внедривших цифровые решения в области охраны труда, показывает устойчивую положительную динамику по ключевым экономическим показателям:

срок окупаемости затрат на внедрение цифровых решений (например, цифровых двойников) составляет в среднем два-три года;

сокращение страховых выплат и оплаты больничных;

снижение простоев оборудования;

оптимизация документооборота и отчетности, что уменьшает административную нагрузку на предприятие.

ESG и регуляторика: цифровизация — стратегическая необходимость

Вызовы требуют от бизнеса не только операционной эффективности, но и соответствия растущим требованиям глобальной ESG-повестки и национального регулирования.

Внедрение упреждающих технологий безопасности напрямую способствует достижению целей устойчивого развития, трансформируя абстрактные принципы в измеряемые результаты:

Экологическая повестка (E). Цифровые двойники и системы предиктивного мониторинга на основе больших данных служат не только для предотвращения несчастных случаев, но и для снижения экологического ущерба. Такие системы, как в "Норникеле", позволяют моделировать сценарии развития аварий и нейтрализовать технологические риски, способные привести к выбросам загрязняющих веществ, обеспечивая тем самым соблюдение экологических стандартов.

Социальная ответственность (S). Технологии радикально повышают уровень защиты персонала. "Запсибнефтехим" ("Сибур") активно тестирует VR-тренажеры для обучения сотрудников. На производственных площадках в Нижневартовске и Ноябрьске проходят опытно-промышленные испытания системы, которая позволяет отрабатывать навыки оказания первой помощи, безопасного выполнения работ на высоте, действий при пожаре и обнаружении нештатных ситуаций. Многопользовательский режим дает возможность тренировать командные действия. При успешном завершении испытаний VR-тренажеры планируется внедрить на всех основных производственных площадках предприятия.

Корпоративное управление (G). Технологии искусственного интеллекта и распределенных реестров обеспечивают новый уровень прозрачности и управляемости. ИИ-платформы, аналогичные тем, что есть у "Газпром нефти", анализируют комплексные данные для формирования объективной картины рисков, а неизменяемые цепочки данных фиксируют каждое действие, создавая аудиторский след, безупречный для проверок регуляторов.

Регуляторное соответствие в эпоху "цифрового иммунитета"

Растущее давление со стороны контролирующих органов делает устаревшие методы охраны труда не только неэффективными, но и стратегически рискованными. "Цифровой иммунитет" становится единственным адекватным ответом на вызовы времени:

Повышение соответствия. Системы на основе IoT и компьютерного зрения позволяют не фиксировать нарушения, а прогнозировать и предотвращать их. Это соответствует прогрессивной логике современного регулирования, снижая риски внеплановых проверок и санкций, демонстрируя регуляторам зрелую систему управления.

Управление на основе данных в реальном времени. В условиях ужесточения законодательства (ФЗ-152, ФЗ-187) именно сквозные данные с датчиков, видеокамер и носимых устройств предоставляют руководству объективную аналитику для обоснования управленческих решений и защиты позиции компании. Это позволяет перейти от культуры оправданий к культуре предвидения.

Таким образом, инвестиции в передовые технологии не только инструмент снижения травматизма, но и стратегическая необходимость для укрепления репутации, управления регуляторными рисками и выполнения обязательств в рамках ESG-трансформации. Без этого компания рискует оказаться в роли догоняющего как в глазах стейкхолдеров, так и перед лицом контролирующих органов.

Безопасность — основа устойчивого развития

Чтобы быть по-настоящему эффективной и человекоцентричной, охрана труда в России должна совершить качественный скачок от устаревшей культуры запретов к передовой культуре предвидения и заботы. Именно в этом и заключается суть цифровой трансформации, которая является не просто модным трендом, а стратегическим императивом для бизнеса.

Ключевые выводы:

Предвидение — главный инструмент снижения травматизма. Фундаментом трансформации является смена парадигмы: от реагирования на произошедшие инциденты к их прогнозированию и предотвращению. Технологии искусственного интеллекта, анализа больших данных и цифровые двойники позволяют выявлять и нейтрализовывать угрозы до их реализации, что напрямую ведет к снижению процента несчастных случаев.

Доказанная эффективность в защите жизни и здоровья. Эффективность цифровых решений в защите жизни и здоровья находит прямое подтверждение в практике промышленных лидеров. Результаты внедрения носят не теоретический, а измеренный характер.

Человеческий фактор и данные — основа успеха. Эффективность любой системы прогнозирования на 90% зависит от качества данных. Не менее важен и человеческий капитал: преодоление "цифрового разрыва" и вовлечение сотрудников через обучение и разъяснение защитной, а не карательной роли технологий критически необходима для достижения результата.

Стратегическая необходимость, а не просто экономия. Хотя цифровизация дает операционную эффективность (сокращение трудозатрат, ускорение процессов), ее главная ценность — в создании "цифрового иммунитета". Это стратегическая инвестиция, которая за 2–3 года окупается не только деньгами, но и спасенными жизнями, снижением страховых выплат и защитой репутации компании.

Проактивный подход за счет использования технологий меняет саму философию охраны труда. IoT-датчики, ИИ-аналитика и VR-тренажеры — это не просто набор инструментов, а элементы единой системы, работающей на главный КПЭ: сохранение жизни и здоровья человека. В конечном счете именно этот результат оправдывает любые инвестиции. Формируемый таким образом "цифровой иммунитет" — это уже не протокол, а новая этика ведения бизнеса, где безопасность сотрудника — безусловный и неоспоримый приоритет.

Для справки: Название компании: *Горно-металлургическая компания Норильский никель, ПАО (ГМК Норильский никель, Норникель, NORILSK NICKEL, ИНН 8401005730)* Адрес: *123100, Россия, Москва, 1-ый Красногвардейский пр-д, 15* Телефоны: *+74957877667; +7(495)7855800* E-Mail: *gmk@nornik.ru; pr@nornik.ru* Web: *https://www.nornickel.ru* Руководитель: *Пенни Гарет, председатель Совета директоров; Потанин Владимир Олегович, генеральный директор, председатель Правления, президент*

Для справки: Название компании: *Новолипецкий металлургический комбинат, ПАО (НЛМК)* Адрес: *398040, Россия, Липецкая область, г. Липецк, пл. Металлургов, д. 2* Телефоны: *+74742444222; +74742441111; +78005113039* E-Mail: *info@nlmk.com* Web: *https://nlmk.com/ru/; https://lipetsk.nlmk.com/ru* Руководитель: *Кананович Роман Анатольевич, Директор дирекции по внешней логистике; Каратаев Сергей Михайлович, президент, председатель правления*

Для справки: Название компании: *СИБУР, ООО - управляющая организация СИБУР Холдинг, ПАО* Адрес: *117997, Россия, Москва, ул. Кржижановского, д. 16, корп. 1* Телефоны: *+74957775500; +74957805500; 79772685545* E-Mail: *info@sibur.ru* Web: *https://www.sibur.ru/ru* Руководитель: *Карисалов Михаил Юрьевич, председатель Правления, Генеральный директор ООО "СИБУР"* (РБК.Отрасли 15.12.25)

К СОДЕРЖАНИЮ

Искусственный интеллект

Владимир Путин заявил о необходимости взвешенного подхода к использованию ИИ.

Президент Владимир Путин назвал вопрос использования искусственного интеллекта и big data одновременно "важным и чрезвычайно сложным". Он подчеркнул, что отказ от этих технологий означает потерю конкурентоспособности, а их бездумное применение может привести к серьезным рискам. Такие заявления он сделал в ходе заседания Совета по развитию гражданского общества.

Глава государства отметил, что современные цифровые инструменты необходимо внедрять аккуратно, чтобы не допустить утечки данных, разрушения национальной идентичности и передачи чувствительной информации тем, "кто воспользуется ею недобросовестно".

Особое внимание Путин уделил образованию. По его словам, важно не допустить ситуации, когда молодое поколение перестанет самостоятельно мыслить и будет полагаться исключительно на цифровые подсказки. "Мы ни в коем случае не должны потерять поколение молодых граждан, которые вместо того, чтобы думать, будут просто нажимать кнопочку", – сказал Путин.

Президент предупредил о риске формирования узкой элиты из людей, способных к творческому и аналитическому мышлению, в то время как "основная масса" окажется в роли простых пользователей технологий. Путин подчеркнул, что государству предстоит найти баланс между развитием ИИ и сохранением человеческого потенциала, назвав задачу "очень сложной, но критически важной".

8 декабря премьер-министр России Михаил Мишустин заявил, что правительство РФ формирует план внедрения генеративного искусственного интеллекта на уровне государственного управления, регионов, а также ключевых отраслей.

19 ноября Путин, выступая на пленарном заседании конференции "Сбера", подчеркнул, что развитие ИИ является одним из крупнейших технологических проектов в истории. (Ведомости 09.12.25)

К СОДЕРЖАНИЮ

На Вершинном месторождении урана в Бурятии испытали российскую буровую установку с ИИ.

"Росатом" протестировал установку для бурения скважин ZBO S15E на месторождении Вершинное в Бурятии, сообщила компания-разработчик АО "Завод бурового оборудования". Испытания проводились в экстремальных климатических условиях при температуре ниже -25°С.

"Установка уже отработала неделю в сложнейших геологических и климатических условиях севера Бурятии. Эти семь дней показали рост производительности на 10% по сравнению с применявшимися ранее импортными аналогами. Это первый шаг к созданию российской полностью роботизированной буровой установки", — отметил директор по развитию "РУСБУРМАШа" (сервисное подразделение "Росатома") Владислав Чащин.

Буровая установка оснащена системой мониторинга Smart drill на базе ИИ, что позволяет технике самостоятельно создавать отчеты, проверять состояние оборудования и уведомлять сотрудников о необходимом обслуживании. Технологические процессы отображаются на планшете, а этапы работы сохраняются.

Для справки: Название компании: *Государственная корпорация по атомной энергии Росатом (ИНН 7706413348)* Адрес: *119017, Россия, Москва, ул. Большая Ордынка, 24* Телефоны: *+74999494535; +74999494412; +74999494634; +74999494221* E-Mail: *info@rosatom.ru; press@rosatom.ru* Web: *https://rosatom.ru* Руководитель: *Лихачев Алексей Евгеньевич, генеральный директор; Кириенко Сергей Владиленович, Председатель наблюдательного совета* (Недра ДВ 16.12.25)

К СОДЕРЖАНИЮ

В Росатоме не исключили перспектив применения ИИ в атомной промышленности.

В компании допустили, что языковые модели могут стать помощниками инженеров в решении рутинных задач, связанных с технической документацией

Технологии искусственного интеллекта (ИИ) могут стать востребованным инструментом в реализации исследовательских и инженерных задач в том числе в проектах для атомной отрасли. Такое мнение высказал директор по информационным и цифровым технологиям ГК "Росатом" Евгений Абакумов.

"Мы стоим перед постановкой, когда в сложной научно-исследовательской и проектно-конструкторской деятельности у нас с вами будет максимально интегрирована эта технология. Если говорить про ИИ для атома, то хочется, может быть, изначально не атомную станцию, а что-то более простое. Хочется сделать

какой-то проект, результат проекта национального суверенитета с применением максимально возможного количества технологий искусственного интеллекта", - сказал Абакумов, выступая на открытой конференции Института системного программирования имени В. П. Иванникова РАН.
Представитель госкорпорации напомнил о необходимости решения множества вопросов применения ИИ, связанных с сертификацией и информационной безопасностью. При этом он допустил, что в перспективе языковые модели могут стать помощниками инженеров в решении рутинных задач, связанных, к примеру, с технической документацией.
"Если мы возьмемся за задачу действительно большого проекта, то там будет понятно, какое место занимает ИИ в системах высокой ответственности, в системах суверенитета. Неважно что это - автомобиль, самолет, атомная станция. Но жизненный цикл сложного продукта для нас будет важной историей. И, конечно, в нынешних условиях нам с вами надо использовать эти технологии в том числе для того, чтобы нашим зарубежным партнерам их открывать и продвигать, может быть, совместно", - заключил он.

О конференции

Открытая конференция Института системного программирования имени В. П. Иванникова РАН проходит 9-10 декабря в инновационном кластере "Ломоносов" в Москве. В этом году она посвящена 85-летию со дня рождения основателя и первого директора института академика Виктора Петровича Иванникова. Ученый возглавлял научный центр до 2015 года, руководил кафедрами системного программирования в МФТИ и МГУ имени М. В. Ломоносова, опубликовал свыше 100 научных работ.

Для справки: Название компании: *Государственная корпорация по атомной энергии Росатом (ИНН 7706413348)* Адрес: *119017, Россия, Москва, ул. Большая Ордынка, 24* Телефоны: *+74999494535; +74999494412; +74999494634; +74999494221* E-Mail: *info@rosatom.ru; press@rosatom.ru* Web: *https://rosatom.ru* Руководитель: *Лихачев Алексей Евгеньевич, генеральный директор; Кириенко Сергей Владиленович, Председатель наблюдательного совета* (ТАСС 09.12.25)

К СОДЕРЖАНИЮ

"Росатом" будет строить зарядные станции в выявленных ИИ Яндекса точках высокого спроса.

Соглашение о сотрудничестве заключили "Росатом Сеть зарядных станций" и "Яндекс Электро" "Росатом Сеть зарядных станций" (входит в Электроэнергетический дивизион "Росатома") и "Яндекс Электро" (новое бизнес-направление "Яндекса" по развитию электротранспорта и зарядной инфраструктуры) объединяют технологии и инженерный опыт для развития инфраструктуры электротранспорта в России. "Росатом" планирует расширить собственную сеть до 11 000 электрозарядных станций в 53 регионах страны к 2030 году, специальная ML-модель Яндекса на основе анализа обезличенных данных о городах, движении транспорта и привычках пользователей поможет спрогнозировать спрос на зарядку и выбрать конкретные зоны для строительства новых ЭЗС.
Соглашение также предусматривает, что для удобства автолюбителей и профессиональных водителей электромобилей "Яндекс" встроит ЭЗС "Росатома" в свои сервисы: они смогут находить и оплачивать зарядку через Яндекс Карты, Яндекс Заправки или приложение для водителей и курьеров Яндекс Про.
"Миллионы водителей ежедневно пользуются сервисами "Яндекса", среди них постоянно растет число тех, кто выбирает электромобили. Для полномасштабного перехода на электротранспорт нужна охватная и технологичная электрозарядная инфраструктура. Вместе с "Росатомом" мы рассчитываем создать среду, в которой электротранспорт сможет полноценно решать повседневные транспортные задачи любого водителя, а инвесторы получат максимальную окупаемость вложений в инфраструктуру", – заявил руководитель "Яндекс Электро" Тембот Керефов.
"Наша ключевая задача – создание в стране современной зарядной инфраструктуры, которая сделает переход на экологичный транспорт по-настоящему массовым и удобным. Сотрудничество с "Яндексом" – важный шаг на этом пути. Мы строим физическую инфраструктуру, а "Яндекс" интегрирует её в цифровую экосистему, которой ежедневно пользуются миллионы. В результате водители смогут легко найти, забронировать и оплатить зарядку в привычных сервисах. При этом важно, что электроэнергия на наших станциях подтверждается сертификатом "Чистая энергия Росатома", что делает использование электромобиля по-настоящему "зеленым" выбором", – отмечает генеральный директор "Росатом Сеть зарядных станций" Валерий Маркелов.

Для справки: Название компании: *Государственная корпорация по атомной энергии Росатом (ИНН 7706413348)* Адрес: *119017, Россия, Москва, ул. Большая Ордынка, 24* Телефоны: *+74999494535; +74999494412; +74999494634; +74999494221* E-Mail: *info@rosatom.ru; press@rosatom.ru* Web: *https://rosatom.ru* Руководитель: *Лихачев Алексей Евгеньевич, генеральный директор; Кириенко Сергей Владиленович, Председатель наблюдательного совета*

Для справки: Название компании: *Яндекс, МКПАО* Адрес: *119021, Россия, Москва, ул. Льва Толстого, 16* Телефоны: *+74957397000; +74959743581; +77085647895* E-Mail: *pr@yandex-team.ru; vic.gryaznov@yandex-team.ru* Web: *https://yandex.ru/company/* Руководитель: *Корнева Марина Анатольевна, генеральный директор* (INFOLine, ИА (по материалам компании) 10.12.25)

К СОДЕРЖАНИЮ

Глава Сбера Герман Греф: финансовый эффект Сбера от ввода ИИ достигнет 550 млрд рублей в 2026 году.

Это коснется роста доходов от индивидуализации предложений, ценообразования, снижения кредитных рисков, а также оптимизации расходов

Совокупный финансовый эффект Сбера от внедрения искусственного интеллекта во всех направлениях достигнет 550 млрд рублей в 2026 году, заявил глава банка Герман Греф в рамках "Дня инвестора".

"Общий эффект от внедрения ИИ во всех направлениях достигнет в 2026 году 550 млрд рублей. Это коснется и роста доходов от индивидуализации предложений, и ценообразования, и снижения кредитных рисков, а также оптимизации наших расходов", - сказал он.

По словам главы Сбера, сейчас в банке внедрены сотни ИИ-агентов, которые применяются в ключевых процессах, более тысячи агентов находятся в разработке.

"К примеру, в нашем базовом процессе есть ИИ-агент, который формирует кредитные предложения для клиентов. Сегодня уже 96% корпоративных клиентов, использующих услуги кредитования, получили индивидуальные кредитные предложения. ИИ помогает нам защищать интересы наших клиентов: мы создаем ИИ-помощников, которые ежедневно обрабатывают более 500 млрд событий в области кибербезопасности - это в 10 раз больше, чем четырьмя годами ранее", - отметил он.

Для справки: Название компании: *Сбербанк, ПАО (ИНН 7707083893)* Адрес: *117997, Россия, Москва, ул. Вавилова, 19* Телефоны: *+74955058885; +78005008743; +74959575731; +74957473731* E-Mail: *scs@sberbank.ru; media@sberbank.ru* Web: *https://www.sberbank.com/ru; https://www.sberbank.ru* Руководитель: *Греф Герман Оскарович, президент-председатель Правления* (ТАСС 10.12.25)

К СОДЕРЖАНИЮ

Расходы, налоги, инвестиции: "Сбер" представил новых ИИ-помощников.

На конференции "Сделано в "Сбере" 10 декабря был представлен ряд инноваций от банка. В их числе — комплекс персональных ассистентов на основе нейросетевой модели GigaChat, призванных значительно упростить процесс управления финансами.

Первый заместитель председателя правления "Сбера" Кирилл Царев заявил, что банк последовательно формирует экосистему умных помощников, экономящих время и деньги клиентов. По его словам, искусственный интеллект выводит персонализацию сервиса на принципиально новый уровень, делая возможности, ранее доступные лишь премиальным клиентам, массовыми для всех россиян.

Так, например, теперь каждый владелец инвестиционного портфеля в "Сбере" может получить персонального советника по капиталу. Для этого достаточно сообщить сервису о своих финансовых целях, приемлемом уровне риска и ожидаемой доходности, после чего ассистент самостоятельно предложит оптимальные варианты вложений, сформирует сбалансированный портфель и, с одобрения клиента, будет осуществлять его своевременную корректировку.

Помощник по расходам, также созданный на базе GigaChat, позволяет оптимизировать траты без снижения качества жизни. Он формирует еженедельные и ежемесячные аналитические дайджесты, выделяет ключевые тренды в расходах, анализирует финансовое поведение клиента в сравнении с пользователями схожего профиля и дает индивидуальные рекомендации.

Еще одним нововведением стал налоговый помощник, интегрированный с платформой социальных налоговых вычетов, которую "Сбер" запустил при поддержке ФНС. Он автоматически идентифицирует подходящие для возврата средств траты — на лечение, обучение или фитнес. Если организация, услугами которой воспользовался клиент, задействована в этом сервисе, вычет оформляется полностью автоматически: "Сбер" находит операции, готовит необходимые справки и направляет их партнеру для последующей передачи в ФНС. Налоговая инспекция формирует заявление в личном кабинете налогоплательщика, и клиенту остается лишь в один клик его подписать для получения денег. Если же компания еще не подключена к системе, помощник предоставит пошаговую инструкцию для самостоятельного оформления вычета. (РосБизнесКонсалтинг 11.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Алгоритм для поиска нефти и газа улучшили с помощью ИИ.

В новом варианте алгоритм использует не только сейсмические и скважинные материалы, но и имеющуюся геологическую информацию с представлениями о развитии коллекторов на участке исследования

Ученые Института нефтегазовой геологии и геофизики СО РАН с помощью машинного обучения усовершенствовали методы интерпретации сейсмических данных, важные при поисках залежей углеводородов. Об этом сообщили в пресс-службе института.

Сейсмофациальный анализ - это способ "заглянуть" под землю без бурения, используя сейсмические волны. Традиционные методы такого анализа имеют свои ограничения, такие как сложность обработки больших объемов данных и необходимость вручную оценивать сейсмические образы. Для того, чтобы уменьшить трудозатраты и повысить достоверность решаемых задач геологи-интерпретаторы стали применять методы машинного обучения, основанные на кластеризации и классификации. Одним из эффективных математических инструментов, применяемых при решении задач, является Байесовский классификатор - алгоритм, который определяет класс объекта, рассчитывая вероятности на основе его признаков и формулы Байеса. Такая формула позволяет уточнить вероятность какого то события, когда уже есть предварительные данные и получена новая информация.

"В новом варианте алгоритм использует не только сейсмические и скважинные материалы, но и имеющуюся геологическую информацию с представлениями о развитии коллекторов на участке исследования. По словам ученых, это помогло повысить достоверность получаемых прогнозов", - рассказали в пресс-службе.

Специалисты уже использовали усовершенствованный алгоритм, исследуя участок нефтегазоконденсатного месторождения в Оренбургской области. По итогам анализа прошло успешное повторное перфорирование имеющихся скважин - это пробивание отверстий в обсадной колонне (металлической трубе, укрепляющей стенки скважины) и цементном кольце на уровне продуктивного пласта, чтобы нефть, газ или вода могли поступать в скважину. Вместе с бурением это подтвердило результаты предположений ученых. "Применение усовершенствованного алгоритма на стадии разведки и разработки месторождений углеводородов может существенно уточнить интерпретацию сейсмических данных", - приводятся в сообщении слова исследователей.

Все это позволяет выделить новые перспективные объекты, спрогнозировав зоны распространения коллекторов для дальнейшей постановки поисково-разведочного и эксплуатационного бурения. В дальнейшем ученые планируют дальнейшее развитие разработки для повышения точности прогнозов.

Для справки: Название компании: *Институт нефтегазовой геологии и геофизики им. А.А. Трофимука СО РАН, ФГБОУН (ИНГГ СО РАН, ФГБОУН)* Адрес: *630090, Россия, Новосибирская область, Новосибирск, просп. Академика Коптюга, 3* Телефоны: *+73833332900* Факсы: *+7(383)3302807* E-Mail: *ipgg@ipgg.sbras.ru* Web: *http://www.ipgg.sbras.ru/ru* Руководитель: *Глинских Вячеслав Николаевич, директор* (ТАСС 12.12.25)

К СОДЕРЖАНИЮ

"Газпром нефть" за счет ИИ приблизила старт разработки месторождений примерно на год.

Директор по геологоразведке Юрий Масалкин напомнил, что "Газпром нефть" приступила к созданию цифровых геологических моделей для поиска и добычи углеводородов еще 30 лет назад

Специалисты "Газпром нефти" за счет использования технологий искусственного интеллекта (ИИ) смогли ускорить интерпретацию результатов сейсморазведки от 10% до 30%, что позволило приблизить старт разработки месторождений примерно на год. Об этом сообщил журналистам директор по геологоразведке Юрий Масалкин в кулуарах конференции "ПроГРРесс".

"Благодаря внедрению ИИ "Газпром нефти" удалось значительно сократить цикл геологоразведочных проектов. С помощью интеллектуальных алгоритмов компания ускорила этап интерпретации результатов сейсморазведки от 10 до 30 процентов, что позволило приблизить старт разработки месторождения примерно на год", - сказал он.

По словам Масалкина, искусственный интеллект помогает быстро и точно интерпретировать данные сейсморазведки. И это касается не только новых проектов.

"С помощью ИИ мы получаем возможность заново открыть для себя хорошо изученные и знакомые районы, в том числе в Волго-Уральской нефтегазоносной провинции и в Западной Сибири, где добыча ведется уже около 50 лет", - добавил он.

Цифровые инструменты также помогают компании объединить огромные массивы ранее проведенных исследований, найти в них закономерности, которые традиционными методами обнаружить было невозможно. "Это позволяет открыть новые залежи, которые при выходе в эти регионы десятилетия назад не были видны", - отметил Масалкин.

Он напомнил, что "Газпром нефть" приступила к созданию цифровых геологических моделей для поиска и добычи углеводородов еще 30 лет назад.

Для справки: Название компании: *Газпром нефть, ПАО* Адрес: *190000, Россия, г. Санкт-Петербург, ул. Почтамтская, д. 3-5, литер А, ч. пом. 1Н, каб. 2401* Телефоны: *+78123633152; +7(800)7005151* Факсы: *+7(812)3633151* E-Mail: *info@gazprom-neft.ru; pr@gazprom-neft.ru* Web: *https://www.gazprom-neft.ru/* Руководитель: *Дюков Александр Валерьевич, председатель Правления, генеральный директор* (ТАСС 15.12.25)

К СОДЕРЖАНИЮ

В РФ разрабатывают нейросеть для ускорения проектирования летательных аппаратов.

Для проведения вычислений будет достаточно мощности обычного персонального компьютера, сообщили в Московском авиационном институте

Ученые Московского авиационного института (МАИ) разрабатывают нейросетевой алгоритм, способный с допустимыми потерями быстро моделировать динамику воздушных потоков на персональном компьютере вместо суперкомпьютера. Это поможет ускорить проектирование различных летательных аппаратов с нескольких недель до нескольких часов, сообщили ТАСС в пресс-службе вуза.

"Традиционно задачи вычислительной гидрогазодинамики требуют колоссальных вычислительных мощностей. Недели расчетов на суперкомпьютерах замедляют как исследования, так и внедрение новых разработок. Наш проект призван сократить время численного эксперимента с нескольких недель до считанных часов. Более того, для проведения вычислений будет достаточно мощности обычного персонального компьютера", - утверждает аспирант кафедры "Вычислительная математика и программирование" и инженер лаборатории искусственного интеллекта МАИ Антон Федоров, чьи слова приводятся в сообщении.

В основе проекта лежит специальный алгоритм машинного обучения - графовый нейросетевой аппроксиматор, который работает с информацией как с сетью связанных узлов и особенно, как считают в вузе, эффективен в работе со сложной геометрией. Нейросеть обучается на данных прошлых расчетов, анализируя физические процессы и выявляя закономерности. Это позволяет ей создавать упрощенные, но достаточно точные модели течения воздушных потоков. Ключевая особенность разработки - ее применение в трехмерном пространстве, тогда как ранее подобные исследования чаще всего демонстрировали эффективность на более простых двумерных моделях.

"Данный аппроксиматор работает быстро, но с потерями в точности. Тем не менее такой точности достаточно для предварительного анализа", - добавил Федоров.

Проект находится на стадии прототипирования. Завершить работы планируется в течение трех-четырех лет, уточнили в МАИ.

Для справки: Название компании: *Московский авиационный институт, ФГБОУ ВО (МАИ)* Адрес: *125993, г. Москва, А-80, ГСП-3, Волоколамское шоссе, д. 4* Телефоны: *+74991589209* E-Mail: *mai@mai.ru* Web: *http://mai.ru* Руководитель: *Погосян Михаил Асланович, ректор* (ТАСС 12.12.25)

К СОДЕРЖАНИЮ

"Магнит" запустил ИИ-ассистента в своем мобильном приложении.

Он помогает подбирать товары, а в будущем сможет искать самые большие скидки

В мобильном приложении "Магнит: акции и доставка" заработал ИИ-ассистент "Мэджик". Об этом сообщила пресс-служба ритейлера. "Мэджик" — собственная разработка технологической команды "Магнита", созданная с использованием open-source технологий и сторонней коммерческой LLM (большой языковой модели).

ИИ-ассистент помогает подбирать товары по заданным критериям. Например, для определенного приема пищи – завтрака, обеда или ужина. В будущем он научится искать самые большие скидки на товары, давать подсказки в магазине и на кассах самообслуживания, а также подбирать косметику и уходовые средства с учетом особенностей кожи.

С его помощью также можно будет уточнить статус заказа и решить проблему без обращения в службу поддержки.

"Магнит" первым на рынке продуктового ритейла запускает умного помощника, сообщил директор департамента по развитию продуктов бизнес-группы "Магнит Омни" Андрей Корыстин. "Мы считаем, что в конечном итоге победит не "самый умный" алгоритм, а тот, который лучше понимает потребности людей и делает их жизнь проще", – отметил он.

Сейчас "Мэджик" работает у части пользователей. Это позволит команде "Магнита" видеть, как покупатели взаимодействуют с ним, и постепенно дорабатывать его, "чтобы сделать незаменимой частью процесса покупок". Вскоре ИИ-ассистента откроют для всех пользователей приложения.
"Магнит" активно внедряет технологии и в работу своих магазинов. В апреле 2024 г. ритейлер создал лабораторию искусственного интеллекта для разработки и внедрения технологий на основе генеративного ИИ, а в июле 2024 г. – лабораторию для тестирования технологий в ритейле.
В 2025 г. ИИ-ассистентов внедрили "Яндекс" (в приложения "Яндекс лавка", "Яндекс еда" и "Яндекс маркет") и Wildberries. Ozon планирует запустить ИИ-ассистента для помощи в поиске товаров. Своего ИИ-ассистента разрабатывает и "Авито".

Для справки: Название компании: *Магнит, ПАО (Торговая сеть Магнит)* Адрес: *350072, Россия, Краснодарский край, Краснодар, ул. Солнечная, 15/5* Телефоны: *+78612109810; +7(800)2009002* Факсы: *+7(861)2109810* E-Mail: *info@magnit.ru; press@magnit.ru* Web: *https://magnit-info.ru/; https://magnit.ru/; https://cosmetic.magnit.ru/* Руководитель: *Случевский Евгений Сергеевич, генеральный директор; Райан Чарльз Эммитт, председатель Совета директоров; Корня Алексей Валерьевич, исполнительный директор* (Shopper's 16.12.25)

К СОДЕРЖАНИЮ

Минпромторг озаботился разработкой дорожной карты для создания ИИ-ускорителей. "Ведомости". 10 декабря 2025

Документ позволит отрасли консолидировать свои планы

Дорожная карта по разработке российских ускорителей для искусственного интеллекта (ИИ) (GPU) появится до июля 2026 г. Об этом заявил замминистра промышленности и торговли Василий Шпак на презентации программно-аппаратных комплексов (ПАК) "Группы Астра" 9 декабря. Без таких решений технологически независимого информационного стека построить не получится, подчеркнул он. Зачем России нужны свои ИИ-ускорители и что может войти в дорожную карту по их развитию, разбирались "Ведомости. Инновации и технологии".
В 2024 г. продажи ускорителей разных типов для ИИ во всем мире достигли $26,03 млрд. При этом около 40% от общемировых расходов пришлось на Азиатско-Тихоокеанский регион. Это следует из исследования американской Fortune Business Insights, результаты которого опубликованы 25 сентября 2025 г. При этом крупнейшими игроками традиционно выступают американские Nvidia, AMD, Intel, тайваньская TSMC, южнокорейская Samsung Electronics и др. В 2025 г. аналитики Fortune Business Insights прогнозируют, что объем мирового рынка ИИ-ускорителей достигнет $33,69 млрд при среднегодовом темпе роста 30,7%.
Данных о российском рынке ИИ-ускорителей нет, но объем российского рынка можно оценить по ИИ-серверам, в которых используются GPU. Например, аналитики J'son & Partners Consulting оценили рынок высокопроизводительных серверов в России в 2024 г. на уровне 30 млрд руб.
При этом полноценных российских аналогов GPU от вышеперечисленных компаний тоже нет. Компания "Байкал электроникс" в июне 2025 г. опубликовала на IT-портале "Хабр" описание собственных разработок современных GPU, но с тех пор судьба проекта не известна. Представитель "Байкала" не стал отвечать на вопросы о проекте компании. Но, как отметил Шпак, "не одним "Байкалом" живы" (его цитату приводил Telegram-канал "Неискусственный интеллект"). По словам чиновника, проработкой ИИ-ускорителей занимаются еще как минимум две организации, не называя конкретных.

Карты и ориентиры

Дорожные карты нужны, чтобы прекратить хаос с параллельными разработками и разрозненным финансированием, утверждает заместитель исполнительного директора ЦК НТИ по большим данным МГУ Гарник Арутюнян. Без них проект по разработке на 5-7 лет превращается в лотерею без конкретных планов, говорит он.
Обучать свою нейросеть можно и на чужих решениях, используя не только GPU, но и другие процессоры - тензорные, TPU, отмечает руководитель отдела цифровой трансформации НОЦ ФНС России и МГТУ им. Н. Э. Баумана Александр Староверов. "Дорожная карта - хороший инструмент лишь для быстрого стратегического взгляда, в ней указаны цели и сроки - общая фактура. Это не конкретный план, поскольку не отвечает на вопрос "как", а значит, пока сложно оценить потребность ресурсов", - рассуждает он.
В государственном управлении дорожные карты действительно становятся полезным инструментом, особенно когда речь идет о сложных, многозадачных проектах, согласен директор департамента расследований T.Hunter Игорь Бедеров. Они позволяют синхронизировать усилия различных ведомств, компаний и научных институтов и, как показывает практика, например, в транспортной отрасли, такие документы помогают структурировать переход на отечественные решения, определяя поэтапные шаги и ответственных, говорит он. Однако ключевой вопрос - не в создании самой карты, а в ее реалистичности и обеспечении ресурсами, подчеркнул эксперт.
Пока что планов по формированию единой стратегии развития ИИ или ПАКов для него в России нет. Тем не менее Минцифры уже разрабатывает введение специальных требований для производителей ПАКов, подходящих для работы с решениями в сфере ИИ, писали "Ведомости" в октябре 2025 г. Новые требования позволят продуктам этих компаний попасть в реестр российского программного обеспечения (ПО).

Эти требования включают в себя наличие собственного дата-центра в России мощностью не менее 10 МВт, следует из документа. Аппаратная часть ПАКа должна включать до восьми чипов, обеспечивающих не менее 75% вычислительной мощности и производительность от 100 петафлопс (1 петафлопс - 1 квадриллион операций с плавающей точкой в секунду) FP4. FP4 - один из новых форматов вычислений, адаптированный под задачи нейросетей, прежде всего больших языковых моделей, объясняет генеральный директор Comnews Group Леонид Коник.

Помимо этого аппаратная часть должна содержать сетевые адаптеры со скоростью не ниже 800 Гбит/с с поддержкой RDMA (позволяет получать доступ к памяти другого компьютера по сети, минуя центральный процессор. - "Ведомости"), а ПО обязано обеспечивать хранение не менее 1 эксабайта (1 млн терабайт) данных и возможность обучения моделей на 1000 GPU. Опрошенные "Ведомостями" эксперты в октябре 2025 г. соглашались, что пока что нет производителей, способных реализовать все пункты одновременно.

Свои и чужие GPU

Свои ускорители нужны, чтобы в какой-то момент не остаться без вычислительных мощностей из-за внешних ограничений, объясняет Арутюнян. Разработчиками таких решений могут стать МЦСТ, "Астра", "Ростех", "Яндекс", говорит он. "У всех этих компаний есть наработки в области центрального процессора и частично нейроускорителей, но настоящего GPU у страны пока нет, только прототипы", - подчеркнул эксперт.

Главный же барьер сейчас - отсутствие полного цикла производства, собственных IP-библиотек, техпроцесса, массового производства и экосистемы софта, подчеркивает он. При этом сделать за два года это невозможно ни при каких бюджетах, сетует Арутюнян. Рынок уже завязан на решения Nvidia, AMD и китайские решения уровня Ascend и Biren. В реальности появления отечественных продуктов такого класса не стоит ждать раньше 2030 г., говорит эксперт.

С этим согласен и руководитель проектов компании "Интеллектуальная аналитика" Тимофей Воронин. По его мнению, процесс перехода на собственные ускорители может занять длительное время - до 10-15 лет, говорит он. Еще столько же может потребоваться на то, чтобы отечественные решения стали востребованы и конкурентоспособны, говорит он. В Китае только начинает появляться что-то сопоставимое, но они все равно отстают минимум на одно поколение, подчеркнул Воронин. У Китая ушло примерно 10 лет, чтобы сократить технологический разрыв, добавил он. "Проблема не только и не столько с GPU, сколько с экосистемой решений вокруг них. У Nvidia свой проприетарный технологический слой CUDA, с которым совместим распространенный фреймворк написания моделей PyTorch. Huawei также делает свой стек", - пояснил он.

Реалистичный сценарий импортозамещения лежит не в копировании западных образцов, а в создании прагматичных, специализированных решений для конкретных задач российской экономики, с фокусом на энергоэффективность и интеграцию в готовые программно-аппаратные комплексы, продолжает Бедеров. "Только такой подход может превратить стратегическую необходимость в реальное конкурентное преимущество. Думаю, что в срок до трех лет мы можем увидеть адаптацию ПО под имеющуюся отечественную элементную базу, а лишь затем, к 2030 г., выход на рынок первых российских специализированных ускорителей", - добавил он. (Ведомости 10.12.25)

К СОДЕРЖАНИЮ

Интеллект под угрозой. "КоммерсантЪ". 10 декабря 2025

В России начал формироваться рынок защиты ИИ

Российский рынок защиты систем искусственного интеллекта только формируется, но уже в 2026 году может превысить 1 млрд руб. Крупнейшие компании начинают внедрять инструменты анализа защищенности ИИ-систем на фоне громких утечек персональных данных и коммерческих тайн из чат-ботов. При этом участники рынка предупреждают о новых серьезных угрозах: злоумышленники все чаще маскируют кибератаки под легитимный трафик больших языковых моделей, что резко увеличивает их скрытность. Наиболее уязвимыми оказываются финансовый сектор, промышленность и ритейл.

По прогнозу IT-компании AppSec Solutions, российский рынок защиты ИИ в 2026 году составит не менее 1 млрд руб., достигнув в 2029 году 11 млрд руб. Рынок только формируется, но от него ожидают роста в геометрической прогрессии. Источник "Ъ", близкий к крупной IT-корпорации, приводит более позитивные оценки: 3–4 млрд руб. в 2026 году и 25–30 млрд в 2030-м. При этом российский рынок генеративного ИИ к концу года достигнет 58 млрд руб. при объеме 13 млрд руб. в 2024 году (см. "Ъ" от 9 декабря).

На рынке в 2025 году зафиксированы первые публичные инциденты, которые связаны с утечками персональных данных и коммерческой тайны из GenAI-моделей, отмечает директор по кибербезопасности "СберТеха" Всеслав Соленик. По его словам, это формирует новый сегмент рынка: "С ростом применения ИИ в бизнесе и госсекторе защита от специфичных угроз, таких как манипуляции с ИИ-моделями, становится необходимостью".

У китайской компании—разработчика ИИ-чат-бота DeepSeek в начале 2025 года была выявлена первая крупная утечка данных из-за неправильно настроенной облачной базы, открывшей доступ к более чем миллиону записей, включая чаты пользователей, API-ключи и системные логи, по данным международной организации OWASP.

Также в марте 2025 года злоумышленники воспользовались уязвимостью внедрения подсказок в ChatGPT, что привело к раскрытию конфиденциальных данных пользователя, сообщал OWASP.

Крупнейшие компании в области финтеха уже внедряют инструменты анализа защищенности ИИ-систем на устойчивость к атакам, говорит гендиректор AppSec Solutions Юрий Сергеев. "Наши ключевые заказчики — это крупные компании и организации, активно проходящие AI-трансформацию, включая финансовые организации, телеком и промышленные предприятия",— добавляет господин Соленик.

При этом традиционные подходы к кибербезопасности — антивирусы, фаерволы, системы обнаружения внедрений — недостаточны для защиты больших языковых моделей, отмечает бизнес-партнер по ИБ Cloud.ru Юлия Липатникова: "Эффективная защита таких систем требует других принципов: постоянного анализа контекста, поведенческих аномалий и самообучения механизмов безопасности".

Злоумышленники знают, что в большинстве организаций ИИ-интеграции растут быстрее, чем системы контроля безопасности, и потому выбирают интеграции в качестве идеального укрытия, объясняет эксперт центра мониторинга и противодействия кибератакам компании "Информзащита" Шамиль Чич. "Самая серьезная угроза в том, что компании воспринимают LLM-трафик как доверенный по умолчанию",—добавляет он. Кроме того, злоумышленники уже используют маскировку под трафик больших языковых моделей, что "увеличило незаметность кибератак на корпоративный сектор на 42%", говорит он:

"Именно эта "легитимная оболочка" делает новые атаки особенно опасными. ИТ-системы воспринимают их как штатное взаимодействие с ИИ, тогда как фактически речь идет о полноценном канале управления зараженными устройствами".

Наиболее подверженными новым атакам оказались три ключевых сектора экономики, добавляет господин Чич: финансовые организации (34%), промышленность и высокотехнологическое производство (27%), ритейл и e-commerce (21%). Оставшиеся 18% составляют государственные, образовательные и медицинские учреждения, где высокий трафик и сложная инфраструктура усиливают риск появления скрытых угроз, говорит он. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

Слепой ведет слепых. "КоммерсантЪ". 10 декабря 2025

Низкое качество данных становится препятствием для внедрения ИИ

Все российские системообразующие банки используют в работе искусственный интеллект. Банки ускоряют внедрение искусственного интеллекта (ИИ), рассчитывая на автоматизацию процессов, более точные риск-модели и персонализацию клиентских сервисов. Но по мере роста числа ИИ-проектов становится очевидно: большинство таких инициатив упирается в один и тот же барьер — низкое качество данных. До системного решения этой задачи инвестиции в ИИ не будут давать сопоставимый результат.

Нейросети ограниченной точности

Центральный банк отмечает, что банки используют ИИ в большинстве ключевых процессов: от кредитного скоринга и оценки рисков до антифрода, персонализации продуктов, анализа трансакций и обслуживания клиентов. Из 12 системообразующих банков 11 используют ИИ в скоринге, 9 — в профилировании клиентов и персонализации, а модели глубокого обучения и генеративный ИИ уже применяются для автоматической подготовки документов, обработки изображений, классификации обращений и маршрутизации запросов. Для розничного кредитования степень автономности алгоритмов, по оценке банков, "приближается к 100%": выдача кредитов в массовых сегментах проходит полностью автоматически, а участие человека ограничивается настройкой, валидацией и запуском моделей.

Инвестиции крупнейших игроков подтверждают масштаб тренда. Сбербанк планирует увеличить вложения в ИИ до 350 млрд руб. к 2026 году, ожидая от этого 1,4 трлн руб. дохода за трехлетний период. ВТБ, по заявлению главы ВТБ Андрея Костина, уже сэкономил 15 млрд руб. за счет алгоритмов и рассчитывает увеличить эффект до 50 млрд руб. в ближайшие два года; Т-Банк прогнозирует прямой экономический результат в "десятках миллиардов" рублей в текущем году.

При этом проникновение ИИ в финансовый сектор остается неоднородным. Согласно опросу ЦБ, 24% банков активно используют ИИ, еще у 19% банков ИИ в стадии пилотного проекта, а самые "автоматизированные" сценарии — когда решения принимаются без участия человека — сегодня есть во всех системно значимых банках и страховых компаниях.

Искусственный интеллект применяется и в миграционных проектах. В компании Arenadata отмечают, что модели помогают автоматизировать подготовку преобразований данных и упрощать проверку структур перед переносом, снижая объем рутинных операций. Такие подходы позволяют сократить сроки миграций, но требуют базовой согласованности хранилищ и прозрачной логики формирования данных.

ИИ уже используется в банках для автоматизации отдельных этапов работы с информацией. Модели помогают выявлять аномалии, подсказывать возможные дубли и обращать внимание на некорректные поля — то, что раньше требовало большого количества ручных операций. Директор по отраслевым решениям в коммерческих банках

К2Тех Василий Куць считает, что нейросети могут "частично упорядочивать данные и подсказывать вероятность ошибок", но остаются вспомогательным инструментом, а не основой критичных процессов.

Наиболее заметный эффект ИИ дает при выполнении задач каталогизации: алгоритмы помогают сопоставлять атрибуты, определять вероятные типы данных и выявлять связи между объектами. Это сокращает время инвентаризации и упрощает выстраивание процессов Data Governance (система правил и процессов управления качеством и жизненным циклом данных). Но и здесь технологии работают только при наличии минимального порядка и единых правил формирования данных.

Несмотря на высокий уровень цифровизации, российские банки подходят к развитию ИИ с разнородной архитектурой и накопленным за десятилетия массивом несовместимых данных. По мнению экспертов, с увеличением числа продуктов и каналов обслуживания данные распределялись между десятками систем, каждая из которых формировала собственные хранилища и логику обработки. Это привело к расхождениям в атрибутах, дублям клиентских записей и разрыву между оперативными данными и данными аналитики. Кроме того, постоянный запуск новых сервисов при сохранении старой инфраструктуры сделал архитектуру данных разнородной и фрагментированной.

Ситуацию усиливает и отсутствие единой стратегии работы с данными. "Отсутствие четкой стратегии по управлению данными приводит к своеобразному хаосу, когда в компании нет системного подхода и каждый вносит свою логику. Основная задача — не допускать накопления некорректных данных и организовывать профилактику с помощью специальных решений Data Quality",— отмечает Василий Куць. Он полагает, что нейросети и современные алгоритмы не всегда могут справиться с ситуацией: хотя они частично упорядочивают данные, точность их ограниченна. При этом объем данных растет быстрее, чем банки успевают выстраивать процессы их контроля. Клиентские сведения меняются, вводятся вручную, не всегда проходят валидацию, а отдельные параметры остаются неактуальными годами. В результате качество данных, важное для операционных задач, становится критичным для ИИ-моделей, которые зависят от согласованности и полноты входной информации.

В техническом долгу перед ИИ

Появление ИИ усилило значение качества данных. Раньше аналитические системы могли работать даже с неполной или частично структурированной информацией. Сегодняшние модели требуют строгой согласованности: даже небольшое различие между системами приводит к тому, что ИИ начинает выдавать разные или непредсказуемые результаты. И тогда слепой ведет слепых.

Особенно чувствительными оказались модели для риск-менеджмента, скоринга, антифрода и KYC (англ. "know your customer" — "знай своего клиента", процесс проверки личности клиентов, который используется финансовыми организациями и другими компаниями для предотвращения мошенничества, отмывания денег и финансирования терроризма): в этих зонах ИИ зависит от полноты и актуальности клиентских данных, и ошибки недопустимы. Наличие дублей, расхождения в паспортных данных, устаревшие контакты или несовместимые форматы становятся ограничением, которое ИИ не может компенсировать.

Высокая стоимость вычислений делает качество данных еще важнее: чем больше ошибок и несоответствий, тем дороже обходится обучение моделей. Значительная часть усилий уходит не на сами алгоритмы, а на подготовку данных: их очистку, проверку и приведение к единому виду. По оценкам рынка, на эти задачи дата-сайентисты тратят до 70–80% рабочего времени. В итоге ИИ, который должен был ускорить работу, становится скорее показателем слабых мест в архитектуре данных. То, что ранее считалось техническими нюансами, теперь напрямую ограничивает внедрение ИИ и снижает его практическую отдачу.

Долгое время банки воспринимали качество данных как техническую задачу, которую можно решать внутри ИТ-подразделений по мере необходимости. Такой подход работал, пока речь шла о локальной аналитике или отдельных отчетах. Но с ростом объемов данных и появлением ИИ стало понятно, что несогласованность процессов приводит к накоплению ошибок и мешает масштабировать новые технологии.

Во многих организациях данные формировались по мере запуска новых сервисов, без единого набора правил. Часто не было понятно, какие сведения считать эталонными, кто отвечает за их актуальность и как фиксировать изменения. С точки зрения владельца продукта PIX BI Сергея Полехина, абсолютной точности и полной согласованности данных добиться невозможно, но важно обеспечить такой уровень их качества, "при котором данные остаются надежной основой для принятия решений", а фрагментация и дублирование только усложняют эту задачу.

В последние годы банки начали переходить к более системной работе: создают дата-офисы, вводят ответственных за качество данных, формализуют метрики. По словам зампредседателя правления банка ДОМ.РФ Николая Козака, качественные данные требуют не только технологий, но и общей культуры — "единых подходов к приоритизации, правилам формирования и контролю". Однако подобный подход пока внедрен не во всех организациях, и процессы нередко остаются разрозненными.

Дополнительная сложность связана с технологическим долгом. На это прямо указывает директор по продукту "Триафлай" Александр Щелканов: "Многие банковские системы долгие годы развивались несогласованно, и сегодня выравнивание данных превращается в масштабный технологический долг, который необходимо закрывать, прежде чем строить полноценные решения на базе ИИ". По сути, речь идет о многослойной инфраструктуре, где

новые проекты ложатся на еще не согласованную архитектуру данных. Это снижает точность моделей и делает эффект от ИИ менее заметным, чем он мог бы быть при сопоставимых инвестициях.

Если данные в разных системах расходятся между собой, возможности ИИ оказываются ограниченными. Как подчеркивает Сергей Полехин, если в разных системах хранятся разные значения одного и того же параметра, никакая модель не сможет стабильно работать: "Даже качественные данные, собранные из разных источников, могут оказаться непригодными для использования, если у них отсутствуют общие идентификаторы или метаданные, позволяющие их увязать. Например, разрозненные данные могут быть связаны по времени или типу операций, но, если первоначально не были предусмотрены механизмы интеграции, их совместное использование затрудняется". Поэтому даже продвинутые модели остаются зависимыми от качества исходной информации и не заменяют базовых процессов валидации, реконсиляции (процесс сравнения и согласования данных между двумя или более системами для обеспечения их целостности и идентичности) и контроля данных.

По мере того как банки переходят от разрозненных проектов к более упорядоченной работе с данными, возможности ИИ будут расширяться. Технология станет эффективной в тех сегментах, где удастся обеспечить достаточную точность, актуальность и полноту данных. В этих условиях ИИ может стать не дополнительным инструментом, а частью базовой операционной инфраструктуры, влияя на принятие решений и качество обслуживания. Однако для отрасли в целом этот переход требует времени. Масштабное применение ИИ станет возможным только в тех организациях, где работа с данными включает единые стандарты, оценку рисков и непрерывный контроль качества.

Пока данные остаются разнородными, фрагментированными и недостаточно управляемыми, эффект от применения ИИ будет ограничен. Даже самые продвинутые модели опираются на согласованные, актуальные и проверенные данные, и в отсутствие такого фундамента они не смогут работать предсказуемо и масштабироваться. Для банковского сектора это означает, что инвестиции в ИИ начнут приносить сопоставимый результат только тогда, когда качество данных достигнет уровня, при котором информация во всех системах совпадает по ключевым параметрам, регулярно обновляется и проходит прозрачный контроль. Иначе искусственный интеллект останется надстройкой, которая вынуждена компенсировать архитектурные проблемы, а не раскрывать собственный потенциал. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

"Интерес к ИИ обусловлен необходимостью быстрее адаптироваться к меняющейся деловой среде". "КоммерсантЪ". 10 декабря 2025

Об опыте применения искусственного интеллекта в одном из крупнейших банков страны

Процесс импортозамещения, его влияние на макроэкономические показатели и цифровизация финансового сектора стали главными темами прошедшего 16-го инвестиционного форума ВТБ "Россия зовет!". О цифровых переменах в ВТБ и применении искусственного интеллекта в интервью "Ъ" рассказала руководитель финансового департамента—старший вице-президент ВТБ Наталья Сурова.

Банк ВТБ — международная финансовая группа, предоставляющая широкий спектр финансово-банковских услуг. В России ВТБ предоставляет весь спектр банковских услуг через разветвленную региональную сеть. Дочерние организации группы предоставляют услуги по лизингу, факторингу, другие финансовые сервисы и продукты.

— ВТБ завершил основной этап внедрения платформы данных на базе российских решений Arenadata. Она объединила информацию из ключевых информационных систем ВТБ в единое пространство. Какие выводы можно сделать по итогам проекта?

— Перевести на российское ПО решения, которые развивались более 15 лет,— задача нетривиальная. В ряде случаев переход мог привести к отличиям в производительности, поэтому для нас критична готовность вендора дорабатывать продукт под реальные потребности банка. Здесь ВТБ выступает сильным заказчиком: мы хорошо понимаем прикладные требования финансовой функции и опираемся на большой опыт использования разных систем.

За последние три года мы перевели на российское ПО системы бизнес-планирования и обработки финансовых данных и завершили основной этап внедрения платформы данных на базе Arenadata. Она объединила данные ключевых систем в единое пространство и обеспечила централизованную аналитику и взаимодействие с регуляторами. Технологическое ядро включает аналитическую СУБД Arenadata DB, озеро данных на Arenadata Hadoop и оперативное хранилище.

На старте мы столкнулись со снижением скорости обработки, но совместно с технологическим блоком вернули ее к прежнему уровню. При этом в отдельных бизнес-процессах уже даже превзошли западные аналоги. Одновременно перенос на новый стек стал естественным аудитом существующих витрин и процессов — часть решений удалось оптимизировать. Наш главный вывод: при активном участии вендоров переход на отечественные решения возможен без потери качества и скорости.

— Какие изменения в работе финансовой функции ВТБ вы считаете наиболее значимыми благодаря внедрению технологий искусственного интеллекта? В каких направлениях эффект оказался наиболее измеримым?

— Мы применяем технологии искусственного интеллекта как в рутинных задачах, так и в стратегических направлениях финансовой функции. Интерес к ИИ обусловлен не только поиском эффективности, но и необходимостью быстрее адаптироваться к меняющейся деловой среде.

Для нас важно не только искать эффективность, но и понимать реальные ограничения ИИ, чтобы внедрение дорогостоящих решений давало измеримый эффект — особенно с учетом того, что для банков затраты на программное обеспечение напрямую уменьшают капитал.

Поэтому мы начинаем с областей, где уже есть подтвержденные результаты: закупки, обработка финансовых документов, формирование договоров, контроль качества данных. В этих задачах ИИ позволяет ускорять процессы и снижать трудозатраты.

Мы также развиваем проект "Цифровые советники финансового департамента" — платформу ИИ-агентов, которая автоматически определяет исполнителя запроса и обрабатывает его с помощью нужной модели. ИИ-агенты позволяют упростить подготовку закупочной документации, проводить анализ ценовых предложений, а также обеспечивают сопровождение участников закупочного процесса. Фактически ИИ становится помощником в типовых операциях и инструментом повышения прозрачности.

— Вы отмечаете важность понимания "масштаба эффекта" и ограничений ИИ. Какие ограничения сегодня наиболее существенны для банка и где, наоборот, технология уже доказала свою экономическую отдачу?

— Мы внимательно отслеживаем технологические тренды и оцениваем их практическую ценность для финансовых процессов. ИИ успешно работает в колл-центрах, например при первичной обработке обращений, но его возможности также имеют и ограничения: алгоритмы требуют точной постановки задач, чувствительны к неоднозначностям и опираются на исторические данные.

При работе с конфиденциальной информацией также необходимы дополнительные меры безопасности. Поэтому ИИ может усиливать экспертизу, но не заменяет профессиональное финансовое сообщество — в вопросах стратегии, корпоративной культуры, управления репутацией и разработки новых гипотез. Здесь человеческий опыт по-прежнему незаменим.

— Как меняется система закупок после внедрения ИИ? Какие процессы удалось автоматизировать и какие результаты вы считаете ключевыми?

— В банке работает комплексная система iProc, которая автоматизирует закупки от подачи потребности до заключения договора и полностью соответствует требованиям 223-ФЗ. Решение изначально построено на отечественном технологическом стеке и отличается высоким уровнем цифровизации: члены комиссии могут принимать решения через мобильное приложение, типовые договоры формируются роботами, а конструктор договоров автоматически собирает проекты документов. Благодаря этому скорость закупочных процедур выросла примерно на 50%, а удовлетворенность внутренних заказчиков превышает 90%.

Следующий шаг — внедрение ИИ-агентов на базе больших языковых моделей. Они помогут анализировать закупочную документацию, формировать аналитические справки, искать рыночные цены и предоставлять консультации пользователям. Это обеспечит дальнейший рост эффективности закупочного сервиса.

— Какую роль искусственный интеллект играет в сценарном моделировании? Какие задачи уже решаются сейчас и что остается в планах на более длинный горизонт — 10–20 лет?

— В стратегических финансах сценарий — это предположение о развитии событий, оценка его последствий и набор действий в ответ. Инструмент сложный, требующий аккуратной интерпретации. ИИ в этой области выполняет вспомогательную роль. Он может формировать качественные вводные, проверять полноту предпосылок, помогать в разработке финансовых моделей и методик на основе научных публикаций или выявленных закономерностей. При необходимости ИИ способен написать код модели.

Машинное обучение и языковые модели используются для интерпретации и структурирования разноформатных данных, что усиливает инструменты анализа. Новые решения позволяют оперативно корректировать методики прогнозирования и настраивать модели в режиме реального времени. Дальнейшее развитие мы видим в создании и актуализации моделей прогнозирования и ситуационного анализа на базе интеграции данных и внешней информации — ИИ помогает проводить суммаризацию данных из документов, анализировать качественные факторы и уточнять подходы к моделированию.

— Одним из направлений внедрения ИИ вы называете качество данных. О каких задачах идет речь и какие подходы позволяют обеспечивать устойчивое повышение качества?

— В первую очередь технологии ИИ помогают выявлять аномалии и ошибки в данных, интерпретировать их, направлять инциденты ответственным командам и контролировать их устранение.

В более долгосрочной перспективе мы рассматриваем применение ИИ для управления самой структурой данных. Каждый год появляются новые признаки и показатели, информационная модель растет, а скорость устаревания данных увеличивается: часть атрибутов перестает использоваться, отдельные алгоритмы обработки не обновляются, хотя на это уже есть основания. Именно здесь мы видим значительный потенциал ИИ — в

оптимизации процессов управления качеством данных и снижении затрат на их поддержку. Для крупных компаний эта функция постоянная и ресурсозатратная, поэтому внедрение подобных инструментов способно принести ощутимый эффект.

— Вы говорите, что сейчас уникальное время, когда крупные заказчики фактически участвуют в формировании рынка отечественного ПО. Какую роль в этом процессе играет ВТБ и какие компетенции заказчика становятся критичными?

— На примере проекта по внедрению системы консолидации хорошо видно, какую роль может играть крупный заказчик. Наш опыт построения предыдущей системы и глубокое понимание процессов формирования консолидированных данных позволили формулировать задачи очень конкретно с учетом нюансов пользовательских функций, требований к технологическому регламенту и архитектуре решения.

Сегодня заказчик с крупными объемами данных и высокими требованиями к скорости обработки обязан разбираться не только в бизнес-процессах, но и в технологических вопросах. Понимание возможностей и ограничений платформы, специфики интеграционных решений и критичных характеристик позволяет нам формировать четкое и реалистичное техническое задание и фактически участвовать в развитии продукта вместе с вендором.

— Как вы оцениваете перспективы цифровизации финансовой сферы в России в ближайшие три-пять лет? Какие направления, на ваш взгляд, станут определяющими как для крупных банков, так и для регулирования рынка в целом?

— Перспективы цифровизации у банков, как мне кажется, будут определяться горизонтом и масштабом экономического эффекта. Будут расти требования к гибкости и прозрачности. Например, решение задачи планирования требует вовлечения все большего числа участников, учета все большего количества вводных параметров и ограничений. При этом прогнозы должны будут оставаться интерпретируемыми — изменения финансовых показателей нужно будет объяснить всем участникам процесса. Это может кому-то показаться непростой задачей, но вполне реализуемой в ближайшей перспективе.

Для справки: Название компании: *Банк ВТБ, ПАО (Группа ВТБ)* Адрес: *191144, Россия, Санкт-Петербург, Дегтярный пер., 11, лит. А* Телефоны: *+78001002424; +7(495)7772424; +79103450535* E-Mail: *info@vtb.ru; pr@vtb.ru; aleksey.baranov@open.ru* Web: *https://www.vtb.ru* Руководитель: *Костин Андрей Леонидович, президент-председатель правления* (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

Интеллектуальное внедрение. "КоммерсантЪ". 11 декабря 2025

Как компаниям и госучреждениям эффективно использовать ИИ

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.

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 Б1 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. "Ъ" 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 Сидорюк.

Финансовый сектор, по словам господина 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, по словам руководителя направления ИИ в ИТ-холдинге Т1 Сергея Голицына, технологии искусственного интеллекта активно внедряются в государственное управление. Сектор использует ИИ для обработки обращений граждан, документооборота, прогнозирования и аналитики, контроля исполнения 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 Б1 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 Т1. Указ президента "О развитии искусственного интеллекта в Российской Федерации", подходы Минцифры России, а также основные направления 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 госпожа Егорова. В современном бизнесе искусственный интеллект стал крайне 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 технологии не решает проблемы госслужбы, а даже может стать дополнительной нагрузкой — сотрудникам приходится перепроверять 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 может 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 "Ъ" 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 снизит 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-компании) 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, автоматизирующее 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Экономика нейросетей. "КоммерсантЪ". 11 декабря 2025

Как бизнес учится измерять финэффекты от внедрения искусственного интеллекта

Рынок искусственного интеллекта давно перешел от этапа технологического эксперимента к массовой коммерциализации: ИИ-решения все активнее внедряются в банки, телеком, ритейл и облачные сервисы. Так, "Яков и партнеры" прогнозирует, что к 2028 году финансовый эффект от использования ИИ во всем мире будет составлять $17-26 трлн в год, а в России экономический потенциал этой технологии достигнет 22-36 трлн руб.
Вместе с объемом рынка растут и потребности бизнеса. Автоматизация, персонализация и ускорение процессов уже дают измеримые экономические эффекты и влияют на рост прибыли в будущем. На конференции AI Journey директор по ИИ Т-Банка Виктор Тарнавский рассказал, что компании уже не хотят просто разрабатывать и внедрять ИИ из-за тренда на него, они начинают задавать правильный вопрос: "Как же грамотно применять ИИ так, чтобы технология действительно принесла бизнесу пользу"? Но он отмечает, что правильно рассчитывать эффекты от применения нейросетей - это достаточно сложная задача, потому что ИИ - это все-таки прикладная технология, а не конечный продукт.
От прямой экономии к трансформации бизнес-моделей
Компании сталкиваются сегодня с некоторыми барьерами массового внедрения ИИ в бизнес-процессы, считает директор центра бизнес-образования и аналитики Центрального университета, партнер-эксперт "Яков и партнеры" Илья Иванинский. Так, по его словам, для того чтобы массово внедрять ИИ, в компании должна быть выстроена гибкая и стабильная ИТ-инфраструктура. "Бизнес только учится правильно измерять эффекты от внедрения технологий, есть и кадровые ограничения - только формируется класс руководителей и инженеров, которые понимают, какие технологии нужно внедрять и для чего". Однако он отмечает, что крупный бизнес уже широко использует ИИ для достижения целого ряда эффектов.
Это подтверждают и в Т-Банке. По словам Виктора Тарнавского, результаты от применения ИИ могут быть разного типа. Один из них - прямые экономические эффекты, которые отражаются в P&L компании за год. В основном они связаны с операционными затратами, где ИИ повышает эффективность разных функций, например поддержки или продаж, путем оптимизации издержек или персонала. Однако существуют и другие способы влиять на P&L, например, улучшать рекомендацию продуктов, замечает господин Тарнавский. "Если ты рекомендуешь свои продукты, особенно в цифровом мире, более правильным клиентам, то стоимость привлечения одного клиента на продукт получается меньше. Это измеримый эффект от ИИ, от которого можно посчитать пользу в денежном

эквиваленте",- поясняет он. Другой пример - экономические эффекты будущего. Их нельзя посчитать прямо сейчас, но в долгосрочной перспективе для компаний они показывают большие финансовые результаты.

Так, долгосрочные эффекты делятся на несколько категорий, замечает Виктор Тарнавский. Первая категория - это проекты, связанные с ускорением работы сотрудников в штате, например, в областях разработки или аналитики. "Компания начинает развиваться быстрее, решает свои задачи в ускоренном темпе, но быстро этот эффект нельзя перевести в деньги прямым образом. Поэтому такие изменения характеризуются "эффектами будущего дня", которые отражают быстрое движение компании и ее результативность",- объясняет эксперт.

Вторая категория - это "эффекты на лояльность", характеризующиеся проектами компании, от которых ее конечный клиент становится счастливее. "Такие эффекты влияют на удержание клиента, на его долгую лояльность по отношению к бизнесу, однако их также сложно посчитать в моменте, потому что они показывают результат в перспективе ближайших пяти или десяти лет",- напоминает Виктор Тарнавский.

Однако есть еще и нефинансовые эффекты. В проекты с такими метриками предприниматели инвестируют средства, но ожидают не денежных результатов, а улучшения других показателей. Например, к ним относятся системы безопасности, которые защищают средства пользователей и повышают уровень доверия к бизнесу. Нефинансовые эффекты также могут повлиять на отношения с инвесторами или на удовлетворенность сотрудников, напоминает господин Тарнавский.

В рамках Альянса искусственного интеллекта Т-Банк совместно с другими компаниями развивает методологию правильного подсчета эффектов от нейросетей. Компания выстроила несколько принципов работы с эффектами от ИИ в рамках такой методологии.

Во-первых, вести расчеты только через P&L. Это необходимо для того, чтобы учитывать исключительно те эффекты, которые напрямую связаны с ростом выручки или снижением затрат, не включая, например, потенциальные или брендовые эффекты.

Во-вторых, использовать в методологии только контролируемые подтвержденные эксперименты. Например, точные методы A/B-тестирования или длительные контрольные группы, результаты которых имеют научную доказательную базу и могут четко выделить влияние ИИ.

В-третьих, правильно учитывать стоимость затрат на ИИ. Из расчетов вычитаются все сопутствующие расходы: разработка моделей, инфраструктура, сторонние сервисы, операции, и от внедрения ИИ-технологий считается только чистый экономический эффект.

В-четвертых, выбирать строгие базовые сценарии сравнения. Здесь важнее проводить аналитику между лучшим доступным решением не на базе ИИ, чем с отсутствием решения вовсе. Например, рекомендации на базе ML оцениваются относительно уже существующих аналитических или rule-based-стратегий.

Так, по словам Виктора Тарнавского, на основе данной методологии Т-Банк уже рассчитал и внедрил для работы в компании три основных блока эффективности результатов от применения ИИ. Среди них, например, операционная эффективность, благодаря которой компания автоматизирует процессы, снижает трудозатраты и повышает скорость обслуживания в контактных центрах, бэк-офисе и операционной обработке. Еще один результат - ИИ-улучшение скоринговых и антифрод-моделей, которое снижает уровень финансовых рисков или потерь от мошенничества. Также при помощи нейротехнологий компания улучшила рекомендации и персонализацию продуктов для своих клиентов. Прямой экономический эффект в компании оценивают в десятки миллиардов рублей ежегодно.

"В Т-Банке уже сейчас 30% кода пишет ИИ, но эффекты, связанные с ускорением процессов, сложно измерить в деньгах: основную массу эффектов мы увидим в будущем, когда ИИ-системы станут значимо сильнее",- заключает Виктор Тарнавский.

Эффекты от применения ИИ видят и в "Яндексе". Там рассказали "Деньгам", что отмечают значительное повышение эффективности бизнес-процессов, а также сокращение времени на выполнение рабочих задач. "Половина разработчиков "Яндекса" уже использует ассистентов, за полгода их применение выросло в десять раз",- пояснили в пресс-службе компании. Там добавили, что после внедрения ИИ-агента в службу поддержки "Яндекс Такси" нейросеть стала сама решать 60% текстовых обращений, что позволило в 1,5 раза увеличить скорость ответа пользователям. "Ожидается, что автоматизация позволит сервису сэкономить на операционных расходах более 600 млн руб. в 2026 году",- прогнозируют в компании.

В "Сбере" говорят, что, по их оценкам, уровень проникновения генеративного ИИ среди российского бизнеса достиг отметки 70-80%. Там добавляют, что интеграция нейросети GigaChat в бизнес-процессы "Сбера" позволила кратно повысить их скорость и эффективность, а финансовый эффект от внедрения технологии в компании в текущем году может достигнуть 50 млрд руб.

Бизнес смотрит в нейробудущее

Одним из главных трендов на рынке в 2026 году будет появление единой технологической среды, которая становится основой для ИИ-трансформации компаний, считают в MWS AI (входит в МТС). Такой средой выступают платформы, в которых организации могут в едином окне и без программирования создавать и управлять ИИ-агентами, а также тестировать ключевые гипотезы, объясняет гендиректор компании Денис Филиппов. "Бизнес стремится получать финансовый эффект, а для этого необходимо, чтобы каждое решение было измеримым",-

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

заключает эксперт. С ним соглашаются в "Яндексе", отмечая, что внедрение ИИ-агентов и мультиагентских систем в бизнес характеризуется тем, что они умеют самостоятельно определять, как выполнить задачу, и взаимодействовать с внешними приложениями.
В "Сбере" считают, что в 2026 году значительно увеличится спектр профессий, где генеративный ИИ станет незаменимым инструментом повышения производительности труда, важнейшей тенденцией будет широкое распространение физических воплощений технологии - роботизированных устройств и автономных транспортных средств.
"ИИ влияет на современное общество в самых разных аспектах: его положительное воздействие распространяется от медицины и физики до маркетинга и индустрии развлечений",- считает Илья Иванинский. Глобальный тренд в этой сфере - это то, что ИИ будет распространяться все дальше и быстрее, через пару лет уже не останется компаний, которые не используют нейросети в своих бизнес-процессах, заключает эксперт. (КоммерсантЪ 11.12.25)
К СОДЕРЖАНИЮ

Иностранный бизнес позарился на российские ИИ-решения. "ComNews.ru". 16 декабря 2025

70% представителей иностранного бизнеса высказались за интеграцию российских ИИ-технологий в инфраструктуру компаний. 20% зарубежных компаний полностью доверяют разработчикам из России. Однако 30% считают, что при интеграции решений могут столкнуться с проблемой их совместимости с зарубежным программным обеспечением.
Компания WMT AI (входит в WMT Group - ООО "Изи прожектс") в рамках участия в первой Всемирной выставке искусственного интеллекта (ИИ) AIE 2025 в Макао провела исследование, из которого выяснила, что 70% представителей иностранного бизнеса выразили готовность интеграции российских ИИ-технологий в инфраструктуру компаний. Единственное требование для них - возможность предварительного тестирования ИИ перед внедрением. При этом полностью доверяют ИИ-разработчикам из России 20% респондентов, а 10% опрошенных вообще не видят необходимости использования зарубежного ИИ.
В исследовании приняли участие иностранные представители ИТ бизнеса, промышленности, образования, здравоохранения и других сфер. Большинство опрошенных - 60% - относятся к малому и среднему предприятию с численностью персонала до 300 человек. 30% - компании со штатом 300-700 сотрудников, а также крупные игроки на рынке с численностью от 700 человек - 10%.
"ИИ в российской деловой среде перешел из стадии эксперимента в инструмент массового применения - его уже используют две трети компаний. Однако текущее внедрение часто фрагментарно и сосредоточено на аналитике и автоматизации. Чтобы превратить этот тренд в устойчивое конкурентное преимущество, бизнесу необходимо двигаться от точечных решений к комплексной цифровой трансформации, инвестируя в компетенции и подготовку данных. Ключом к выходу на международную арену станет не просто импортозамещение, а создание адаптивных, "бесшовных" отечественных ИИ-платформ, способных интегрироваться в глобальные цепочки", - сказал основатель WMT Group и WMT AI Игорь Никитин.
"Перспективы на новых рынках мы оцениваем осторожно. Там мы сталкиваемся с новыми конкурентами, мировыми игроками, лидерами отрасли, и это в том числе является драйвером нашего развития. Помимо глобальных игроков, конкурентами являются стартапы и локальные команды. По сути, на новых рынках мы и сами стартап, поэтому должны думать и действовать как стартап - быстро, инновационно и адаптивно. Подходить через асимметрию и контрпозиционирование в противовес мировым лидерам отрасли", - отметил директор департамента "Банки и финансы" ООО "Рексофт" Алексей Лебедев.
"На мой взгляд, интеграция российских ИИ-технологий в иностранную инфраструктуру - это взаимовыгодный процесс. Видится, что этот путь может ускорить цифровую трансформацию зарубежных компаний и одновременно усилить позиции России как технологического лидера", - считает руководитель проектов развития AI-решений ООО "Директум" (Directum) Илья Петухов.
"Ключ к успеху - это концепция "бесшовной" интеграции. Будущее за теми российскими компаниями, которые изначально проектируют решения как часть глобальной цифровой экосистемы, а не как изолированный продукт, который потом придется адаптировать. Это требует инвестиций и стратегического видения, но именно такой подход превратит интерес иностранного бизнеса в реальные контракты", - уверен директор по развитию ИИ и web-технологий Artezio (входит в ГК "Ланит") Сергей Матусевич.
Почти треть компаний (30%) видят основной риск использования российских ИИ-разработок в сложности интеграции их с зарубежным программным обеспечением. Надежность и достоверность данных, предоставляемых российскими ИИ, беспокоит 26% респондентов, а риск утечек и компрометации данных - 24%. Актуальность и своевременность обработки данных вызывает опасения у 12%, низкая скорость работы ИИ-решений - лишь у 8% компаний.
Руководитель центра компетенции GenAI "Дар" (входит в ГК "КОРУС Консалтинг") Игорь Терехин назвал три основные группы рисков внедрения ИИ: "Во-первых, это доверие к данным и прозрачность работы ИИ. Для международного рынка критичны вопросы explain ability (свойство системы ИИ, позволяющее человеку понять причину принятия того или иного решения - прим. ComNews), воспроизводимости результатов, контроля качества

данных и моделей. Во-вторых, это информационная безопасность и комплаенс. Иностранные компании очень внимательно относятся к вопросам хранения данных, трансграничной передачи, стараются соответствовать локальным требованиям (GDPR, отраслевые стандарты). Наконец крайне важна операционная зрелость поставщика. Поддержка, SLA, обновления, жизненный цикл продукта, способность решения масштабироваться вместе с бизнесом заказчика - это часто более существенный барьер, чем сама технология".

"Сложности интеграции российских ИИ-решений с зарубежным ПО возможны, но в большинстве случаев это решаемая инженерная задача в случае, если продукт изначально рассчитан на внедрение: есть стандартные интерфейсы интеграции, документация и пилотный контур. В этом смысле российские технологии готовы к массовой интеграции, но не "в среднем по рынку", а там, где решения доведены до продуктового уровня и поставщик умеет сопровождать их в продакшене", - отметил технический директор ООО "Осми-ИТ" (OSMI IT) Денис Нагаев.

"Западный комплаенс (GDPR) и российские требования регуляторов к безопасности - разные философии, а не просто стандарты. Запад выбрал приватность, мы ставим контролируемость и интерпретируемость в ИИ. Датасет каждой компании уникален, и адаптировать его под оба режима станет вызовом. Иностранные компании привыкли к западным стандартам верификации, а наши аудиты безопасности идут глубже и жестче. Но это не цена бюрократии - это цена суверенной защиты. После такого аудита заказчик получает гарантию, которую не даст ни один западный вендор", - считает директор по ИИ группы компаний "Астра" Станислав Ежов.

Однако директор департамента проектирования и разработки ООО "ИБС Экспертиза" (IBS) Максим Ковтун уверен, что сложности в интеграции не возникнет совсем: "В базе решений российских компаний лежат общедоступные решения, технологические механизмы интеграции также общеприняты, поэтому каких-то технологических сложностей я не вижу. Может возникнуть вопрос релевантности данных, на которых обучена модель, но он решается путем предварительного тестирования".

Технический директор ООО "МД Аудит" (MD Audit, входит в ГК Softline) Юрий Тюрин рассказал о выгоде обеих сторон от внедрения российских ИИ-технологий: "Для иностранного бизнеса ключевая выгода - доступ к конкурентоспособным ИИ-инструментам, которые позволяют ускорять процессы, повышать качество аналитики и запускать новые цифровые сервисы. Для российского рынка - это возможность выхода в международные цепочки создания ценности, накопление опыта внедрения в сложных гетерогенных средах и повышение зрелости продуктов. В долгосрочной перспективе такие интеграции стимулируют развитие экспортно ориентированных ИИ-платформ и усиливают технологическую кооперацию на уровне решений, а не отдельных экспериментов".

"Я не вижу практических примеров интеграции вне РФ, где мы интегрируем ИИ с уже существующими техплатформами, которые еще не замещены или не будут замещены. История про фактическую интеграцию крупных ИИ-решений пока представляется скорее фантастической", - убежден генеральный директор ООО "Экспанта" Александр Смоленский.

"Для иностранных компаний российские ИИ-решения станут эффективной альтернативой крупным американским вендорам, что позволит снизить зависимость и диверсифицировать поставщиков технологий. Кроме того, российское ПО зарекомендовало себя как более доступное по стоимости без потери в качестве, что ведет к сокращению издержек. Таким образом, сотрудничество создает взаимовыгодный эффект - ситуацию "вин-вин" для обеих сторон", - считает основатель ИИ-поиска "Жижи" Алексей Нечаев.

На иностранном рынке подавляющее большинство компаний уже активно используют ИИ в рабочих процессах - 66,7%. Еще 23,3% находятся на пилотном или тестовом этапе внедрения. Пока не рассматривают возможность использования ИИ в работе 6,7% опрашиваемых, а планируют начать использование только 3,3%. (ComNews.ru 16.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Автоматизация

ММК получил награду ComNews за лучший проект в металлургии.

Магнитогорский металлургический комбинат (ММК) стал лауреатом престижной ИТ-премии "ComNews Awards. Лучшие решения для цифровой экономики", получив награду в номинации "Лучший проект в металлургии". Высокой оценки экспертов удостоилась успешно реализованная автоматизированная система управления сквозными материальными потоками между кислородно-конвертерным цехом и листопрокатными цехами №10 и №4.

Решение, разработанное специалистами АО "КОНСОМ СКС" и ООО "ММК-Информсервис" совместно с ПАО "ММК" и ООО "Объединенная сервисная компания", обеспечивает комплексный мониторинг и управление движением материалов на всех этапах в сталеплавильном и прокатном переделах.

"Эта система объединяет производственные и технологические данные в едином цифровом контуре, работая в режиме реального времени. Это создает полную прозрачность логистики, начиная от производства слябов и заканчивая отгрузкой готовой продукции", — отметил Андрей Картунов, начальник научно-технического центра.

На основе технологий Big Data реализован интеллектуальный анализ потоков и прогнозирование узких мест. Система обеспечивает своевременное и точное информационное сопровождение процессов планирования и управления производством, предоставляя данные о позиционировании каждой единицы металлопродукции на всех этапах технологического маршрута. Кроме того, система прогнозирует время поступления металлопродукции на контролируемые участки, позволяет автоматизировано управлять поставками. Решение позволило исключить человеческий фактор из процесса контроля за сопровождением металлопродукции по переделам.

В рамках проекта создан комплекс программно-аппаратных решений, включающий систему машиночитаемой маркировки, интеграцию весоизмерительных комплексов и корпоративных систем, а также инструменты визуализации и аналитики.

Сегодня эта система позволила предприятию выйти на новый уровень эффективности, управляемости и достоверности данных.

Для справки: Название компании: *ММК-Информсервис, ООО* Адрес: *455019, Россия, Челябинская область, Магнитогорск, пр. Пушкина, 2* Телефоны: *+7(3519)240111* Факсы: *+7(3519)240112* E-Mail: *it@mmk.ru* Web: *http://is-mmk.ru* Руководитель: *Феоктистов Вадим Николаевич, директор* (По материалам компании 11.12.25)

К СОДЕРЖАНИЮ

Роботизация

Плотность роботизации в России в 2025 году увеличится на 36%.

По данным Kept и "Промышленной робототехники", плотность роботизации в России в 2025 году составит 40 роботов на 10 тыс. работников, увеличившись на 36%. В прошлом году отношение числа промышленных роботов к количеству сотрудников на предприятии (плотность роботизации) увеличилось на 53%, до 29 машин на 10 тыс. работников.

Согласно указу президента Владимира Путина о национальных целях развития, Россия к 2030 году должна войти в топ-25 стран по показателю плотности роботизации. В Kept и "Промышленной робототехнике" считают, что по консервативному сценарию плотность роботизации к 2030 году в России не достигнет этой цели и составит 134 робота на 10 тыс. работников. При таком сценарии среднегодовой темп прироста "будет выше мирового и составит 29%, что характерно для стран догоняющего развития", а общий парк достигнет 95,9 тыс. штук.

По оптимистичному сценарию прирост плотности будет на уровне 36%, что позволит к 2030 году достичь показателя в 185 роботов на 10 тыс. работников, уточняют аналитики Kept и "Промышленной робототехники". Объем парка роботов к 2030 году с учетом позитивного прогноза достигнет 131,8 тыс. единиц промышленных машин.

На консервативный сценарий влияют факторы, которые снизили темпы прироста в прошлом году, объяснили в Kept и "Промышленной робототехнике": снижение закупочной активности предприятий, спад производительности промсектора, сокращение инвестиционной активности из-за высокой ключевой ставки. (КоммерсантЪ 09.12.25)

К СОДЕРЖАНИЮ

В России роботизировали процессы в области энергетики и сэкономили 38 млн рублей.

В Управлении главного энергетика Магнитогорского металлургического комбината (ММК) создана безошибочная система управления энергоресурсами на основе RPA (роботизированной автоматизации процессов). Программные роботы в режиме 24/7 готовят отчеты до начала смены, прогнозируют поломки оборудования, обрабатывают заявки и выполняют другую рутину. Об этом CNews сообщили представители ООО "ЦТР "Некст".

RPA (Robotic Process Automation) – технология автоматизации рутинных задач с помощью программных роботов. В промышленности RPA применяют для управления ресурсами, контроля качества и операционной отчетности.

Контекст и задачи проекта

Управление главного энергетика обеспечивает работу всего металлургического производства (ММК), объединяя три собственные электростанции, цех электросетей и подстанций, паросиловой и газовый цехи, цех водоснабжения, кислородный и энергоцех, а также цехи инженерного обеспечения, центр энергосберегающих технологий и центральную электротехническую лабораторию. В 2024 г. совокупное потребление энергии предприятиями группы ММК составило 327,95 млн ГДж.

Целью проекта по внедрению RPA – технологии роботизированной автоматизации процессов – была не просто оптимизация рутины, а создание безошибочной системы управления.

Реализация и ключевые роботизированные процессы

Интегратор и разработчик RPA – Центр технологий роботизации "Некст" роботизировал в Управлении главного энергетика 22 процесса в четырех функциональных областях: управление материально-техническими ресурсами (МТР); управление техобслуживанием и ремонтами оборудования; формирование отчетов с технико-экономическими показателями; учет и прогнозирование электроэнергии.

Примеры роботов и эффекты от них

Робот-аналитик запасов готовит отчет за один час вместо двух дней, предоставляя данные по запросу в любой момент. Робот-обработчик заявок работает круглосуточно и завершает многоэтапную проверку данных за два дня вместо недели.

Робот-складской аудитор полностью исключает повторные закупки идентичного оборудования. Робот-аудитор дефектов на 40% сокращает среднее время устранения неисправностей за счет превентивного мониторинга.

Робот-составитель рапортов формирует 100% точные суточные отчеты ночью, экономя до двух часов рабочего времени начальников цехов ежедневно.

Робот-ремонтный координатор формирует ежемесячный отчет за два часа вместо трех дней.

Эффекты от внедрения RPA

Экономический эффект: 38 млн руб. накопленной экономии с 2019 г. за счет предотвращения простоев, штрафов и оптимизации ФОТ.

Для справки: Название компании: *Магнитогорский металлургический комбинат, ПАО (ММК, ИНН 7414003633)* Адрес: *455000, Россия, Челябинская область, Магнитогорск, ул. Кирова, 93* Телефоны: *+73519247709* Факсы: *+73519247309* E-Mail: *infommk@mmk.ru; Gavrishev.ks@mmk.ru* Web: *http://www.mmk.ru* Руководитель: *Шиляев Павел Владимирович, генеральный директор* (Cnews.ru 16.12.25)

К СОДЕРЖАНИЮ

Алтайское предприятие активно использует в производственном процессе роботов.

Производитель замороженных мучных полуфабрикатов "Алтайхлеб" лидирует в Сибири по объемам производства и один из первых в стране по прибыли среди родственных предприятий. А в этом году он стал победителем в трудовом соревновании работников пищевой и перерабатывающей промышленности Алтайского края. Мы приехали на завод, чтобы понять, за счет чего коллективу удается добиться таких результатов.

Перед тем как познакомить с производством, для журналистов провели инструктаж по технике безопасности.

– Если вы видите, что едет робот или человек, управляющий рохлей (гидравлическая тележка для поддонов. – Прим. ред.), то организованно, как железнодорожники, в одну сторону отходим и пропускаем его, – объясняет журналистам директор предприятия Дмитрий Гостяев. Вместе с ним заходим в цех, преодолевая дверь, электронный замок которой открывается по отпечатку пальца директора, и попадаем на участок приготовления слоеного теста.

– Это немецкий тестомес, это китайская линия, – рассказывает экскурсовод. – В смесь, помимо дрожжей, муки и соли, добавляем лед, чтобы она была холодной и маргарин не растекся.

Ледяную крошку производят тут же две машины. Она ссыпается в емкость, которую пока поднимают вверх с помощью лифта вручную, но скоро этот процесс автоматизируют: лед пойдет по шнеку.

Обычно на хлебозаводах дежу (емкость) с готовым тестом катят к машине, которая его разделывает. Здесь этот вопрос решен по-другому. Дно дежи открывается, тесто проваливается в приемную воронку и по транспортерам направляется на линию. Нож его делит на куски. Весь процесс контролирует молодой человек по имени Курбан. Он внимательно следит на пульте за подачей ингредиентов в тестомес и периодически отщипывает от общей массы кусок, мнет его руками, определяя таким образом ее готовность.

Этот парень зарабатывает в месяц около 100 тыс. рублей, так как находится в начале технологического процесса и его ошибка обойдется предприятию дорого. А в конечном счете и Курбану. Но за большую ответственность и платят хорошо. Хотя и других не обижают: в этом году средняя зарплата в компании выросла на треть.

Тем временем тесто по транспортерам приехало в цех слоеных изделий на линию по производству круассанов. Валы раскатывают его в тонкий широкий пласт, на который сверху по центру поступает слой маргарина. Затем валики заворачивают края теста так, что маргарин оказывается внутри. Этот конверт вновь раскатывают. Таким образом формируется первый слой. Но в тесте в зависимости от вида изделия их должно быть от 36 до 120. И машина умудряется получить такой результат, разрезая непрерывный пирог на части и накладывая сразу несколько стопкой и вновь раскатывая. Количество слоев растет в геометрической прогрессии.

На заключительном этапе машина разрезает тесто на треугольники, наносит на них шоколадную начинку и с помощью вакуума закручивает. Готовые круассаны по транспортеру едут в камеру расстойки, где тесто в теплом и влажном воздухе поднимается. На заводе наличие камер расстойки считают своим конкурентным преимуществом, так как пекари в магазинах экономят на этом время. Тесто практически готово к выпечке, но, перед тем как попасть в магазин, идет в камеру шоковой заморозки, где -35 оС.

За смену получается 80 тысяч изделий. Их упаковывают в коробки частично с применением ручного труда, а затем роботы отвозят на склад готовой продукции, который полностью автоматизирован. Там нет шныряющих вдоль стеллажей электрокаров и людей. На складе вообще нет свободного пространства. Автоматика проверяет сохранность поддона и отправляет с помощью вертикальных и горизонтальных перемещений маленьких тележек в заданную точку. Благодаря этому удается максимально использовать объем помещения. Когда надо, поддон с нужной продукцией тележка доставит к автомобилю-рефрижератору, а он отвезет полуфабрикаты в магазин. На складе -20 ОС и темно, потому что роботам свет не нужен.

Но вернемся в цех, где на соседней линии производят хачапури по 120 тыс. штук за смену.

– Эта современная китайская линия превосходит европейские аналоги, – говорит оператор Дмитрий Толстов. Он управляет этим оборудованием с помощью планшета или смартфона. Толстов – бывший военнослужащий, трудится на предприятии третий месяц, но уже освоил сложный технологический процесс. Говорит, что ему нравится такая работа.

Помимо полуфабрикатов, предприятие еще производит салаты по 10 тонн в смену. Это "атавизм", который остался с давних пор, когда их делали только для "Марии-Ра", но теперь покупают "Пятёрочка" и "Магнит". Как скоропортящийся продукт, салаты возят не дальше 1000 км. Производство нам не показали, но упаковывает их в основном автоматика, причем часть линии изготовили местные механики. Для увеличения срока годности воздух из салата замещают смесью азота и углекислого газа.

Для справки: Название компании: *Алтайхлеб, ООО (ИНН 2221194848)* Адрес: *658087, Россия, Новоалтайск, ул. Октябренок, 68, корп. А* Телефоны: *+73852557262; +73852350510* E-Mail: *east@altayhleb.ru; ko4@altayhleb.ru; office@altayhleb.ru* Web: *http://altayhleb.ru/* Руководитель: *Гостяев Дмитрий Викторович, генеральный директор*

Для справки: Название компании: *Алтайхлеб, ООО (ИНН 2221194848)* Адрес: *658087, Россия, Новоалтайск, ул. Октябренок, 68, корп. А* Телефоны: *+73852557262; +73852350510* E-Mail: *east@altayhleb.ru; ko4@altayhleb.ru; office@altayhleb.ru* Web: *http://altayhleb.ru/* Руководитель: *Гостяев Дмитрий Викторович, генеральный директор* (INFOLine, ИА (по материалам Администрации) 10.12.25)

К СОДЕРЖАНИЮ

ГК ТОЧНО внедряет роботов Сколково в строительство ЖК "Первое место" (Краснодарский край).

Девелопер ТОЧНО (владелец — бизнесмен Николай Амосов) продолжает сотрудничество с Фондом "Сколково" (Группа ВЭБ.РФ).
В строительстве одного из самых масштабных проектов региона "Первое место" применят роботов и экзоскелеты.
ГК ТОЧНО анонсировала внедрение роботов и экзоскелетов в строительство ЖК "Первое место" — одного из крупнейших жилых комплексов в Краснодарском крае. В рамках рабочего визита строительную площадку проекта посетил директор по городским и строительным технологиям Фонда "Сколково" Юрий Хаханов.
Так, в рамках партнерства девелопер применит в строительстве ЖК "Первое место" разработки резидентов Сколково, участников акселератора Build UP — программы поиска и внедрения инновационных технологий в сфере строительства и девелопмента, партнером которого выступает ТОЧНО. Перспективные технологии уже прошли отбор экспертов фонда и проектной команды девелопера — ранее их презентовали на V Конгрессе молодых ученых, который на днях завершился на федеральной территории "Сириус".
Среди инновационных решений — экономичный робот-уборщик, который ранее представили Президенту России; роботизированный комплекс по укладке газобетона; высокопроизводительный робот для проведения сносно-демонтажных работ; а также эргономичные промышленные экзоскелеты, которые снижают нагрузку на позвоночник оператора до 30% при переносе и установке тяжелых блоков.
Девелопер отмечает: внедряемые технологии увеличат скорость и снизят себестоимость строительства. В планах ТОЧНО — применить перечисленные инструменты и на других проектах в восьми регионах присутствия.
"Год назад начали партнерство с Фондом "Сколково". Это не эксперимент, а системный поиск лучших решений. Мы делаем ставку на роботов, которые берут на себя сложную работу, повышая безопасность и эффективность. Уже сейчас тестируем роботизированные системы. Сотрудничество со Сколково превращает смелые идеи в инструменты, меняющие отрасль",— комментирует директор ГК ТОЧНО Анастасия Маслёха.
Напомним, что ГК ТОЧНО сотрудничает со Сколково с декабря 2024 года — команда девелопера рассмотрела более 500 разработок в рамках акселератора Build UP.
"Уже более 10 лет Сколково поддерживает перспективные проекты в сфере робототехники, предоставляя грантовое финансирование, доступ к инфраструктуре, менторство и возможность для первых контактов и реализации пилотных проектов. Благодаря комплексным мерам поддержки создаются передовые технические решения, которые находят практическое применение в том числе у ведущих девелоперов недвижимости в рамках отраслевой программы Build UP",— рассказал директор по городским и строительным технологиям Фонда "Сколково" Юрий Хаханов.
"Первое место" — проект комфорт-класса из 18 кварталов площадью более 71 га, который реализуется в микрорайоне Новознаменский, в северо-восточной части Краснодара. В жилом районе запланированы 31 многоквартирный дом переменной этажности — от 8 до 18 этажей, а также насыщенная инфраструктура: две школы, шесть детских садов, детская и взрослая поликлиники. Сегодня здесь уже открыты и принимают детей школа на 1100 учеников и детский сад на 250 мест. В активной стадии проектирования — храмовый комплекс в честь иконы Божией Матери "Знамение".
До конца 2025 года купить квартиру в ЖК "Первое место" можно со скидкой до 26% по акции "Берите сейчас, но это вам на Новый год".

Для справки: Название компании: *Группа компаний ТОЧНО, ООО (ГК ТОЧНО, ИНН 2312295177)* Адрес: *350061, Россия, Краснодарский край, Краснодар, ул. им. Мачуги В.Н., д. 108, оф. 115* Телефоны: *+78612138201* E-Mail: *info@tochno.life* Web: *https://tochno.life/* Руководитель: *Маслеха Анастасия Владимировна, директор; Амосов Николай Андреевич, председатель Совета директоров*

Для справки: Название компании: *Государственная корпорация развития ВЭБ.РФ (ИНН 7750004150)* Адрес:

125009, Россия, Москва, ул. Воздвиженка, 10 Телефоны: *+74956046363* Факсы: *+74957219291* E-Mail: *info@veb.ru* Web: *https://вэб.рф/* Руководитель: *Шувалов Игорь Иванович, председатель*

Для справки: Название компании: *Фонд развития Центра разработки и коммерциализации новых технологий, НО (Фонд Сколково)* Адрес: *121205, Россия, Москва, территория инновационного центра «Сколково», ул. Нобеля, д. 5* Телефоны: *+74959560033; +78002500921* Факсы: *+74957395306* E-Mail: *skfoundation@sk.ru; skzakupki@sk.ru* Web: *https://sk.ru/* Руководитель: *Перов Сергей Евгеньевич, председатель Правления* (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

Предприятия Тульской области активно внедряют промышленных роботов на производствах.

11 сентября в Москве под председательством Полномочного представителя Президента РФ в ЦФО Игоря Щёголева состоялось заседание Инвестиционного совета Центрального федерального округа.
От Тульской области в мероприятии принял участие заместитель председателя Правительства Павел Татаренко.
Заместитель председателя Правительства сообщил, что Тульская область входит в группу регионов, активно внедряющих роботизацию (топ-15 по итогам 2024 года). На предприятиях обрабатывающей промышленности региона используются сотни промышленных роботов. На ряде площадок, в том числе в крупном частном секторе, плотность роботизации существенно превышает средний мировой уровень. Например, на производственном комплексе "Металл-Пласт" показатель плотности роботизации составляет 415 машин на 10 000 сотрудников, что почти в 3 раза выше среднемировых значений. Это показывает, что при грамотной организации процессов за короткое время роботизация может стать реальным производственным стандартом.
В этом году делегация Тульской области во главе с Губернатором Дмитрием Миляевым посетила Челябинский кузнечно-прессовый завод и его дочернюю компанию "Завод роботов". Их опыт взят за основу при формировании нашей региональной модели. Одно из ведущих предприятий ОПК региона — НПО "Сплав" - и "Завод роботов" заключили соглашение о сотрудничестве. Так, на базе тульского предприятия будет создан центр по обучению роботизации.
Кроме того, в Тульском государственном университете будет создан Центр промышленной робототехники. Сейчас вуз участвует в отборе центров компетенции по роботизации в рамках национального проекта "Средства производства и автоматизации". Это позволит объединить возможности образования, науки и промышленности: создавать и тестировать роботизированные участки, готовить инженеров новых компетенций, сопровождать предприятия на всех стадиях внедрения роботизации.
На заседании Павел Татаренко обозначил вопросы, сдерживающие на сегодняшний день развитие роботизации. Один из них – дефицит высококвалифицированных кадров, способных сопровождать все этапы роботизации производства. Второй — фискально-регуляторный, заключающийся в подходах к ценообразованию по государственному оборонному заказу (ГОЗ).
"Для Тульской области роботизация – это практический инструмент выполнения задач, поставленных Президентом Российской Федерации и Правительством Российской Федерации по укреплению обороноспособности, достижению технологического суверенитета и росту производительности труда", - подчеркнул Павел Татаренко.
Инвестиционный совет ЦФО поддержал предложения тульского региона по интеграции региональных центров роботизации в систему федеральных проектов по подготовке кадров и развитию средств производства, совершенствованию ценообразования по ГОЗ с учётом задач роботизации предприятий и развитию финансовых и организационных механизмов поддержки комплексных проектов роботизации.

Для справки: Название компании: *Завод Роботов, ООО (ИНН 7449141049)* Адрес: *454012, Россия, Челябинская область, Челябинск, ул. Горелова, 12, офис 608* Телефоны: *+73512020365* E-Mail: *info@robotfactory.ru* Web: *https://robotfactory.ru; https://rusrobot.ru/* Руководитель: *Горькуша Александр Сергеевич, генеральный директор*

Для справки: Название компании: *Научно-производственное объединение СПЛАВ имени А.Н. Ганичева, АО (НПО СПЛАВ)* Адрес: *300004, Россия, Тульская область, Тула, ул. Щегловская засека, 33* Телефоны: *+7(4872)464800; +7(4872)464409* E-Mail: *mail@splavtula.ru* Web: *http://splav.org* Руководитель: *Смирнов Александр Владимирович, генеральный директор* (INFOLine, ИА (по материалам Администрации Тульской области) 11.12.25)

К СОДЕРЖАНИЮ

"Пулково" ждет внедрение ЭПР для запуска беспилотных роботов во II квартале 2026 года. "Ведомости. Санкт-Петербург". 11 декабря 2025

Аэропорт к 2028 г. рассчитывает начать полноценное использование роботов-тягачей и роверов-охранников

Запуск экспериментального правового режима (ЭПР) для использования беспилотных технологий должен состояться в аэропорту "Пулково" во II квартале 2026 г. Таким прогнозом поделились в пресс-службе компании "Воздушные ворота Северной столицы" (оператор аэропорта). Полноценную эксплуатацию беспилотной техники планируют начать к 2028 г.

На федеральном уровне работу по запуску ЭПР по использованию беспилотной наземной техники на территории аэропортов ведут Минэкономразвития совместно с Минтрансом. "Ведомости Северо-Запад" направили запросы в эти ведомства о сроках принятия соответствующего постановления правительства РФ.

В ноябре 2025 г. в Минэкономразвития сообщили, что программу эксперимента и проект постановления об установлении нового экспериментального правового режима по использованию беспилотной наземной техники на территории аэропортов Москвы, Сочи и "Пулково" в Санкт-Петербурге планируют внести на рассмотрение в Правительство РФ в 2026 г. Директор департамента цифрового развития и экономики данных Минэкономразвития Владимир Волошин тогда же отмечал, что для тестирования режима обсуждается использование технологий российского производства - беспилотных тягачей для перевозки багажа пассажиров.

Каких роботов будут внедрять в "Пулково"

ВВСС в рамках ЭПР планируют начать внедрение беспилотного багажного тягача от компании Cognitive Pilot. Форвардный контракт между компанией Cognitive Pilot и ООО "Воздушные ворота Северной столицы" об использовании полностью беспилотного и бескабинного робота-тягача для задач авиагавани подписали 25 июня 2025 г. в Министерстве промышленности и торговли РФ. В рамках соглашения, до конца 2028 г. оператор аэропорта может закупить у компании до 45 единиц беспилотной техники.

В октябре "Пулково" начал испытания робота-тягача в условиях максимально приближенных к реальным. Тестирование, которое стартовало на специальном закрытом участке, продлится до конца марта 2026 г. На первоначальном этапе тягач будет доставлять багаж к воздушному судну и от воздушного судна. Еще один робот, которого начнут использовать в аэропорту после запуска ЭПР - ровер-охранник. Его будут применять для патрулирования территории аэропорта. Ровер начали тестировать в 2025 г. Однако в пресс-службе не сообщили, сколько таких роботов планируется запустить в следующем году.

"Пулково" - один из первых аэропортов в России, который проводит полномасштабные испытания подобных решений. При этом ни один робот не будет допущен к самостоятельной работе без прохождения полного цикла тестирования и строгого соответствия требованиям безопасности", - сказал изданию "Ведомости Северо-Запад" директор по инновациям аэропорта Григорий Кузнецов.

Ранее "Ведомости" со ссылкой на генерального директора ВВСС Леонид Сергеева писали, что в среднесрочной перспективе компания планирует вложить в развитие беспилотных технологий и роботизации на территории аэропорта не менее 500 млн руб. Это позволит оптимизировать от 5 до 15% расходов на персонал, которые составляют 66% от всех расходов аэропорта, отмечал Сергеев. По данным ВВСС, в настоящее время в операционной деятельности аэропорта задействовано около 340 единиц техники. В пресс-службе добавили, что к 2030 г. около 30% всей аэродромной техники в "Пулково" будут составлять беспилотные технологии, которые смогут работать в автономном режиме.

В пресс-службе также отметили, что внедрение беспилотных технологий позволит повысить эффективность операций, сократить время обслуживания и перераспределить персонал на более сложные и квалифицированные задачи. Помимо этого в рамках долгосрочной стратегии "Пулково" по цифровой трансформации и автоматизации ключевых процессов в 2026 г. петербургский аэропорт в качестве пилотной площадки начнет тестирование на ограниченной группе пользователей российского сервиса посадки на самолет по биометрии "Мигом". В октябре текущего года в аэропорту завершили монтаж и настройку необходимого оборудования для тестирования полного функционала сервиса. Однако для реализации проекта также необходимо подготовить ряд изменений в законодательство. По подсчетам оператора аэропорта, внедрение автономных машин и биометрии способно обеспечить ежегодную экономию свыше 150 млн руб.

И экономия, и риски

Как отмечают эксперты, опрошенные изданием, в долгосрочной перспективе благодаря внедрению беспилотных технология аэропорт сможет экономить за счет снижения операционных затрат, увеличения пропускной способности, а также уменьшения выбросов и шума, что снизит затраты на экологические платежи. Эксперт практики бизнес-консультирования "Технологии Доверия" (ТеДо) Александр Герасимов уточнил, что в течение нескольких лет экономия от внедрения беспилотных устройств может составлять несколько сотен млн руб.

"Несмотря на значительные затраты на приобретение и внедрение роботов, их эксплуатация обходится дешевле, чем содержание эквивалентного штата людей и техники в старой парадигме. Особенно заметна выгода на длительном горизонте, когда первоначальные инвестиции окупятся", - сказал он.

Кроме того, одним из главных эффектов от внедрения беспилотных устройств станет повышение точности и предсказуемости операций. Партнер практики "Цифровая трансформация" компании Strategy Partners Сергей Кудряшов, ссылаясь на данные швейцарской компании Assaia, пояснил, что внедрение ИИ в наземное обслуживание аэропортов сокращает медианную задержку вылетов на 25%. "Для аэропорта масштаба "Пулково" с более 20 млн пассажиров в год это означает существенное улучшение операционных показателей и снижение

компенсационных выплат", - добавил он. Кудряшов также подчеркнул, что роботизация транспортного узла позволит решить проблему дефицита кадров в авиационной отрасли, где фиксируется острая нехватка персонала на позициях наземного обслуживания.
В то же время эксперты обращают внимание и на риски, связанные с внедрением беспилотной техники на критически важной инфраструктуре, такой как аэропорты. "Количество кибератак на авиационную отрасль выросло на 74% с 2020 г. Автономные роботы - это подключенные устройства с программным управлением, и они становятся потенциальными точками входа для злоумышленников. Компрометация системы управления беспилотным парком может привести к остановке наземных операций, а в худшем случае - к инцидентам безопасности на летном поле", - отметил Кудряшов.
Второй блок рисков, по его словам, напрямую связан с обеспечением непрерывной работы беспилотных технологий. Аэропорту необходимо подготовить план действий при массовом отказе беспилотных устройств, иметь резерв ручных операций и план по переключению на альтернативные сценарии работы.
Герасимов, в свою очередь, отметил, что указанные риски можно контролировать при грамотном подходе. "Аэропорт "Пулково", как пионер, фактически испытывает на себе все эти вызовы, чтобы затем предложить отработанные решения другим. Уже сейчас видно понимание: тестирование ведется постепенно, сперва в ограниченном режиме с операторами, юридические моменты закрыты ЭПР, создана IT-система для интеграции, персонал обучается. Да, риски есть, но они не являются непреодолимыми", - заключил он.

Для справки: Название компании: *Аэропорт Пулково, АО* Адрес: *196210, Россия, Санкт-Петербург, ул. Внуковская, 2* Телефоны: *+7(812)6120512; +7(812)6120500; +7(812)6120520* Факсы: *+7(812)6120509* E-Mail: *office@airport-spb.ru* Web: *www.airport-spb.ru* Руководитель: *Бабюк Ирина Анатольевна, председатель Совета директоров; Чернышев Ростислав Сергеевич, генеральный директор* (Ведомости. Северо-Запад 11.12.25)

К СОДЕРЖАНИЮ

От доставки до строительства: в каких городских профессиях осваиваются роботы. "Ведомости". 12 декабря 2025

Автономные сервисные машины готовы создать в умных городах профессии будущего

В 2025 г. в российских городах не хватает полицейских, дворников, строителей и курьеров. Как правило, в этих профессиях много повторяющихся и однотипных задач. Возможно, преодолеть дефицит помогут роботы, которые становятся все распространеннее в городах благодаря цифровизации. "Ведомости. Город" разбирался, какие роботы уже используются в умных городах и способны ли они создать новые профессии.

Без роботов как без рабочих рук

По данным сервиса по поиску подработки "Наймикс", дефицит курьеров в России оценивается в 250 000 человек. Нехватка персонала наблюдается и в жилищно-коммунальном хозяйстве. Дефицит линейных и квалифицированных специалистов отрасли составляет 20%, по некоторым позициям - до 50%, свидетельствуют данные компании.
По итогам 2024 г. дворники возглавили топ-20 самых дефицитных вакансий, подготовленный HH.ru. Существенный дефицит кадров наблюдается и в МВД России: здесь открыто более 172 000 вакансий. Количество свободных должностей выросло вдвое, рассказывал в эфире РБК глава Общественного совета при МВД адвокат Анатолий Кучерена. Не хватает участковых уполномоченных полиции, в отдельных регионах дефицит оценивается в 66%.
Отрасль строительства также сталкивается с дефицитом. У крупных девелоперов нехватка кадров доходит до 20-30%, рассказывали представители застройщика "Самолет".
Некоторые функции в умных городах на себя готовы взять роботы. "Каждый новый робот на улице - курьер, уборщик или строитель - не просто выполняет задачу, помогая устранить дефицит кадров. Он оцифровывает пространство, выявляет проблемы инфраструктуры и заставляет ее совершенствоваться", - считает директор по коммуникациям 168robotics Ярослав Сапрыкин. По его словам, город с помощью роботов становится умнее, а сервисы - доступнее и качественнее для каждого жителя.
Цифровизация городов станет сильным драйвером появления новых профессий, связанных с управлением роботами, их диагностикой и ремонтом, считает бизнес-консультант по роботизации Алиса Конюховская.
Широкомасштабное внедрение автономных машин позволит сделать малопривлекательные отрасли более интересными для молодого поколения. "Мало кто захочет работать дворником с лопатой. Появятся новые профессии, например, "оператор парка роботов-уборщиков". Такая вакансия звучит более благозвучно", - добавил Ярослав Сапрыкин.
Также благодаря цифровизации роботы станут более доступными. "При росте количества выпускаемых роботов, возможно, потребуется ввести специальную тарификацию - "робо-нормо-час". Это позволит городским службам вместо покупки арендовать автономные машины. Тем самым снизится себестоимость работ и сократится срок окупаемости инвестиций", - прогнозирует Ольга Мудрова.

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Главным барьером для массового внедрения автономных машин в городе остается недостаточное количество зарядных станций, считает Алиса Конюховская. По ее словам, зачастую роботы до половины заряда аккумулятора тратят на обратный путь до ближайшей базы.

Робота заказывали?

Пожалуй, массово роботы начали появляться на улицах российских городов с 2019 г. Именно с этого времени роверы (автономные наземные четырехколесные роботы) компании "Яндекс" начали развозить заказы по Москве. Теперь география маршрутов рободоставки охватывает Иннополис, Санкт-Петербург и его пригород Мурино. С декабря 2025 г. этот список пополнился Казанью. С начала 2025 г. роверы выполнили более 250 000 доставок.

Роверы работают в дождь и снегопад, а в туман специальные лазерные радары помогают им видеть обстановку на расстоянии 100 м. Грузоподъемность каждого - 25 кг.

Роботизированная доставка добралась до метрополитена. Так, в китайском Шэньчжэне, городе с населением 19 млн человек, курсируют робофургоны Neolix вместительностью 500 кг. В метро машины спускаются в вечернее время.

Автономный транспорт умеет обходить препятствия и не допускает наезда на пассажиров. Робофургон подвозит груз к курьерам, те забирают нужные заказы, садятся в вагон и едут до ближайших от клиентов станций.

Применяются роботы-курьеры и внутри зданий. Например, в Мемориальном госпитале Toyota в Японии медперсоналу из-за рутинных повторяющихся операций, в том числе транспортировки препаратов и оборудования, не хватало времени для общения с пациентами. Проблему решили инженеры: специалисты оснастили больницу робокурьерами и интеллектуальными камерами, которые взаимодействуют с лифтами, дверями и другой инфраструктурой. Это позволяет машинам беспрепятственно курсировать между этажами и помещениями. Автономные курьеры выполняют около 170 доставок в день.

Недавно робота для схожих целей внедрили в подмосковном Детском научно-клиническом центре (ДНКЦ) имени Рошаля. Он транспортирует биоматериалы и пробирки между рабочими станциями. В день совершается до 65 рейсов. Василий, так назвали машину, помогает соблюдать точность и скорость лабораторных процессов.

Роботы припарковались для уборки

Курсируют роботы и по общественным местам, где отвечают за уборку территории. Так, в парках Москвы автономные машины "Пиксель" от разработчика беспилотных электрических роботов-уборщиков "Автономика" подметают щеткой тротуары в парках, наносят противогололедные реагенты, моют дорожки водой под давлением и т. д. Такие роботы могут работать всесезонно.

Роботы БРО от "168 роботикс" также задействованы в столичных парках. Машины обнаруживают и убирают мусор по ходу движения, при необходимости корректируют маршрут. Компания работает над разработкой зимнего варианта БРО.

"Уже отработаны возможности смета снега в условиях продолжительных снегопадов, свойственных средней полосе. Так, планируется разработка нового навесного оборудования для уборки снега для модульной платформы БРО 3. Рассчитываем, что машины уже зимой 2026-2027 гг. смогут убирать улицы от снега и распределять противогололедные реагенты", - рассказал Ярослав Сапрыкин.

Также компания проводит опытную эксплуатацию роботов четырех разных модификаций. Часть из них работает в городах на юге России, здесь круглогодично можно улучшать вакуумную уборку. Дополнительно в производстве находится первая опытно-промышленная партия модернизированных роботов БРО 3.1, которые с весны начнут работать в Москве. Они будут всесезонными, а функционал будет расширен за счет различного навесного оборудования, рассказал Ярослав Сапрыкин.

Привлечение роботов позволяет снизить затраты на комплексную уборку территорий на 20-80%, указал Сапрыкин, сославшись на мировой опыт и расчеты компании.

О перспективах использования роботов для уборки общественных пространств говорит также исполнительный директор Национальной ассоциации участников рынка робототехники Ольга Мудрова. Например, на территории Северного административного округа Москвы расположено семь крупных парков.

"Для их обслуживания в перспективе не понадобятся сотни человек: достаточно будет квалифицированной бригады операторов роботов и мастеров по их эксплуатации", - объяснила Ольга Мудрова.

Не потребуется, как сейчас, постоянно прикреплять к дворникам бригадира, перепроверять работу за сотрудниками и вести фотовидеофиксацию для отчетности. "Если робот исправен и выехал на местность, то точно сделает все хорошо", - добавила эксперт.

Робокопы патрулируют города

В общественных местах роботы следят также за правопорядком. Например, в Астане (Казахстан) четвероногие роботы задействованы для патрулирования территории. Камеры устройств могут идентифицировать лица, обнаруживать угрозы и оперативно на них реагировать. В МВД Казахстана рассматривают перспективы постоянного использования таких роботов в крупных городах.

Патрулируют улицы и гуманоидные роботы. Так, в китайском Шэньчжэне на смену вместе с полицейскими заступают автономные машины. В столице Китая, Пекине, в парке Бода создается комплексная сеть мониторинга. Здесь службу несут робопсы. Машины оборудованы панорамными видеокамерами, которые подключены к умной системе городского видеонаблюдения.

Четвероногие роботы в реальном времени способны обнаруживать нестандартное поведение граждан и чрезвычайные происшествия - задымления, пожары и т. д. Также в Пекине улицы патрулируют беспилотные автомобили.

В России роботы-полицейские пока не задействованы в схожих сценариях. Однако попытки вывести на рынок "робокопа" были. В 2021 г. российский производитель автономных сервисных роботов "Промобот" представил сотрудникам МВД России робота Promobot V.4. Сообщалось, что машина сможет работать в зданиях. Разработчики анонсировали, что робот способен распознавать лица, оружие, речь, сканировать отпечатки пальцев по запросу, выводить данные о человеке из базы МВД.

Девелоперы пробуют пристраивать роботов

Не задействованы роботы и в строительстве многоэтажных зданий. Алиса Конюховская отметила, что роботы для штукатурно-малярных работ и укладки плитки только начинают разрабатываться. По словам эксперта, эта отрасль с большими перспективами для роботизации, так как основы механизации здесь заложены еще с прошлого века.

Реальные примеры - скорее исключение из правил. Так, осенью 2025 г. сообщалось, что автономные машины на возводимом в Москве жилом комплексе помогли установить более 430 стеклопакетов нестандартной формы и весом в 250 кг. Роботы выполнили задачу без ошибок и повреждений конструкций.

На стройплощадке нового корпуса НИИ скорой помощи им. Н. В. Склифосовского в Москве задействован роботизированный беспилотный кран. Руководит работой машины оператор из центра управления поблизости. Обзор территории обеспечивается при помощи установленных на кране видеокамер с панорамным охватом. Решение, говорят строители, позволит ускорить выполнение операций на высоте на 10%, а простои персонала сократить до 40%.

Также разных роботов тестируют в Санкт-Петербурге. Так, эксперты девелопера Setl Group проверяли работу робособак в мониторинге качества и скорости строительства, в частности, при оценке монолитных работ, стяжки, кладки и предчистовой отделки. На одном этаже применение автономных машин сократило процесс в среднем на 10 минут, рассказывали представители компании.

Однако возникают сложности с адаптацией роботов. "Каждый строительный проект уникален. Например, робот-уборщик легко может построить карту плоской территории или же может передвигаться по заранее заданному алгоритму. А стройка - это различная этажность, высота потолков, разное расположение дверных и оконных проемов", - указал директор по строительству Setl Group Виталий Ершов. (Ведомости 12.12.25)

К СОДЕРЖАНИЮ

БПЛА

В Минпромторге России продолжается развитие государственного портала поддержки отрасли БАС.

Государственный портал поддержки отрасли беспилотных авиационных систем (БАС), созданный Министерством промышленности и торговли Российской Федерации, более года успешно работает в интересах участников рынка. За это время он стал ключевой площадкой для взаимодействия производителей, разработчиков, научного сообщества и органов государственной власти, играя важную роль в развитии одного из наиболее перспективных технологических направлений.

За первый год работы портал достиг существенных результатов. Сформирована обширная база данных российских беспилотных систем и их комплектующих, которая способствует продвижению отечественной продукции как на внутреннем рынке, так и за рубежом. Создан реестр эффективных сценариев применения БАС в экономике - от мониторинга трубопроводов и сельскохозяйственных угодий до охраны лесов. Важным итогом стало внедрение сервисов для оценки эффективности беспилотных технологий и расчёта экономического эффекта по сравнению с традиционными решениями.

Ключевая задача на данном этапе - дальнейшее развитие функциональности портала и усиление его аналитических возможностей. Уже внедрены современные инструменты мониторинга рынка и интеграция с государственными реестрами, что создаёт дополнительный стимул для разработки и внедрения инновационных решений.

Представители ведомства подчёркивают, что портал развивается как полноценная экосистема, создающая условия для роста инвестиций в высокотехнологичные проекты и укрепления позиций России на международной арене. Сегодня он может позволить ускорить разработку отечественных беспилотных систем, повысить спрос на российское оборудование и сформировать комфортную среду для притока талантливых специалистов и молодёжи в сектор высоких технологий.

Созданием портала Министерство продолжает выполнение масштабной программы модернизации экономики России, ставящей целью укрепление лидирующих позиций нашей страны в современном технологическом пространстве. (INFOLine, ИА (по материалам Министерства промышленности и торговли) 15.12.25)

К СОДЕРЖАНИЮ

Замминистра промышленности и торговли Российской Федерации Василий Шпак обозначил приоритеты развития рынка БПЛА: фокус на создание сервисных компаний-эксплуатантов.

В рамках 12-го отраслевого Форума по развитию беспилотной авиации "АЭРОНЕКСТ 2025" заместитель Министра промышленности и торговли Российской Федерации Василий Шпак подвел промежуточные итоги развития рынка беспилотных авиационных систем (БАС) и обозначил новые стратегические задачи.

Он отметил, что этап начального формирования рынка, связанный с государственным заказом и отработкой процедур, завершен. В стране сформировалась конкурентоспособная отрасль производства и разработки БПЛА.

"Теперь наша общая задача — обеспечить, чтобы созданная техника массово летала и приносила экономический эффект", — заявил Василий Шпак.

Ключевым барьером для масштабирования рынка он назвал острый дефицит профессиональных сервисных компаний — эксплуатантов.

"Заказчику — будь то сельхозпроизводитель или ведомство — по факту не нужны сами беспилотники. Ему нужен понятный, безопасный и гарантированный результат: мониторинг, доставка, контроль. Риски по содержанию техники, обучению персонала, ответственности должен на себя брать профессиональный игрок — сервисная авиакомпания. Именно таких компаний, особенно в логистике, сегодня на рынке критически не хватает", — пояснил он.

По словам Василия Шпака, новая фаза развития рынка требует смены парадигмы государственной поддержки. Если раньше фокус был на производителях, то теперь необходимо создать условия для появления и роста национальных лидеров в сфере оказания услуг с применением БПЛА. "Государство должно точечно работать с теми, кто готов рискнуть и инвестировать в этот бизнес, помогая им отработать модели и начать работу", — подчеркнул он.

Важнейшую роль в этом процессе должны сыграть регионы. Именно они, как заказчики услуг и регуляторы воздушного пространства на своей территории, должны быть напрямую заинтересованы в открытии "неба" для БПЛА, видя в этом инструмент для решения социально-экономических задач и пополнения бюджетов.

"Мы двигаемся в двух направлениях: поддерживаем как создание сервисных подразделений крупными производителями, так и появление независимых эксплуатантов. Наш следующий шаг — плотная работа с профессиональным сообществом, регионами и потенциальными инвесторами для формирования полноценного сервисного слоя экономики БПЛА", — резюмировал Василий Шпак. (INFOLine, ИА (по материалам Министерства промышленности и торговли) 12.12.25)

К СОДЕРЖАНИЮ

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

Трасса М-12 приоткрывается для беспилотных грузоперевозок.

Ритейлер "Магнит" и технологическая компания Navio провели тестовый рейс на автономном грузовике по трассе М-12 "Восток". В 2026 г. компании планируют сделать рейсы регулярными. "Камаз" в 2026 г. также запустит беспилотный транспорт по трассе М-12. Всего по российским трассам ездят 90 беспилотных грузовиков.

В рамках тестового проезда "Магнита" (ПАО "Магнит") и Navio (ООО "Автотех") грузовик проследовал по маршруту от распределительного центра ритейлера в Санкт-Петербурге до Зеленодольска, а затем вернулся в Санкт-Петербург - всего он преодолел около трех тыс. километров. В 2026 г. "Магнит" планирует запустить по М-12 регулярные рейсы.

Грузовиком управлял ИИ-водитель - он проехал по разрешенным участкам на трассе М-11 "Нева", центральной кольцевой автомобильной дороге А-113 (ЦКАД) и трассе М-12 "Восток". Остальной путь он проделал под управлением живого водителя-испытателя, который контролировал ИИ-систему.

По итогу теста участники сделали вывод, что беспилотный транспорт без водителя в кабине может почти в 2,5 раза сократить доставку грузов на маршруте Санкт-Петербург - Казань по трассам М-11 "Нева", ЦКАД и М-12 "Восток". Стандартный такой рейс с водителем длится около 58 часов, а без него - меньше суток.

"Автономные грузоперевозки позволяют повысить эффективность логистики, в том числе за счет увеличения суточного пробега и оборачиваемости автопарка, а при масштабном внедрении эта технология будет способствовать снижению конечной стоимости продуктов, ведь логистические затраты - значимая часть в формировании цены на полке", - заявил заместитель гендиректора, директор по цепочкам поставок и логистике "Магнита" Федор Павловский. По его словам, в 2026 г. "Магнит" планирует запустить регулярные рейсы по М-12.

"Ранее мы осуществляли проезды по части М-12. В данном случае это первый коммерческий рейс со стороны компании "Магнит", которые совместно с нами запустил первый тестовый рейс на автономном грузовике по новому направлению - трассе М-12 "Восток", - объяснил представитель пресс-службы Navio.

По словам представителя пресс-службы Navio, автономный флот Navio составляет более 220 автомобилей: 180 легковых и 40 грузовых тягачей.

Руководитель проекта "Беспилотные логистические коридоры" в NatCar (АО "Национальный перевозчик") Андрей Пахомов рассказал ComNews, что на российских трассах эксплуатируется 18 высокоавтоматизированных транспортных средств (ВАТС) на базе КАМАЗ 54901. Они работают на магистрали М-11 "Нева" и ЦКАД. На 2026 г. запланирован запуск движения по М-12 "Восток".

Всего по трассам, по данным Минтранса, ездят 90 беспилотных грузовиков. Их пробег - 9,5 млн километров. Ранее ассоциации "Цифровой транспорт и логистика" (АЦТЛ) заявляла о планах транспортной отрасли в 2025 г. увеличить количество действующих автономных грузовиков на трассах до 100, подготовить закон о высокоавтоматизированных транспортных средствах (На данный момент разрабатывается закон о ВАТС, который могут внести в Госдуму в I квартале 2026 г. - прим. ComNews) и разработать концепцию масштабирования беспилотных технологий на дорогах общего пользования.

Как объяснил ComNews представитель пресс-службы Navio, в данный момент в автомобиле обязательно находится водитель испытатель, который контролирует работу системы и всегда готов перехватить управление.

Руководитель проекта "Беспилотные логистические коридоры" в NatCar Андрей Пахомов также объяснил ComNews, что по требованию действующих нормативов кабине обязательно присутствует водитель-испытатель. Но Минтранс допустил высадку человека из кабины при переходе на следующий уровень автономности. "Мы работаем над законом о ВАТС. Его принятие даст нам возможность запустить автомобили без водителя уже в 2027 г.", - ранее сказал Министр транспорта Андрей Никитин.

"В целях предотвращения аварийных ситуации на дороге, ПАО "Камаз" разработало программу "Виртуальный полигон". В программе моделируются и отрабатываются аварийные ситуации с участием ВАТС, происходит настройка алгоритмов поведения ВАТС для автономного движения", - рассказал Андрей Пахомов об обеспечении безопасности.

Экспериментальный правовой режим, который позволяет беспилотным грузовикам ездить по трассам, работает в рамках проекта Минтранса "Беспилотные логистические коридоры". Недавно правительство продлило срок действия ЭПР до 12 ноября 2028 г. После постановления правительства расширился список регионов, в которых действует ЭПР - теперь их 13: Москва, Санкт-Петербург, Московская, Ленинградская, Новгородская, Владимирская, Нижегородская, Свердловская, Тверская области, Пермский край, а также Республика Башкортостан, Республика Татарстан и Чувашская Республика.

В проекте Минтранса участвуют ООО "ПЭК", АО "Национальный перевозчик", ООО "Агро-Авто" (X5), ПАО "Магнит", ООО "Автотех", ООО "Газпромнефть-Снабжение". На трассе используются беспилотные грузовики двух производителей - "Камаз" и Navio ("Автотех").

Для справки: Название компании: *Магнит, ПАО (Торговая сеть Магнит)* Адрес: *350072, Россия, Краснодарский край, Краснодар, ул. Солнечная, 15/5* Телефоны: *+78612109810; +7(800)2009002* Факсы: *+7(861)2109810* E-Mail:

info@magnit.ru; press@magnit.ru Web: https://magnit-info.ru/; https://magnit.ru/; https://cosmetic.magnit.ru/
Руководитель: *Случевский Евгений Сергеевич, генеральный директор; Райан Чарльз Эммитт, председатель Совета директоров; Корня Алексей Валерьевич, исполнительный директор* (ComNews.ru 12.12.25)

К СОДЕРЖАНИЮ

В Оренбуржье намерены задействовать БАС в сельском хозяйстве и строительстве.

Беспилотники в регионе уже применяют предприятия топливно-энергетического комплекса для мониторинга газо- и нефтепроводов

Сельское хозяйство, строительство и контрольно-надзорная деятельность дополнят в перспективе сферы использования беспилотных авиационных систем (БАС) в Оренбургской области после введения в регионе экспериментального правового режим в сфере цифровых инноваций по эксплуатации БАС. Об этом сообщили ТАСС в департаменте информационной политики Оренбургской области.

"В перспективе планируется расширить сценарии применения и использовать БАС в таких сферах, как сельское хозяйство, строительство и контрольно-надзорная деятельность", - сказано в ответе департамента на запрос агентства.

По данным региональных властей, в настоящее время ведущие предприятия топливно-энергетического комплекса уже применяют в Оренбуржье беспилотники с целью мониторинга газо- и нефтепроводов. БАС успешно заменяют традиционную пилотируемую технику и показывают положительный экономический эффект. Кроме того, министерство природных ресурсов, экологии и имущественных отношений Оренбургской области с 2026 года планирует использовать БАС в целях мониторинга лесопожарной опасности.

"Сегодня БАС демонстрируют ряд ключевых преимуществ перед традиционными технологиями в различных сферах применения. Их эффективность проявляется в скорости, точности, экономической выгоде, безопасности и возможности работы в труднодоступных условиях", - уточнили в департаменте.

Экспериментальный правовой режим в сфере цифровых инноваций по эксплуатации беспилотных авиационных систем в соответствии с постановлением правительства РФ начал действовать на территории Оренбургской области в октябре 2025 года. Этот специальный механизм позволяет тестировать и внедрять новые технологии в условиях ограниченного регулирования. Как разъяснили в департаменте, принцип действия режима основан на упрощении процедур допуска к полетам БПЛА, снижении административных барьеров, тестировании технологий в реальных условиях, применении систем управления полетов опытного района, внедрении цифровых платформ для автоматизации процессов и контроля полетов.

Реализация постановления, по данным региональных властей, будет осуществляться поэтапно, с акцентом на интеграцию беспилотных воздушных судов в общее воздушное пространство и их применение в различных отраслях. Эксперимент допускает применение легких (от 5 кг), средних и тяжелых БПЛА (свыше 500 кг) самолетного, вертолетного и мультироторного типа. При этом нет ограничений в зависимости от страны-производителя аппарата. (ТАСС 12.12.25)

К СОДЕРЖАНИЮ

Бесполетные летательные аппараты. "КоммерсантЪ". 15 декабря 2025

Госзакупки гражданских дронов упали более чем в четыре раза за год

Госзакупки гражданских дронов за неполный 2025 год уменьшились более чем в четыре раза, до 2,6 млрд руб. Речь идет в том числе о контрактах, финансируемых по сократившемуся в 2025 году в шесть раз федеральному гражданскому заказу (ГГЗ). По итогам года отраслевая выручка, по прогнозам профильной ассоциации, может упасть на треть. Среди причин эксперты называют насыщение техникой в прошлые два года, дефицит бюджетов субъектов, а главным образом — запрет на использование дронов в регионах и ограничения мобильной связи.

Госзакупки гражданских беспилотников по 44-ФЗ с января по ноябрь 2025 года сократились в 4,3 раза по сравнению с аналогичным периодом 2024 года, подсчитали для "Ъ" в аналитической системе по работе с тендерами "Тендерплан". Если с января по ноябрь 2024 года было совершено 1459 госзакупок на 11,3 млрд руб., то за тот же период 2025 года — 982 госзакупки на 2,6 млрд руб. Лидером по объемам завершенных контрактов этого года в финансовом выражении стала Москва (401 млн руб.), также в топ-5 вошли Санкт-Петербург (211 млн руб.), Подмосковье (189 млн руб.)., Ямало-Ненецкий автономный округ (111 млн руб.) и Приморский край (168 млн руб.).

В прошлом году пятерку крупнейших заказчиков возглавляли Москва (919 млн руб.), Санкт-Петербург (464 млн руб.), Воронежская область (417 млн руб.), Башкирия (413 млн руб.) и Ульяновская область (401 млн руб.).

Снижение во многом связано с сильным сокращением финансирования государственного гражданского заказа на беспилотники.

Если в 2024 году из федерального бюджета на сосубсидирование закупок выделяли более 6 млрд руб., в 2025-м объем средств сократился до 1 млрд руб. (см. "Ъ" от 9 июня). По итогам 2024 года, благодаря масштабному финансированию, как уточнили в "Тендерплан", объем госзакупок по 44-ФЗ вырос в годовом выражении втрое по сравнению с 2023 годом, когда он составил 3,9 млрд руб.

В Минпромторге "Ъ" не ответили. Опрошенные "Ъ" производители беспилотников комментировать ситуацию не стали, но в одной из компаний отметили также сокращение среднего срока контрактов: "Долгосрочные контракты стали большой редкостью". На другом предприятии называют основным фактором общее сокращение региональных бюджетов.

На фоне снижения госзаказа выручка за услуги по итогам 2025 года может быть ниже прошлогодней примерно на 30%, поделились с "Ъ" в профильной ассоциации "Аэронекст".

Исключительно гражданский сегмент в денежном выражении составил в 2024 году 21,7 млрд руб. за продукцию и услуги суммарно, что на 10% больше, чем в 2023 году. В 2025 году, по предварительным оценкам, показатель может остановиться на отметке 15 млрд руб. За первое полугодие рынок услуг в среднем снизился на 20% к аналогичному периоду 2024 года и составил около 3,5 млрд руб.

При этом динамика неравномерна по отдельным видам работ и по регионам, отмечается в материалах "Аэронекст". Так, наибольшее снижение наблюдается по всем видам аэрофотосъемки на объектах линейного и площадного мониторинга. Вместе с тем относительно прошлого года вырос спрос на геологоразведку, для которой выполняются измерения на малой высоте. Статистика страховых компаний показывает существенное увеличение числа страховых событий в 2025 году, что, с одной стороны, может говорить о росте интенсивной эксплуатации беспилотных воздушных судов, с другой — о том, что работы начинают выполнять малоопытные компании и специалисты.

Среди ключевых причин снижения рынка в ассоциации называют сохраняющиеся запреты на использование беспилотниками воздушного пространства в регионах. И даже там, где разработаны регламенты получения разрешений, процедура в большинстве случаев остается слишком долгой и сложной для участников отрасли. "Как ни странно, регионы не стремятся снимать запреты даже там, где беспилотная угроза фактически отсутствует, и не ускоряют процессы согласований",— отмечает глава "Аэронекст" Глеб Бабинцев.

Вторым объяснением снижения объемов рынка может быть то, что региональные власти, "затоваренные" полученными по ГГЗ беспилотниками, начинают выполнять работы сами, или привлекая непрофильных или демпингующих в ущерб качеству и безопасности подрядчиков. Это может объяснить и статистику страховщиков. В результате, продолжает господин Бабинцев, коммерческий рынок добросовестных игроков теряет заказы, а малоизвестные компании банкротятся или выполняют не весь объем выигранных на конкурсах работ, что снижает доверие заказчиков к новым технологиям.

Также существенное влияние на отраслевые показатели оказывают ограничения мобильной связи в регионах, которые не только осложняют работу операторов беспилотников, но и замедляют спрос заказчиков на услуги, говорит основатель сервиса RunAvia Андрей Патраков. Кроме того, даже после отмены сигнала "Ковер" предприятия в регионах часто бесконтрольно применяют средства радиоэлектронной борьбы, что делает невозможным навигационное управление гражданскими беспилотниками, рассказывает он.

Еще одной нерешенной проблемой Андрей Патраков называет засилье рынка теневыми поставками китайской техники и "всего, что завозят обходными путями и пересобирают здесь под видом российских дронов". По его словам, этот фактор сокращает выручку реальных производителей, а также приводит к демпингу в госзаказе.

Сокращение федерального финансирования показало, что самостоятельный гражданский рынок беспилотной техники в РФ пока так и не сформировался, заключает господин Патраков. Административные барьеры, включая запреты на полеты и сложности сертификации, остаются нерешенными с 2022 года, и "поводов для оптимизма на 2026 год пока не проглядывается". Однако отсутствие бюджетных вливаний может послужить стимулом для развития рынка, допускает эксперт. Первым шагом для преодоления падения рынка эксперт считает распространение экспериментальных правовых режимов на большее количество субъектов: "При условии не декларативного объявления режимов, как происходит в ряде регионов, а действительного начала полетов в рамках особого правого поля". (КоммерсантЪ 15.12.25)

К СОДЕРЖАНИЮ

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

MedTech

Сбер развивает ИИ-платформу для фармразработки.

Сбер внедряет искусственный интеллект в фармразработку. Новые технологии помогут исключить тупиковые этапы и ускорить создание терапии.
Сбер совместно с биофармацевтическим сектором работает над разработкой платформы для интеграции искусственного интеллекта в процессы разработки лекарств. Об этом президент, председатель правления Сбербанка Герман Греф рассказал во время онлайн-конференции "Сделано в Сбере".
"Искусственный интеллект помогает с молекулярным моделированием, прогнозированием и исключением наиболее дорогих тупиковых этапов. К примеру, совместное применение искусственного интеллекта, генетических технологий и биоинформатики сокращает сроки разработки лекарств для терапии рака до двух лет", — рассказал Герман Греф.
В сентябре первый заместитель председателя правления Сбербанка Александр Ведяхин рассказал, что дочерняя компания Сбербанка "Сбер Бизнес Софт" разработала решение на базе искусственного интеллекта для онкологических центров. ИИ-модель Сбербанка может планировать на год закупку лекарств и делает это на 42% лучше человека. Разработка поможет избежать приостановки терапии и предотвратить неэффективный расход бюджетных средств.

Для справки: Название компании: *Сбербанк, ПАО (ИНН 7707083893)* Адрес: *117997, Россия, Москва, ул. Вавилова, 19* Телефоны: *+74955058885; +78005008743; +74959575731; +74957473731* E-Mail: *scs@sberbank.ru; media@sberbank.ru* Web: *https://www.sberbank.com/ru; https://www.sberbank.ru* Руководитель: *Греф Герман Оскарович, президент-председатель Правления* (Фармацевтический вестник 10.12.25)

К СОДЕРЖАНИЮ

Сеченовский Университет зарегистрировал уникальную ИИ-систему для массового скрининга сердечной недостаточности.

Сеченовский Университет зарегистрировал программное обеспечение для удаленного скрининга и мониторирования параметров гемодинамики по данным одноканальной электрокардиограммы и пульсовой волны. Разработка предназначена для раннего выявления сердечной недостаточности и других скрытых нарушений работы сердца. Теперь она может применяться в клинической практике — в поликлиниках, телемедицинских центрах и при диспансерном наблюдении.
"Мы получили официальное разрешение на применение разработки по самому сложному, третьему классу медицинских изделий с искусственным интеллектом. Наша технология позволяет по данным одноканальной ЭКГ рассчитывать показатели, которые обычно получают при ультразвуковом исследовании сердца. Это открывает возможности для массового скрининга и удаленного мониторинга пациентов", — отметил директор Института персонализированной кардиологии Сеченовского Университета, профессор Филипп Копылов.

Для справки: Название компании: *Первый Московский государственный медицинский университет имени И.М. Сеченова , ФГАОУ ВО (Сеченовский Университет, ИНН 7704047505)* Адрес: *119991, Россия, Москва, ул. Трубецкая, 8, стр. 2* Телефоны: *+7(499)2480553; +7(495)6091400#2063; +7(495)6091400#2291* Факсы: *+7(499)2480181* E-Mail: *rektorat@sechenov.ru; expedition@mma.ru; pr@sechenov.ru* Web: *https://sechenov.ru* Руководитель: *Глыбочко Петр Витальевич, ректор* (IT Channel News 16.12.25)

К СОДЕРЖАНИЮ

Аналитики посчитали, как ИИ используется в разработке препаратов. "Фармацевтический вестник". 11 декабря 2025

ИИ используется для создания каждого третьего нового препарата, а занимающиеся этим европейские стартапы привлекли более 2 млрд долл. за 2025 год. Однако инвестиции распределяются неравномерно: начальные этапы разработки получают миллиарды долларов, а дорогостоящие клинические испытания — в разы меньше. Эксперты предупреждают: полностью заменить участие пациентов технологиями невозможно, а качество данных для обучения алгоритмов оставляет желать лучшего.

В 2025 году около 30% препаратов создаются с использованием искусственного интеллекта (ИИ), причем 31 из них уже проходит испытания на людях. Это выяснили венчурный инвестиционный фонд Speedinvest и онлайн-сервис бизнес-аналитики Dealroom, опубликовавшие совместный отчет.

Согласно ему, за год в странах Европы учреждено более 150 стартапов, разрабатывающих лекарства при помощи нейросетей. С января крупные корпорации заключили свыше 30 сделок с компаниями из инновационного сегмента. В их числе — покупка Exact Sciences фармконцерном Abbott за 21 млрд долл.

Инвестиции

Представители этого сектора на европейском рынке привлекли более 2 млрд долл. в течение минувших 11 месяцев — второй наибольший показатель за всю историю, следует из анализа. Рекорд — 3,1 млрд долл. в 2021 году.

Великобритания с огромным отрывом опережает остальные европейские государства по объему финансирования сферы ИИ-фармацевтики с результатом в 637 млн долл. Причем 600 млн долл. из этой суммы пришлись на одну компанию — Isomorphic Labs.

"При этом не известна ни одна молекула, которую они разработали", — уточнил для "ФВ" медицинский директор компании "Бионтек" Владимир Якусевич.

Далее идут Испания (116 млн долл., из которых 100 млн долл. получила CuspAI), Франция (103 млн долл.), Италия (97 млн долл.) и Швейцария (93 млн долл.).

Свыше 250 ИИ-фармстартапов родились в стенах университетов. За последние пять лет общий объем внешних капиталовложений в такие бизнесы достиг 5,8 млрд долл. Среди лидеров по числу предприятий этого типа — Кембриджский университет (25), Оксфордский университет (23) и Национальный центр научных исследований во Франции (14). В уходящем году их совокупная рыночная стоимость выросла до почти 25 млрд долл. — в 3,5 раза больше, чем в 2019-м.

Перекос в финансировании

В материале выявлено неравномерное распределение средств: начальный этап создания препаратов — определение патогенного белка и поиск лекарственной молекулы для воздействия на него — собирает больше всего инвестиций — 1,8 млрд долл. Хотя его доля в общей структуре затрат составляет всего 3%. Между тем проведение дорогостоящих клинических испытаний (КИ), на которые уходит до 62% бюджета, располагает скромными 298 млн долл.

"Это объясняется тем, что нельзя заменить КИ на людях использованием ИИ. Согласно официальной позиции Управления по санитарному надзору за качеством пищевых продуктов и медикаментов США (FDA), ИИ может носить вспомогательный характер — симуляция физиологических процессов, оптимизация дизайна КИ, но не их замена", — указал эксперт.

Как отмечается в материале, дисбаланс говорит о потребности в технологиях, которые уменьшат издержки, сроки и риски исследований с участием людей. Для внесения ясности:

- организация I фазы КИ стоит 4 млн долл., III фазы — 105 млн;
- каждый участник обходится в 119—143 тыс. долл.;
- на все три фазы нужно пять-семь лет;
- шанс, что препарат выйдет на рынок, — меньше 10%.

Примечательно, что в 2025 году предлагающие такие решения фирмы привлекли около 200 млн долл. инвестиций. Это в десять раз больше, чем в 2015-м.

Новые направления

За последнее десятилетие наблюдается развитие новых ниш в ИИ-фармацевтике:

автоматизация проверки соответствия стандартам и подготовки документов для подачи в регуляторные органы (+283%);

компьютерное моделирование живых клеток для проверки лекарств в доклинических исследованиях вместо экспериментов в чашках Петри (+187%);

системы для предотвращения утечки опасных патогенов из лабораторий и мониторинга биологических угроз (+155%).

Медленнее растут более классические области, такие как создание инструментов для поиска активных веществ для препаратов и технологий оптимизации производства, — 69 и 19% соответственно.

Вызовы для отрасли

Однако аналитики пишут о проблеме недостатка качественных данных для обучения ИИ. Доступные массивы о химических реакциях содержат в основном успешно завершившиеся эксперименты, тогда как примеры провалов в них отсутствуют.

Без этого алгоритмы не могут точно предсказывать, какие подходы не будут эффективными. К тому же качество информации в некоторых случаях оставляет желать лучшего.

Прогнозы

Грядущие десять лет кардинально преобразуют индустрию, а Европа выступит движущей силой этих изменений, считают в Speedinvest и Dealroom.co. Здравоохранение сильно отстает в цифровизации от других сфер экономики, что может стать источником мощного роста.

"Несомненно, роль ИИ в фармацевтической отрасли будет расти. Тем не менее полностью заменить участие пациентов невозможно и, в определенной степени, нецелесообразно: КИ включают в себя большое число вариабельных факторов, часть из которых не может быть смоделирована компьютером", — подчеркнул Владимир Якусевич. (Фармацевтический вестник 11.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

ЦОД

Вице-премьер РФ Дмитрий Григоренко поручил проработать создание цифровой платформы для развития ЦОД в РФ.

Заместитель председателя правительства РФ Дмитрий Григоренко поручил Минцифры РФ и Аналитическому центру при правительстве проработать предложения по созданию цифровой платформы для развития центров обработки данных (ЦОД), сообщил аппарат вице-премьера.

Предполагается, что платформа объединит набор сервисов для сопровождения полного жизненного цикла ЦОД от строительства и до ввода в эксплуатацию, что поможет упростить и ускорить процесс создания дата-центров, а также агрегирует информацию о доступных в стране вычислительных мощностях.

Как уточняется в сообщении, на платформе предлагается разместить сервисы для подбора земельного участка и заказа проверок по нему (например, на наличие обременений), услугу предоставления информации о доступных льготах, о наличии линий связи, доступности электрических мощностей и другой инфраструктуры. Кроме того, обсуждается создание в рамках платформы маркетплейса оборудования и услуг по проектированию и обслуживанию ЦОДов, которыми сможет воспользоваться бизнес.

"Создание единой цифровой платформы позволит перейти от строительства точечных разрозненных ЦОД к системному формированию их сети за счет объединения на одной площадке всех участников процесса от бизнеса и государства. Кроме того, платформа станет единой точкой сбора информации о существующих ЦОДах, арендных предложениях, потребностях в дополнительных мощностях и доступности инфраструктуры для их строительства", - говорится в сообщении.

В нем отмечается, что новый подход позволит ускорить процесс получения необходимых данных для создания ЦОД, сделать этот процесс прозрачным и сократить сроки строительства и ввода в эксплуатацию.

Минцифры и Аналитический центр при правительстве должны проработать и представить предложения к марту 2026 года. Эти наработки будут вынесены на обсуждение с бизнесом.

"Одна из наших приоритетных задач - это внедрение искусственного интеллекта. Но эта технология требует наличия инфраструктуры и достаточного количества центров обработки данных. Спрос на вычислительные мощности активно растет. Наша задача - упростить и ускорить создание ЦОДов. Для этого прорабатываем вопрос создания цифровой платформы", - приводятся в сообщении слова Григоренко.

По его словам, для бизнеса это даст удобные сервисы, упрощающие порядок строительства ЦОД, а для государства - возможность оценивать ситуацию на рынке дата-центров и определять реальные потребности в новых мощностях. (Интерфакс 12.12.25)

К СОДЕРЖАНИЮ

Запуск одного из крупнейших ЦОД в Сибири перенесли на лето 2026 года (Новосибирская область).

Объем инвестиций составил 1,8 млрд рублей

Компания "Альфа-финанс" планирует ввести в эксплуатацию центр обработки данных (ЦОД) "Сибирь" в Новосибирской области в марте 2026 года, а полный запуск запланирован на июль, сообщили ТАСС в пресс-службе Корпорации развития региона. Ранее объект называли одним из самых ожидаемых в 2025 году.

"Ввод проекта в эксплуатацию запланирован на март 2026 года, полный запуск - июль 2026 года. Общий объем инвестиций - 1,8 млрд рублей. Инвестор прогнозирует, что объем будет увеличен", - сообщили в пресс-службе.

Новосибирская область и "Альфа-финанс" договорились о строительстве дата-центра в Промышленно-логистическом парке региона в 2022 году на площадке Петербургского международного экономического форума. Генеральный директор фирмы Мария Бейлиш заявляла, что ЦОД будет одним из крупнейших в Сибири, он вместит 1,8 тыс. стойко-мест для IT-оборудования. В проекте предполагалось использовать оборудование российского производства и самые актуальные решения в части холодоснабжения и систем бесперебойного электропитания. Изначально запуск объекта планировался в 2024 году. Впоследствии в Минэкономразвития региона называли объект в числе самых ожидаемых к вводу в течение 2025 года.

Промышленно-логистический парк Новосибирской области является крупнейшим индустриальным парком Сибири. Его площадь составляет более 1 тыс. га.

Для справки: Название компании: *Альфа-Финанс, ООО (ГК Альфаком)* Адрес: *127299, Россия, Москва, ул. Большая Академическая, 5, эт/комната 4/424* Телефоны: *+7(495)5430323* E-Mail: *info@alfafin.info* Web: *http://alfkom.ru* Руководитель: *Бейлиш Мария Валентиновна, генеральный директор* (ТАСС 11.12.25)

INFOLine информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

К СОДЕРЖАНИЮ

В Иркутской области планируют создать центр обработки данных мощностью до 200 МВт.

В Иркутской области рассматривается проект строительства центра хранения и обработки данных мощностью до 200 МВт. Заместитель директора по научной работе Института экономики и организации промышленного производства СО РАН Антон Пыжев на пресс-конференции в ТАСС сообщил, что реализация центра позволит создать нового игрока на мировом рынке инфраструктуры данных и даст новый импульс развитию Сибири и Дальнего Востока.

По словам Пыжева, создание центра поможет России занять заметное место в отрасли благодаря имеющимся преимуществам региона. Проект был представлен в рамках исследования Института экономики роста имени П.А. Столыпина под названием "Потенциал создания нового игрока мирового рынка инфраструктуры данных".

Председатель совета по вопросам развития Сибири при председателе Совета Федерации, сенатор Александр Усс подчеркнул конкурентные преимущества региона для размещения дата-центров. Он отметил значительные энергоресурсы и климатические условия, которые облегчают охлаждение серверов, несмотря на будущие расходы на поддержание температурного режима оборудования. (Эксперт Сибирь и Дальний Восток 09.12.25)

К СОДЕРЖАНИЮ

Под вычислительные мощности готовят платформу. "КоммерсантЪ". 11 декабря 2025

Правительство консолидирует поддержку строительства ЦОДов от проекта до подключения

Правительство обсуждает создание под эгидой Минцифры и Аналитического центра (АЦ) при правительстве специального органа для поддержки строительства компаниями новых центров обработки данных (ЦОД). Вычислительные мощности — одна из ключевых потребностей РФ для развития цифровой экономики, но бюджетные инвестиции в эту сферу в рамках нацпроекта "Экономика данных и цифровая трансформация госуправления" должны быть уравновешены частными, иначе управляющая сторона не сможет подключиться к управляемой. Поэтому профильный вице-премьер Дмитрий Григоренко поручил министерству и АЦ найти "платформенное" решение для поддержки строительства частных ЦОДов — для упрощения их строительства и подключения к инфраструктуре. Также это сведет на одной площадке все данные о частных цифровых мощностях.

Как стало известно "Ъ", "цифровой" вице-премьер Дмитрий Григоренко подписал поручение Минцифры и Аналитическому центру при правительстве (отраслевой think tank Белого дома) к марту 2026 года проработать идею "цифровой" платформы по поддержке строительства частных ЦОДов для работы искусственного интеллекта (ИИ) как приоритетного для государства направления в отраслях экономики, госуправлении и соцсфере. Профильное совещание о задачах и предложениях по развитию ЦОДов прошло 3 декабря.

Цифровая платформа (экосистема сервисов) для сопровождения полного жизненного цикла создания и обслуживания ЦОДов должна "вобрать" в себя такие сервисы, как подбор земельного участка, предоставление информации о наличии льгот, доступности электрических мощностей и наличии линий связи, заказ проверок, изысканий, исследований, обременений по участкам для строительства. Кроме того, на ней планируется разместить маркетплейс оборудования и услуг по проектированию, строительству и обслуживанию ЦОДов. Предложения власти обсудят с бизнесом — как отмечают в аппарате вице-премьера, обратная связь от индустрии позволит понять, какие сервисы нужны в первую очередь, к каким можно будет вернуться в развитии, а на какие нет спроса.

Напомним, что в октябре 2025 года на форуме "Инфотех" в Тюмени Дмитрий Григоренко говорил, что правительство разрабатывает программу развития ЦОДов, их число планируется увеличить к 2030 году вдвое.

Сеть ЦОДов будет работать по единым стандартам по всей стране, отмечал Дмитрий Григоренко. В свою очередь, возможность для разработки и запуска комплексных мер поддержки для всей отрасли стала возможна после того, как на законодательном уровне (в федеральном законе № 244-ФЗ от 23 июля 2025 года) было закреплено само понятие ЦОДа.

Идея "платформенной" поддержки преследует одновременно несколько целей: новые ЦОДы критически необходимы для развития цифровой экономики, одного из прорывных и приоритетных направлений работы правительства. Также сведение на одной платформе всех инициатив по их строительству даст аппарату Белого дома точные знания о частных инициативах в этой области и позволит координировать их пространственное размещение в зависимости от наличия участков, возможностей подключения к энергомощностям и магистральному оптоволокну.

Сейчас, по разным оценкам, 70–90% ЦОДов сосредоточены в Москве и Санкт-Петербурге как центрах экономической активности, и дальнейшая их концентрация угрожает избыточной нагрузкой на сети и удорожанием проектов из-за стоимости земли и подключений, а также физически небезопасна при затягивании военной операции на Украине — в правительстве хотели бы распределить ЦОДы, в частности, по сибирским регионам.

Еще одно соображение в пользу поддержки развития частных ЦОДов — "подтягивание" уровня цифровизации экономики к уже достигнутому в правительстве: для "бесшовного" обмена данными, который предполагает нацпроект "Экономика данных и цифровая трансформация госуправления".

Для этого частная сторона должна обладать сопоставимыми мощностями, а госинвестиции в этой сфере уже заложены в бюджет нацпроекта, и теперь перед Белым домом стоит задача стимулирования сопоставимого прогресса в корпоративном секторе.
"Инфраструктурная поддержка", отметим, выступает в решении этой задачи "пряником", функции кнута же выполняет уже подписанное постановление правительства, которое требует наличия собственных ЦОДов у ИИ-разработчиков, желающих сохранить льготы по налогам и соцвзносам, связанные с включением программных продуктов в реестр российского ПО. Де-факто в области ИИ-проектов Белый дом готов предоставлять их только достаточно мощным компаниям, способным инвестировать в такое строительство. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

ЦОДы – ближе. "Iksmedia". 15 декабря 2025

Энергетики уделяют центрам обработки данных все больше внимания. Так, на прошедшей в середине октября Российской энергетической неделе был выдвинут ряд важных инициатив.
В частности, замглавы Минэнерго России Эдуард Шереметцев, заявив, что существующая программа строительства электросетевых объектов и объектов генерации потребности дата-центров учитывает, предложил, чтобы "те, кто курирует ЦОДы, имели собственный стратегический документ", на основе которого Минэнерго сможет эффективнее планировать технологическое присоединение и удовлетворять растущий спрос со стороны потребителей. Одним из ключевых решений, по его мнению, может стать разделение дата-центров по функциональным направлениям. Это поможет рациональнее задействовать избыточные мощности, например, в северных районах страны. "Функциональное разделение ЦОДов позволит использовать профицит энергии и положительно скажется как на ТЭК, так и на отрасли, развивающей искусственный интеллект", – заключил Э. Шереметцев.
По мнению директора по цифровой трансформации Системного оператора ЕЭС Станислава Терентьева, в настоящее время дата-центры появляются стихийно – на тех территориях, где им удалось найти возможности для технологического присоединения к сети. Такой подход усугубляет риск возникновения дефицита мощности и нерационального использования сетевой инфраструктуры. Важной задачей текущего этапа он назвал кропотливую работу по планированию размещения ЦОДов с тем, чтобы увязать наращивание потенциала нового вида энергоемких потребителей с имеющимися энергоресурсами и планами по развитию энергосистемы.
Функциональное разделение ЦОДов действительно наметилось – за счет выделения объектов, специализирующихся на задачах обучения ИИ-моделей. Для этих задач менее значимы наличие высокоскоростных каналов связи и близость к потребителям ИТ-сервисов, а потому, возможно, ЦОДы для ИИ будут тяготеть к местам с профицитом электроэнергии и точкам ее генерации. Но таких ЦОДов вряд ли будет много.
Большинство же дата-центров остаются и, по всей видимости, останутся универсальными объектами. Особенно это касается коммерческих ЦОДов: поскольку нельзя предвидеть, с какими задачами к ним придут заказчики лет через пять–десять, ориентация на конкретный функционал неприемлема. Зато важны наличие скоростных каналов связи и близость к клиентам, и поэтому выбор места размещения не может диктоваться одной только энергетикой.
В условиях же энергодефицита будет развиваться локальная генерация, в первую очередь газовая. Да, снова придется договариваться с монополистом, хотя и с другим. Но по крайней мере выбор у ЦОДов будет. (Iksmedia 15.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Информационная безопасность

Ученые НГТУ имени Р.Е. Алексеева изобрели способ выявления киберугроз цифровых подстанций.

Изобретение относится к области электротехники и направлено на повышение кибербезопасности цифровых подстанций — ключевых узлов современной интеллектуальной энергетики.
Авторами изобретения 2850734 "Способ выявления киберугроз цифровых подстанций" являются сотрудники НГТУ: Александр Леонидович Куликов и Антон Алексеевич Лоскутов.
Разработанный в НГТУ им. Р.Е. Алексеева способ решает задачу своевременного и достоверного выявления киберугроз на самой подстанции, опираясь на фундаментальные законы электротехники и анализ реальных режимов работы оборудования.
Данный способ учитывает отраслевую специфику электроэнергетики в отличие от известных способов кибербезопасности (межсетевые экраны, шифрование данных, аутентификация и пр.).
Суть способа заключается в том, что электрическая подстанция условно разделяется на силовые узлы, в каждом из которых соединяются несколько электрических присоединений. В реальном времени измеряются фазные токи всех присоединений и напряжения на узлах, полученные данные передаются по цифровой шине. Одновременно контролируется исправность трансформаторов тока, производится пофазное суммирование токов всех присоединений каждого силового узла с учетом направления токов. Если все трансформаторы тока исправны и сумма токов узла с учетом направления равна нулю, фиксируется штатный режим без признаков киберугроз. Если же при исправных трансформаторах сумма токов не равна нулю, превышает заданный порог, а скорость изменения токов выше характерной скорости переходных процессов при реальных повреждениях и переключениях, система интерпретирует это как возможную кибератаку. Алгоритм оценивает соблюдение фундаментальных электрофизических законов (Кирхгофа, Ома и пр.). При недостоверных данных он не будет соблюдаться, что расценивается, как угроза.
Одна из возможных кибератак - это подмена данных измерений (Spoofing), поступающих на устройства РЗА, что может спровоцировать ложные срабатывания релейной защиты (или несрабатывание при аварии) и отключить потребителей (или не отключить КЗ). К киберугрозам также относятся случаи, когда в цифровой шине присутствуют данные о токах при отсутствии напряжения на контролируемом силовом узле. В результате - необоснованные отключения электроэнергии со всеми вытекающими последствиями для потребителей. Или, наоборот, отсутствие отключения при возникновении аварии, что влечет за собой пожар, выход из строя дорогостоящего оборудования (генераторы, трансформаторы, кабели и пр.)
Важной особенностью изобретения является использование дополнительных диагностических признаков. Предусмотрен контроль состояния вторичных цепей трансформаторов тока с использованием токов обратной и нулевой последовательностей, а также анализ скорости изменения измеренных токов для отличения кибератак от реальных аварий и штатных переключений в прилегающей сети. Сигнал о киберугрозе формируется на выходе устройства, реализующего данный способ, и передается в автоматизированную систему управления технологическими процессами цифровой подстанции. При этом предусмотрена блокировка этого сигнала в случаях, когда в системе АСУ ТП зафиксированы ошибочные действия персонала, повреждения силовых узлов, насыщение трансформаторов тока, нарушения во вторичных цепях измерительных трансформаторов напряжения или штатное включение силовых узлов в работу — это позволяет снизить вероятность ложных срабатываний.
Важно, что связи блоков устройства, реализующего способ, выполняются независимо от цифровой шины подстанции. Такое конструктивное решение направлено на предотвращение искажений передаваемых сигналов в условиях кибератак, направленных непосредственно на специализированную локальную вычислительную сеть подстанции. В совокупности заложенные в изобретении алгоритмы контроля токов и напряжений, анализ небалансов и скоростей изменения электрических величин, а также использование дополнительной информации из АСУ ТП позволяют выявлять несоответствия данных реальным физическим процессам и тем самым обнаруживать попытки вмешательства в работу цифровой подстанции.
Данный патент закрепляет за НГТУ им. Р.Е. Алексеева приоритет в разработке решений для кибербезопасности цифровых энергетических объектов и подтверждает высокий потенциал научной школы университета в области интеллектуальных электроэнергетических систем и автоматизированных систем управления. Изобретение создает технологическую основу для повышения устойчивости цифровых подстанций к кибератакам и может быть востребовано предприятиями топливно-энергетического комплекса и разработчиками отечественных систем релейной защиты и автоматики.

Для справки: Название компании: *Нижегородский государственный технический университет им. Р.Е.Алексеева, ГОУ ВПО (НГТУ)* Адрес: *603950, Россия, Нижегородская область, Нижний Новгород, ул. Минина, 24* Телефоны: *+7(831)4362331; +7(831)4362325* Факсы: *+7(831)4369475* E-Mail: *nntu@nntu.ru* Web: *www.nntu.ru* Руководитель: *Дмитриев Сергей Михайлович, ректор* (GisProfi 15.12.25)

К СОДЕРЖАНИЮ

"Лаборатория Касперского" отметила ММК за профессионализм в области информационной безопасности.

Магнитогорский металлургический комбинат (ММК) был отмечен "Лабораторией Касперского" знаком "За ответственное отношение к вопросам информационной безопасности". Награда стала признанием комплексного подхода комбината к защите критически важных систем, данных и производственной инфраструктуры.

ММК уделяет особое внимание вопросам информационной безопасности своей IT-инфраструктуры, применяя многоуровневые системы защиты для обеспечения непрерывности производства и противодействия внутренним и внешним угрозам.

"Эта награда – подтверждение того, что внедряемые технологии и профессионализм наших специалистов работают на главный результат – защиту данных и систем компании", – отметил Вадим Феоктистов, главный специалист по информационным технологиям ММК.

Специалисты ММК по информационной безопасности используют современные инструменты для противодействия сложным угрозам и целевым атакам. Одно из таких решений не только обнаруживает аномальное поведение и атаки на уровне конечных узлов (рабочих станций, серверов), но и позволяет найти аномальную активность в сети компании, собирая и анализируя распределенные данные со всех устройств предприятия в режиме реального времени, а также моментально реагировать на выявленную подозрительную активность, предотвращая проведение атаки и информируя специалистов по информационной безопасности.

"Мы вручили почётную награду нашему уважаемому заказчику и партнёру – компании ПАО "ММК". Это признание профессионализма команды и качества нашей совместной работы. Мы не останавливаемся на достигнутом и продолжаем развитие в сфере информационной безопасности, чтобы наши компании были защищены сегодня и уверенно смотрели в будущее", – отметил Артур Хукаленко, региональный представитель "Лаборатории Касперского" по УрФО.

Для справки: Название компании: *Магнитогорский металлургический комбинат, ПАО (ММК, ИНН 7414003633)* Адрес: *455000, Россия, Челябинская область, Магнитогорск, ул. Кирова, 93* Телефоны: *+73519247709* Факсы: *+73519247309* E-Mail: *infommk@mmk.ru; Gavrishev.ks@mmk.ru* Web: *http://www.mmk.ru* Руководитель: *Шиляев Павел Владимирович, генеральный директор*

Для справки: Название компании: *Лаборатория Касперского, АО* Адрес: *125212, Россия, Москва, Ленинградское шоссе, 39, литера А, стр.3, БЦ «Олимпия Парк»* Телефоны: *+74957978700* Факсы: *+74957978709* E-Mail: *info@kaspersky.com* Web: *https://www.kaspersky.ru/* Руководитель: *Касперский Евгений Валентинович, генеральный директор* (По материалам компании 16.12.25)

К СОДЕРЖАНИЮ

Positive Technologies вышла на рынок антивирусов.

Компания начала продажи собственной технологии

Российская компания в сфере кибербезопасности Positive Technologies вышла на рынок антивирусов с собственной технологией, начав ее коммерческие продажи, сообщили ТАСС в пресс-службе компании. Этот сегмент рассматривает и компания "Солар" - дочерняя структура "Ростелекома".

В феврале 2025 года Positive Technologies купила долю в белорусской компании "Вирусблокада" и позднее создала с ним антивирусную лабораторию. Объем антивирусной базы от совмещения экспертиз вырос на 25%. Приводя оценку рынка защиты конечных устройств от ЦСР в 35 млрд рублей в 2024 году, в компании считают, что в 2026 году займут там не менее 5%.

Positive Technologies разрабатывает продукт для бизнеса - антивирус входит в решение MaxPatrol EPP, альфа-версию которого показали в октябре 2025 года. В 2026 году, как уточнили представители компании, они поделятся "планами относительно разработки на b2c рынок".

Осенью 2025 года другая компания на ИБ-рынке - Bi.Zone - сообщила о покупке российского разработчика антивирусного ПО Nano Security. В ответ на вопрос ТАСС о том, когда у Bi.Zone появится технология, в ее пресс-службе заявили, что "пока не называют планируемые даты". В ГК "Солар" же сообщили, что изучают все сегменты рынка, в том числе и антивирусов, "чтобы создать наиболее полный портфель решений для ИБ под ключ".

В России уже есть антивирусные продукты "Лаборатории Касперского", Dr.Web, PRO32, и от других компаний. По оценке "М.Видео-Эльдорадо", рынок антивирусного софта в 2024 году вырос на 28%, до 2,7 млрд рублей, и в количественном выражении тогда первое место заняла "Лаборатория Касперского".

Для справки: Название компании: *Позитив Текнолоджиз, АО (Positive Technologies)* Адрес: *107061, Россия, Москва, Преображенская пл., 8* Телефоны: *+74957440144* Факсы: *+7(495)7440187* E-Mail: *pt@ptsecurity.com* Web: *https://www.ptsecurity.com/ru-ru/* Руководитель: *Баранов Денис Сергеевич, генеральный директор* (ТАСС 10.12.25)

К СОДЕРЖАНИЮ

Юридическая карта киберрисков. "КоммерсантЪ". 10 декабря 2025

Почему "документы в папке" больше не спасают бизнес от кибератак

Более 400 тыс. киберпреступлений с начала года — "новая норма" для российского бизнеса. Ответом должен стать не только рост IT-бюджетов, но и смена парадигмы: юристы становятся ключевыми игроками в команде по кибербезопасности. Юрист "Томашевская и партнеры" Дарья Урманова — о том, как выстроить после инцидента защиту от регуляторных штрафов и исков.

В 2025 году киберугрозы окончательно закрепились для российского бизнеса в статусе операционного риска: по данным МВД, в январе—июле 2025 года было зарегистрировано 424,9 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. По оценкам провайдеров сервисов информационной безопасности, интенсивность атак на бизнес тоже растет: в ряде обзоров отмечается, что с начала 2025 года число кибератак превысило 105 тыс.

Реакция рынка предсказуема: компании увеличивают бюджеты на защиту. Совместное исследование "К2 Кибербезопасность" и Positive Technologies фиксирует, что 56% организаций нарастили расходы на киберзащиту в среднем на 20–40%. На фоне резонансных летних инцидентов с атаками на крупные бренды и инфраструктуру это становится неизбежным, однако усиление "железа" и SOC — только часть ответа. Даже единичная атака быстро превращается в юридическую проблему: претензии клиентов и партнеров, расследования регуляторов, споры о неисполнении договоров, вопросы коммерческой тайны и ответственности менеджмента. И управлять этим набором рисков можно только системно — через комплаенс и процессы, а не через разовые меры.

Во многих компаниях киберугрозы по инерции воспринимаются исключительно как задача соблюдения 152-ФЗ и предотвращения утечек персональных данных. Фокус верный, но узкий: при атаке страдают не только персональные данные (ПД), но и коммерчески значимая информация, отношения с контрагентами, а иногда — статус объектов КИИ и обязательства по безопасности.

На практике юридические риски после инцидента группируются в четыре блока: персональные данные и регуляторика (152-ФЗ, обязанности оператора, уведомления и доказательная база); коммерческая тайна и ноу-хау (введен ли режим, можно ли реально защищать актив и привлекать к ответственности); договорные последствия (конфиденциальность, SLA, ответственность за простой, обязанности по уведомлению); управление и контроль (распределение ролей, исполнение требований стандартов и политик, комплаенс-"след" для проверок и суда).

Оператор ПД должен не просто "иметь политику", а демонстрировать работающий цикл обработки данных: законные основания, минимизация, информирование субъектов, меры защиты, соблюдение требований локализации и корректные уведомления в Роскомнадзор. Внутренние регламенты и уведомления должны отражать фактический процесс: зачем и в каких целях собираются данные, чьи они, что происходит с ними при обработке, сколько они хранятся и как уничтожаются. Критические точки проверки — это соответствие их целому ряду требований: от оснований обработки (согласия, договоры, использование открытых источников в допустимых пределах) и локализации до передачи (договоры при передаче другому оператору, вопрос трансграничной передачи и уведомления), хранения и уничтожения.

Но, конечно, ключевой тренд 2025 года — это смещение акцента с "подготовки документов" на "реагирование". Для бизнеса это означает отстроенный процесс работы с запросами субъектов и инцидентами: сбор доказательств, анализ последствий, контроль сроков хранения и удаления, актуализация категорий данных, матриц ответственности и процедур уведомления.

Отдельный уровень сложности представляют собой компании, работающие на европейский рынок. Даже находясь вне ЕС, бизнес может подпасть под GDPR при обработке данных граждан ЕС в связи с предложением товаров и услуг или мониторингом поведения. В этом случае к списку обязанностей добавляются: оценка воздействия обработки на защиту данных; назначение инспектора по защите персональных данных в зависимости от основной деятельности; требование о незамедлительном уведомлении об утечке персональных данных субъекта при высокой степени риска для прав и свобод. Для трансграничных групп это означает необходимость строить систему информационной безопасности в соответствии с требованиями и российского законодательства, и GDPR.

При атаке компрометируются не только ПД, но и информация, которая имеет коммерческую ценность: клиентские базы, финансовые модели, технологические решения. Чтобы защищать этот массив, недостаточно ссылаться на "конфиденциальность по умолчанию". Нужны юридические меры введения режима коммерческой тайны. Для этого следует: определить перечень сведений, имеющих коммерческую ценность; установить порядок обращения и

контроля его соблюдения; вести учет лиц, допущенных к коммерческой тайне; закрепить условия использования информации в трудовых договорах и договорах с контрагентами; наносить на носители и в документы гриф "Коммерческая тайна".
Без выполнения этих шагов режим признается невведенным и компания теряет существенную часть правовых инструментов защиты. Аналогичная логика применима и к ноу-хау: режим коммерческой тайны не обязателен, но относится к "разумным мерам" конфиденциальности; альтернативой выступают локальные ограничения доступа и NDA-механизмы.
Когда у компании несколько контуров данных и разные категории защищаемой информации, "латание дыр" перестает работать. Практический ориентир — риск-ориентированный подход, закрепленный в ISO 27001 и его российском эквиваленте ГОСТ Р ИСО/МЭК 27001–2021: информационная безопасность строится как система менеджмента, интегрированная в процессы и управление.
Типовые меры включают: разработку и регулярный пересмотр политик информационной безопасности; организацию функции информационной безопасности и распределение ролей; работу с персоналом; менеджмент активов (включая их категорирование); управление доступом, криптографией и физической безопасностью; безопасность эксплуатации; контроль отношений с поставщиками; менеджмент инцидентов и обеспечение непрерывности; соответствие правовым и договорным требованиям.
Для минимизации юридических последствий атаки бизнесу имеет смысл действовать по предсказуемому сценарию: определить стратегию информационной безопасности и критичные угрозы с учетом бизнес-процессов; категоризировать информацию, установить приоритеты и уровни защиты; выявить угрозы и юридические риски, классифицировать их и закрепить меры реагирования; утвердить регламенты и матрицы ответственности (кто, что и когда делает при инциденте); внедрить организационные и технические меры, соразмерные угрозам; обучить сотрудников правилам информационной безопасности и реагированию; проводить регулярный мониторинг, аудит и пересмотр системы.
Кибербезопасность в 2025 году — это не только вопрос инфраструктуры, но и вопрос управления юридическими последствиями. Компании, которые заранее выстраивают процессы информационной безопасности, несут меньший ущерб — как финансовый, так и репутационный. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

"Хакеры в течение суток могут найти уязвимость и внедриться". "КоммерсантЪ". 10 декабря 2025

Как багхантеры повлияли на кибербезопасность банков

Один из ведущих российских экспертов по информационной безопасности, Алексей Лукацкий, рассказал о том, как повлияли на кибербезопасность банков внешние исследователи (белые хакеры, багхантеры). И почему российские банки находятся на несколько шагов впереди планеты всей с точки зрения кибербеза. Однако ни средства защиты, ни люди, ни технологии не спасут, если у руководства банка нет профессиональной компетенции и управленческой зрелости для принятия своевременных и достаточных решений.
Алексей Лукацкий — эксперт по информационной безопасности с более чем 30-летним стажем. Занимал ключевые позиции в крупных международных и российских компаниях. Сейчас является бизнес-консультантом по информационной безопасности ИТ-компании Positive Technologies. Алексей Лукацкий участвовал в разработке отраслевых нормативов, входил в рабочие группы Банка России по созданию требований к защите информации в Национальной платежной системе, а также принимал участие в формировании стандартов в рамках технических комитетов по кибербезопасности при Росстандарте. Автор нескольких книг и образовательных программ по ИБ и постоянный спикер ведущих отраслевых конференций.

"Необходимо стало эмулировать реальные хакерские атаки"

— Российские банки начали привлекать внешних специалистов, исследователей — белых хакеров (багхантеров) — к тестированию информбезопасности в 2023 году?

— Не совсем корректно так говорить. Регуляторные положения о необходимости привлекать внешних проверяющих для поиска проблем безопасности давно присутствуют в нормативных документах ЦБ, а также в ряде международных стандартов. В частности, речь идет о ежегодной проверке, а также ежеквартальном сканировании на предмет поиска багов в инфраструктуре, которая отвечает за платежные сервисы. Банки приглашали компании или команды специалистов для проведения пентестов (от англ. "penetration test" — "тест на проникновение".— "Ъ"). Пробуя взломать систему, внешние специалисты (багхантеры.— "Ъ") получали оплату независимо от результата: нашли или не нашли проблему. Но из реального поиска слабых мест, которые надо закрыть, процедура зачастую превращалась в бумажную отчетность. Обычно результаты тестирования описывались техническим языком: в мобильном банковском приложении найдена такая-то уязвимость, на сайте банка — такая то уязвимость, а еще можно аутентифицироваться в интернет-банке в обход системы.

— Что же изменилось в 2023 году?

— Геополитическая ситуация. В 2022 — начале 2023 годов резко усилились атаки на финансовые организации. Необходимо стало эмулировать реальные хакерские атаки.

— Именно в это время начинается активное создание в России платформ Bug Bounty — сервисов, где компании официально приглашают багхантеров искать уязвимости в своих системах и платят за найденные ошибки?

— Да, многие банки, финансовые организации решили: надо привлекать легальных исследователей (белых хакеров). В рамках Bug Bounty работы оплачиваются только при условии, если будут найдены уязвимости. Bug Bounty привлекает почти неограниченное количество хакеров. Это дает возможность при схожем размере бюджета достичь более существенного эффекта. Багхантеры предложили проводить кибериспытания, в рамках которых мы идем дальше, результаты описываются другим языком. Например, это не просто уязвимость в мобильном приложении — она позволяет увести деньги. А через уязвимость в интернет-банкинге можно заполучить список клиентов приват-банкинга и условия их обслуживания, а это уже прямое воздействие на бизнес.

И вот такая информация уже абсолютно понятна руководству финансового учреждения. Хищение денежных средств или отток лояльных клиентов — удар по репутации!

"Выйти за рамки типичности"

— Как технически осуществляется взаимодействие багхантеров с банковской системой?

— Самой популярной формой остаются пентесты. Банк, к примеру, ставит задачу найти уязвимости в своем новом мобильном приложении или при переходе с зарубежного программного продукта на отечественный хочет проверить его защищенность.

— Назовите наиболее подверженные взломам элементы банковских сервисов.

— Можно выделить два самых популярных типа проблем: уязвимости в собственном программном продукте и в программном обеспечении, которое используется как фундамент для автоматической банковской системы, интернет-банкинга и так далее. Например, где-то по-прежнему используется Windows. В нем можно обнаружить огромное количество уязвимостей. А если скомпрометировать платформу, на которой работает банковское приложение, дальше можно делать все что угодно.

Что касается собственных банковских приложений, то, к сожалению, многие компании не соблюдают должным образом процессы их безопасной разработки. Требования установлены Центробанком и правительством. Но нанятые банком программисты далеко не всегда им следуют.

Взять очень типичную историю с полем для ввода пароля. Стандартная длина пароля — от 8 до 20 символов. Но программист не подумал это проверить, поскольку сам использует стандартные пароли.

А у багхантера, наоборот, задача — выйти за рамки типичности. Он вводит в это поле не 20, а 500 символов. Поскольку программа написана криво, такое действие может быть расценено системой как команда. В эту команду можно заложить все что угодно, включая требования слить список всех клиентов, удалить все записи в базе данных, перевести деньги с одного счета на другой.

"Любой инцидент спровоцирован человеческой ошибкой"

— А методы социальной инженерии?

— Это более привычные сценарии, не связанные напрямую с банковской спецификой. В качестве примера можно привести отправку фишингового сообщения операционисту, бухгалтеру или финансисту банка. Якобы речь идет о новых требованиях регуляторов. Электронное письмо может быть замаскировано и под внутренние регламенты финансовой организации. Айтишнику могут отправить послание, что его резюме понравилось компании, в которой открылась высокооплачиваемая вакансия, но прежде надо выполнить тестовое задание. Вредоносный файл из письма позволяет захватить компьютер, оттуда начинается проникновение во внутреннюю инфраструктуру банка. Такой фишинг осуществляется в основном через электронную почту, но в последнее время и через мессенджеры.

Отмечу, что из банков крадут на самом деле не так много данных. Учетные записи клиентов скачивают чаще из почтовых сервисов, соцсетей, с маркетплейсов. Человек — существо ленивое и использует один и тот же пароль для личных сервисов и служебных задач. Утечка пароля помогает злоумышленникам проникнуть в инфраструктуру банка.

— В перечисленных примерах проблему создает человеческий фактор, а не технологическая ошибка. Разве нет?

— По большому счету любой инцидент спровоцирован человеческой ошибкой. Технические решения призваны минимизировать риск. Допустим, в день банковский операционист обрабатывает 30–40 клиентов. Я могу ограничить права его доступа к данным этим числом. Ведь бывает, операционист злоупотребляет неограниченным доступом к клиентским базам. Но банковская архитектура не позволяет ввести ограничения, потому что никто об этом не подумал заранее. А теперь уже сложно вносить изменения в код, потому что у айтишников есть правило: не трогай, пока работает и так далее. Если у руководства банка нет зрелости или ресурсов, такие технические меры реализовать не получится.

— Вы удовлетворены тем, как российские банки реагируют на выявленные угрозы, выстраивают стратегию борьбы за информационную безопасность?

— Десять лет назад была очень популярна схема взлома автоматизированной банковской системы, использование фальшивых платежных поручений и так далее. Сейчас такого практически нет. Процесс перевода денежных средств теперь неплохо защищен. Гораздо более актуальна борьба с DDoS-атаками, когда веб-сайты заваливают

паразитным трафиком, а легальные пользователи не могут подключиться к интернет-банку или мобильному приложению.

Ряд банков архитектурно грамотно подошли к решению этой задачи. Они создали резервную площадку, на которую трафик переключается в ходе атаки. Но это недешевое решение — далеко не каждый может себе это позволить. Банк может сказать: да, я принимаю эти риски и готов нести определенные репутационные потери, поскольку бороться все равно окажется дороже.

В отличие от собственных продуктов банков, мобильные приложения на платформе iOS и Android хакеру очень сложно взломать. Но наш опыт показывает, что через них также можно проникнуть во внутреннюю сеть банка.

По-прежнему проблемой остается банальная невнимательность, когда IT-специалист банка после проведенных работ оставляет открытым внешний доступ к базам с данными клиентов, историей трансакций и т. д. И тогда, подобрав соответствующие настройки, все желающие могут эту информацию скачать.

По нашей статистике злоумышленники начинают активно эксплуатировать обнаруженные уязвимости в течение 24 часов, тогда как айтишники обычно отводят на устранение критических уязвимости семь дней, менее критических — две недели и так далее. То есть хакеры в течение суток могут найти уязвимость и внедриться, а айтишники начинают закрывать дыры в системах через неделю.

— Если сравнить ситуацию примерно двухлетней давности и нынешнюю, уязвимостей стало больше, меньше?

— Объективных данных по России нет, поскольку участников рынка никто не наказывает за непредоставление такой информации. Но ежегодный прирост уязвимостей мы оцениваем примерно в 15%. Об этом же свидетельствует и зарубежная статистика.

"Мы через это уже прошли!"

— Понимаю, что такой статистики тоже нет, но, по вашей оценке, насколько российские банки соответствуют мировому уровню в части кибербезопасности?

— У российских банков зачастую более высокий уровень цифровизации, чем у многих зарубежных финорганизаций. Я имею в виду зрелость технологий, номенклатуру их применения и, главное, цифровой суверенитет. Ряд государств являются в этом смысле заложниками американских компаний.

После отключения средств защиты в России в связи с санкциями многие страны, приняв это во внимание, всерьез задумались о смене цифровой политики или как минимум о том, чтобы иметь запасной план. Мы через это уже прошли, поэтому российские банки находятся на несколько шагов впереди и с точки зрения кибербеза.

Взять США: в этом плане Штаты достаточно консервативная страна. Там даже карты с магнитной полосой до сих пор используются, тогда как в России от них отказались уже много лет назад. В Европе есть достаточно продвинутые банки, а есть менее продвинутые. Работа с финтех-платформами, с тестированием цифрового рубля расширяет наши возможности в области цифровизации и, как следствие, в области технологий кибербеза.

"Число уязвимостей возрастет"

— Какие угрозы появятся в ближайшие два-три года именно для банков?

— Хакеры тоже довольно ленивы, поэтому социальная инженерия останется темой номер один, думаю, еще годы. Человек — самое слабое звено, и, как его ни обучай, он все равно будет ловиться на удочку мошенников. Проблема технических уязвимостей тоже никуда не уйдет. Надо учесть, что программисты теперь для быстрого выпуска продукта на рынок используют различные утилиты с искусственным интеллектом, которые допускают огромное количество ошибок. Мы прогнозируем, что число подобных уязвимостей возрастет. Прибавьте к этому утекшие пароли и учетные данные. Эта тройка лидеров, по нашим данным, не меняется минимум последние пять лет и вряд ли станет иной в ближайшее время.

Что появится нового? По мере того как будет внедряться цифровой рубль, атаки начнутся на него. Мы видим определенные математические ограничения блокчейна и то, что разработчики платформ, связанных с криптовалютами, не уделяют должного внимания безопасности.

Но все это пока будет носить эпизодический характер и на горизонте двух-трех лет не даст злоумышленникам быстрого доступа к деньгам.

Искусственный интеллект сегодня применяют в рамках антифрода, биометрии, анализа огромных объемов данных. Для того чтобы ИИ корректно работал, надо правильно выбирать обучающие данные и модели и защищать их. Иначе есть риск кражи или подмены фальшивыми данными, что приведет к неверному обучению и принятию неверных управленческих решений. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

Хакеры стали чаще атаковать через публичные библиотеки Python. "Ведомости". 11 декабря 2025

Это самый популярный язык у разработчиков, и под ударом может оказаться множество корпоративных решений

Злоумышленники стали активно публиковать библиотеки с зараженным кодом в публичных репозиториях. Количество вредоносных пакетов в репозитории PyPI (Python Package Index), который используется разработчиками на языке программирования Python, за 11 месяцев 2025 г. увеличилось на 54% – до 514 штук

против 333 пакетов в 2024 г. Это приводит к тому, что разработчики, использующие зараженные фрагменты кода, создают решения с уязвимостями. Об этом "Ведомостям" рассказал руководитель департамента Threat Intelligence экспертного центра безопасности Positive Technologies Денис Кувшинов. Специалисты BI.Zone также отмечают рост количества вредоносных пакетов – более чем на 150% по сравнению с прошлым годом.

Python – самый популярный язык программирования в мире, его используют для создания и тестирования прототипов цифровых решений, в аналитике данных и веб-разработке. Доля Python в программировании составляет около 25% по индексу TIOBE (мировой рейтинг популярности языков) в 2025 г. Согласно результатам опроса Stack Overflow 2024, его использовал 51% разработчиков в мире.

Руководитель BI.Zone Threat Intelligence Олег Скулкин указал на рост автоматизации публикаций библиотек с помощью ботов и больших языковых моделей (LLM) для ускоренной генерации больших объемов вредоносного кода. Мошенники применяют тайпсквоттинг – создают библиотеки с названиями, похожими на оригинальные, и публикуют их в открытых репозиториях, добавил он. По словам руководителя направления сертификации Cloud.ru Сергея Барсукова, тайпсквоттинг используется примерно в 70% всех атак с вредоносными пакетами.

В таких библиотеках злоумышленники могут прятать инфостилеры, которые крадут пароли жертв, майнеры, которые используют мощности зараженного устройства для добычи криптовалюты, или трояны-вымогатели, которые шифруют пользовательские файлы и требуют выкуп, говорит Кувшинов. Вредоносные библиотеки могут быть зарегистрированы самим злоумышленником либо публикуются от имени скомпрометированного разработчика уже существующей библиотеки, добавил он.

Некоторые публичные репозитории, например Visual Studio Code Marketplace, Anaconda Packages, автоматически проверяют новые библиотеки на возможные проблемы, говорит Кувшинов. PyPI и NPM (Node Package Manager – главный репозиторий пакетов для JavaScript) не делают таких проверок перед публикацией, но позволяют сообществу информбезопасности (ИБ) и энтузиастам пожаловаться на вредоносную библиотеку, отмечает эксперт.

Но, по данным Positive Technologies, в NPM в 2025 г. количество вредоносных пакетов снизилось почти в 5 раз по сравнению с предыдущим годом. В 2024 г., в мае – июне, прошла крупная кампания вредоносов, уточняет Кувшинов. В NPM уменьшилось и среднее время обнаружения угроз – с 81 дня в 2024 г. до 18 дней в 2025-м, отмечают специалисты Positive Technologies. Барсуков предположил, что в 2026 г. период обнаружения вредоносного пакета может сократиться до 24 часов.

Вредоносная активность, затрагивающая публичные репозитории кода, как правило, не ограничивается какой-то одной страной, ставя цель охватить как можно больше жертв, подчеркивает Кувшинов. "Угроза с распространением вредоносных пакетов касается в том числе и разработчиков из России, но целенаправленного создания вредоносных пакетов под страну, отрасль или компанию мы не наблюдали", – отметил он.

Главной целью злоумышленников остается кража информации, причем особый упор делается на криптовалюту, подтверждают Кувшинов и Скулкин: с помощью вредоносного кода злоумышленники отслеживают буфер обмена для подмены кошельков. При этом как в PyPI, так и в NPM продолжают распространяться стандартные стилеры, нацеленные на конфиденциальные данные, отмечают опрошенные эксперты.

Атака через зараженные пакеты опасна для разработчиков, так как это влечет за собой риск утечки чувствительных данных, кражу ключей и внедрение вредоносов на этапе сборки, говорит Скулкин. От таких атак также могут пострадать компании и госструктуры: вредоносный пакет, используемый в сборке продукта, приводит к компрометации организации. Безусловно, риску подвержены и цепочки поставок, атаки на которые влекут за собой утечки данных, финансовые потери и т. д., добавил эксперт.

По данным BI.Zone TDR, злоумышленники используют зараженные пакеты как для сложных таргетированных атак на конкретные организации, так и для массового заражения. В последнем случае в качестве жертв выступают любые организации или даже физические лица, которые используют то или иное ПО, уточнил Скулкин.

В числе тех, кто находится под угрозой реализации атак с зараженными пакетами и представляет интерес для злоумышленников, Барсуков отмечает корпоративный сектор, которому может грозить утечка коммерческой тайны и клиентских данных, компрометация производственных систем, финансовые потери от простоев, репутационный ущерб и потеря доверия клиентов. "Также стоит отметить облачных провайдеров, которые после реализации атаки могут столкнуться с несанкционированным использованием вычислительных ресурсов, как для создания бот-сетей для реализации DDoS-атак, так и для криптомайнинга", – заключил он. (Ведомости 11.12.25)

К СОДЕРЖАНИЮ

На письмо поставят киберпечать. "КоммерсантЪ". 11 декабря 2025

Как главный почтовый оператор страны развивает ИБ-инфраструктуру в ответ на потребности рынка

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 итогу 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 кибератаками. 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 оградить их от угроз как внутри страны, так и извне. В том числе привлекая опытных партнеров, которые занимаются кибербезопасностью 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 организовывать 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 отдельную 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.

Для справки: Название компании: *Почта России, АО* Адрес: *125252, Россия, Москва, 3-я Песчаная ул., 2а* Телефоны: *+74959562067; +7(800)2005888; +7(495)9569962; +7(343)2270436; +7(343)3567800; +74952765555; +78001000000* Факсы: *+7(495)9569951* E-Mail: *press_service@russianpost.ru; Client@russianpost.ru; reklama-info@russianpost.ru; office@russianpost.ru; client@russianpost.ru* Web: *https://www.pochta.ru; www.market.pochta.ru* Руководитель: *Волков Михаил Юрьевич, генеральный директор* (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

На киберфронте без перемен. "КоммерсантЪ". 11 декабря 2025

Как завершается год для хакеров и их жертв

Подводя предварительные итоги 2025 года, эксперты в области кибербезопасности констатируют качественное изменение угроз: атаки становятся целенаправленнее и разрушительнее, а их продолжительность растет. Финансовый ущерб для бизнеса увеличивается — максимальный запрошенный выкуп достиг 400 млн руб., что на 67% выше показателей 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 разделились. 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 Servicepipe 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 действительно 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 наносят шифровальщики и вайперы (уничтожают данные без возможности восстановления)",— 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 добрались до систем резервного копирования и виртуализации.

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

Наибольшую опасность, по мнению Валерия Баулина, представляют так называемые группы двойного назначения, которые могут, с одной стороны, атаковать жертву и требовать у нее выкуп, как традиционный киберкриминал, а в другом случае — проводить кибердиверсии без требования денег из-за идеи, поскольку аффилированы со спецслужбами других стран.

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 "ненадлежаще невнимательное взаимодействие корпоративных пользователей с внешними ресурсами". Андрей Янкин видит проблему шире: "Если говорить об общих ошибках, то это инерция мышления. Злоумышленник воспринимается как неодушевленный 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 злоумышленникам 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 перехода 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. Взломают рано или поздно всех — вопрос в том, к чему это приведет: к остановке бизнеса или ограниченному ущербу 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. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

"Для злоумышленника важен не размер компании, а наличие у нее данных". "КоммерсантЪ". 11 декабря 2025

Эксперты Positive Technologies о том, почему просто антивируса бизнесу уже недостаточно

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 закрывать 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 остановки 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. Продукт 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?

— Экономия 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 рассмотрение 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 (САВЗ и СОР). 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 (САВЗ) и новые требования к средствам обнаружения и реагирования (СОР) — 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 разрабатывающимся почтовым шлюзом PT Email Security для анализа вложений из почтового трафика. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Как найти свои данные быстрее хакеров. "КоммерсантЪ". 11 декабря 2025

Как трансформируется рынок решений защиты данных в условиях ускоренной цифровизации

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 "Ъ-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. Проблему усугубляют 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 Шкуропата, 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 "СерчИнформ" 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 "нетиповые" каналы передачи, оставляя пробелы.

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 Шкуропат.

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 Staffcop 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".

"Несогласованные 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, злоумышленник может завершить атаку",— предупреждает господин Шкуропат.

При этом эксперты "Кросс технолоджис" 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 продолжать атаку.

Руководитель департамента развития и архитектуры "Кросс технолоджис" 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 координат 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 Рыжков, 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 происходят утечки.

По словам Виктора Рыжкова, 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, DCAP — 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,— поясняют 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 компании обречены на бег впереди угроз, теряя контроль над своей главной цифровой ценностью. (КоммерсантЪ 11.12.25)

К СОДЕРЖАНИЮ

Ущерб бизнеса от корпоративного мошенничества может достигать 5% выручки. "Ведомости". 15 декабря 2025

Ущерб от атак на промышленные компании складывается как из прямых потерь, так и из последствий для операционной деятельности

Средний ущерб промышленных компаний от корпоративного мошенничества составляет около 5% от их выручки, заявил директор департамента управления инвестиционными проектами безопасности и планирования "Норильский никель" Алексей Малинский на форуме "Антифрод Россия" 11 декабря. Он уточнил, что в эту оценку входит как ущерб от умышленных и непреднамеренных действий сотрудников, так и от внешних атак.

С его оценкой согласились и опрошенные "Ведомостями" эксперты. Оценка в 5% в целом совпадает с данными международных исследований по корпоративному мошенничеству среди компаний из разных отраслей, отмечает руководитель направления аналитики и спецпроектов экспертно-аналитического центра InfoWatch Андрей Арсентьев. При этом ущерб небольших промышленных предприятий от корпоративного мошенничества во многих случаях может быть выше 5%, особенно если нарушитель или группа нарушителей остаются незамеченными долгое время, уточнил он.

Экономический ущерб от атак на промышленные компании складывается как из прямых потерь, так и из последствий для операционной деятельности, говорит главный инженер направления информационной безопасности (ИБ) компании "Уралэнерготел" Сергей Ратников.

Существенная часть ущерба приходится на простои оборудования и производственных линий, уточняет он: для крупного предприятия каждый такой день может означать миллионы рублей недополученной выручки. К этому добавляются затраты на восстановление, продолжает эксперт: мобилизация внутренних специалистов, привлечение внешних экспертов, форсированная закупка и внедрение решений по ИБ и модернизации инфраструктуры. В итоге суммарный ущерб почти всегда оказывается значительно выше "первой" суммы хищений или прямого ущерба от инцидента, подчеркнул Ратников.

Подобные случаи тяжким бременем ложатся на бизнес компаний, особенно если компания испытывает проблемы с ликвидностью и только начинает расти. Помимо прямых потерь корпоративное мошенничество влечет ряд косвенных, связанных с изменением настроений инвесторов, контрагентов и клиентов, продолжает Арсентьев. Многие партнеры не хотят продолжать работу с компанией, за которой тянется шлейф уголовных дел и скандалов.

Ощутимость потери в 5% от выручки кардинально различается для компаний в зависимости от их масштаба, говорит директор департамента расследований T.Hunter Игорь Бедеров. Для гигантов промышленности это колоссальные, но чаще всего управляемые суммы, отмечает он: потери исчисляются миллиардами, но диверсифицированная структура бизнеса позволяет смягчить удар.

Место России в мировой промышленности

Согласно данным Всемирного банка, в 2024 г. российская промышленность заняла пятое место среди десятки крупнейших экономик и показала наибольший рост: вклад промышленности в ВВП страны составил $668 млрд.

Чем меньше предприятие, тем значительнее последствия, отмечает Ратников. При этом именно средний бизнес часто недооценивает риски и экономит на комплексных решениях безопасности, становясь легкой целью, добавил Бедеров.

В отдельную группу рисков входят компании, участвующие в государственных закупках или работающие с чувствительными технологиями, отмечает Бедеров. "Для них ущерб от мошенничества не ограничивается финансами. Утечка коммерческой тайны или данных о госзаказе может привести к потере контракта, дисквалификации с торгов и огромным штрафам", – пояснил он.

По данным Curator (ранее Qrator Labs) и BI.Zone, в I квартале 2025 г. на промышленные компании пришлось от 6 до 11% всех целевых кибератак на российские организации, сообщали "Ведомости" в июне. В то же время специалисты сервиса Anti-DDoS группы компаний "Солар" с января по апрель 2025 г. зафиксировали 4600 DDoS-

атак, направленных на предприятия промышленного сектора. В среднем на одну компанию пришлось 72 атаки – это почти на 42% меньше, чем за аналогичный период 2024 г., и на 53% меньше по сравнению с тем же отрезком 2023 г.

В 57% случаев атаки на промышленные компании совершались с целью шпионажа, а в 43% – с целью финансовой выгоды, уточнял представитель BI.Zone.

По оценке F6 (ранее F.A.C.C.T.), выкуп, запрашиваемый вымогателями, в 2024 г. для крупных и средних предприятий начинался от 5 млн руб. "Раньше в действиях хакеров преобладали финансовые цели, но сейчас растет доля атак с политической подоплекой и шпионажем, что является следствием глобального переустройства мира", – подчеркивал Бедеров.

Фишинговые рассылки по-прежнему остаются основной "точкой входа" в информационные системы предприятий, следует из данных F6: в 2024 г. до 80% всех случаев приходилось на вредоносное ПО в фишинговых рассылках, включая шпионское ПО и инфостилеры. Например, в январе 2025 г., по данным F6, APT-группировка Rezet (Rare Wolf) под видом приглашений на семинары по стандартизации оборонной продукции распространяла вредоносные файлы, заражавшие рабочие станции.

"Кроме того, хакеры могут получить и использовать легитимные учетные записи для входа в корпоративные сети поставщиков и уже через них атаковать инфраструктуру жертвы", – напоминал технический руководитель F6 Threat Intelligence Елена Шамшина. (Ведомости 15.12.25)

К СОДЕРЖАНИЮ

Евгений Касперский: "Любое уважающее себя государство шпионит за всеми". "Ведомости". 15 декабря 2025

Основатель "Лаборатории Касперского" о роли искусственного интеллекта в обеспечении цифровой защиты и стратегии развития компании "Лаборатория Касперского" в условиях санкций

Когда в мире еще не задумывались о важности искусственного интеллекта (ИИ), в каждой российской квартире на компьютере уже стоял антивирус "Лаборатории Касперского". Но за последнее десятилетие мир киберпреступлений стремительно эволюционировал от действий хакеров-одиночек к профессиональным цифровым преступникам и государственному шпионажу. В интервью "Ведомостям" основатель "Лаборатории Касперского" Евгений Касперский рассказал о тенденциях в кибербезопасности, влиянии геополитики и технологий ИИ, а также о стратегии развития компании на международном рынке в условиях санкций и ограничений. Среди ключевых тем беседы также - попытки хакеров проникнуть в саму "Лабораторию" и возможное привлечение новых инвесторов.

- Как изменился характер кибератак за последние три года?

- Мир киберзловредства стал гораздо более широким и более профессиональным. Раньше нам приходилось бороться с хулиганами, которые какой-то ерундой занимались, затем произошел качественный скачок - появилось гораздо больше высокопрофессиональных хакерских атак. Геополитика стала довольно жесткой, и хакеры превратились в полноценных кибершпионов. Теперь любое уважающее себя государство шпионит за всеми.

Помимо того, мы все чаще встречаемся со случаями киберсаботажа. То есть когда атаку совершают не для того, чтобы украсть или подсмотреть что-нибудь, а чтобы уничтожить. Соответственно, и решения по безопасности сейчас гораздо сложнее и более развиты, чем те, что были раньше. Поэтому иногда провести грань между тем, что понимается под антивирусом, и вообще всей линейкой продуктов безопасности очень сложно.

- Как ИИ повлиял на кибератаки и на инструменты защиты от них?

- Технологиями, которые сейчас называются искусственным интеллектом, мы занимаемся уже более 20 лет. Это умные, сложные системы, где полно математики, но это не интеллект. Изначально речь шла о том, что нам нужно создать систему автоматической обработки входящей информации. Сейчас мы каждый день анализируем примерно 15 млн подозрительных файлов, которые получаем с ханипотов, краулеров, спам-ловушек, благодаря мониторингу ботнетов, через Kaspersky Security Network (анонимизированно и добровольно), от экспертов и энтузиастов по всему миру, через обмен экспертной информацией об угрозах с партнерами и другими вендорами, а также в рамках технической поддержки и реагирования на инциденты. Даже с конкурентами мы ведем постоянный обмен нашего улова. Чтобы выяснить, что из этого является зловредным, а что нет, 99,98% обрабатывается автоматически, с помощью ИИ.

Еще есть системы, например детекторы аномалий для выявления подозрительной активности в режиме реального времени, которые тоже подходят под категорию ИИ. Допустим, в сети на рабочих станциях или в телефонах происходит что-то не то. Например, компьютер какого-то сотрудника внезапно начинает массово подсоединяться к устройствам, с которыми раньше никогда не взаимодействовал. Система классифицирует это как подозрительную активность и может заблокировать действие или предупредить пользователя. Таким образом удается вылавливать самые зловредные и профессиональные атаки.

Ежедневно мы обнаруживаем около полумиллиона новых вредоносных файлов. Мы даже можем определять зловреды, которые сделаны с помощью ИИ, но пока это единичные случаи.

"Падение продаж в Европе компенсировалось взрывным ростом в России и Азии"

- В российском информационном поле довольно часто говорят о киберугрозах и о том, как компании с ними справляются, из-за чего уровень осознанности у российского обывателя достаточно высокий. Такой же ли он высокий и в других странах?

- Это зависит от региона. Если говорить про Европу - да, они там все понимают. Если говорить про Латинскую Америку, то уровень осознанности ниже. В Азии это зависит от страны. В 2010-2015 гг. мне приходилось объяснять, что кибератаки могут быть такими, что ущерб может быть неприемлем. Тогда на международных конференциях объявляли "пункт номер шесть, кибербезопасность". Сейчас, наверное, это пункт номер один.

- Как у вас распределена выручка по регионам?

- Можно провести грань между российскими продажами и зарубежными и между потребительским (b2c) и бизнес-(b2b) сегментами. Потребительский сегмент сейчас приносит нам примерно треть всей выручки, но он стагнирует. Это связано с тем, что в США нам заблокировали продажи, это сильно ударило по потребительскому направлению. В то же время корпоративный бизнес растет очень быстро, в прошлом году продажи выросли на 19%.

- В целом на потребительский бизнес у вас какая доля продаж приходится?

- Сейчас примерно 30%, но она уменьшается в этом году. Не люблю прогнозы, но не исключаю, что по результатам этого года может оказаться 25%. Зато b2b у нас очень хорошо идет.

Сразу отвечу по поводу продаж в России. Их доля сильно зависит от геополитической ситуации. В 2015 г., когда в России был экономический кризис, но при этом геополитическая напряженность еще не достигла нынешнего уровня, структура выручки выглядела так: около 20% приходилось на Россию и 80% - на зарубежные рынки. Сейчас, из-за ухода западных поставщиков из России и из-за ограничений, которые ввели западные страны в отношении нас, ситуация выровнялась - примерно 50 на 50%. В США для нас фактически введен запрет на работу. В Европе последние три года объемы снижались примерно на 10% ежегодно. Падение продаж в Европе после 2022 г. компенсировалось за счет взрывного роста в России и на Ближнем Востоке, в Азии.

За что я люблю Азию? В Европе страны, конечно, разные, но в целом они похожи. В Латинской Америке ситуация схожая: государства формально разные, но в основе у них общее испанское или португальское наследие. Азия - совсем другое дело. Здесь все по-настоящему разное: религии, культуры, модели поведения, уклад жизни. Абсолютно все отличается.

- Как это влияет на бизнес?

- Прямо.

- Есть страны, которые не имеют никаких проблем в отношениях с Россией, а есть государства, которые находятся под сильным влиянием Соединенных Штатов. Например, Япония.

- В Азии есть четыре территории, которые находятся в зависимом положении: Япония, Тайвань, Южная Корея и Сингапур. Сингапур старается проводить более самостоятельную политику, и его государственные структуры даже являются нашими клиентами - не в большом объеме, но тем не менее. Таиланд, Индонезия - совсем другая история, там геополитика не так сильно отражается на бизнесе.

- В Европе некоторые страны выступали за то, чтобы отказаться от продуктов "Лаборатории Касперского", как в США, но такого запрета в итоге принято не было?

- Во-первых, я не исключаю, что некоторые госорганизации остаются нашими клиентами. Во-вторых, у нас есть серьезные клиенты - компании в Европе, которые, несмотря на рекомендации отказаться от российских продуктов, все равно пользуются нашими решениями. Раскрыть я их по объективным причинам не могу. Основная проблема рынка в Европе - большая зависимость от США, но, к счастью, аналогичных ограничений принято не было.

- Ликвидируете ли вы свои иностранные активы?

- Американскую компанию закрываем, юрлицо в Великобритании - тоже. При этом холдинговая компания, зарегистрированная в Великобритании, продолжает свою работу. Мы закрываем там, где не нужны активы больше, а где хорошо - открываем или оставляем, например в Германии, Испании, Италии, Франции. В 2023 г. открыли в Саудовской Аравии офис, в 2024-м - в Колумбии, во Вьетнаме совсем недавно тоже.

- Кто ваши партнеры сейчас?

- По всему миру у нас более 18 000 партнеров, с которыми мы развиваем бизнес. Это разные компании, которые делают продукты и сервисы на наших технологиях, реселлеры, системные интеграторы и сервис-провайдеры.

"Даже iOS с закрытой экосистемой не застрахована от уязвимостей"

- Очень часто вирусятся новости, когда "Лаборатория Касперского" находит уязвимости в продуктах каких-нибудь крупных компаний вроде Apple, Huawei или Android. Как в этих компаниях реагируют на такое?

- Когда нашли уязвимости у Apple, они их оперативно закрыли. Один из азиатских производителей ноутбуков, где мы нашли серьезную уязвимость, тоже отреагировал и выпустил патч, но не сразу. Это было около пяти лет назад. В основном говорят "спасибо, что нашли" и выплачивают вознаграждение, но и негативные ситуации тоже бывают.

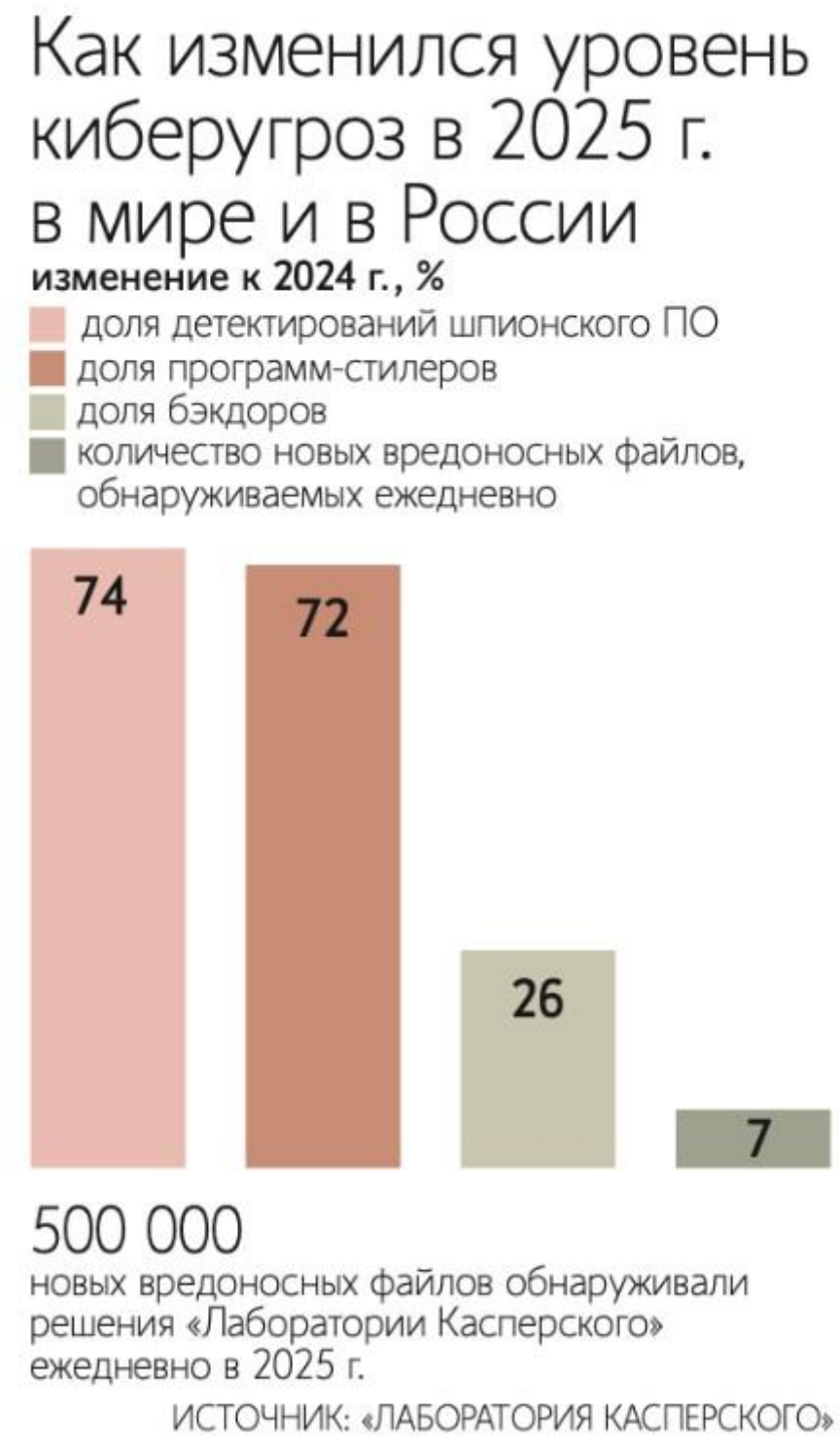
- Сталкивались вы со случаем промышленного или коммерческого шпионажа в вашей компании?

- Первый раз это было в 2015 г. В отелях в Швейцарии, где проходили переговоры по иранской ядерной программе, мы нашли вирусную шпионскую программу - Duqu. Те же злоумышленники залезли к нам прямо в вирлаб - туда,

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

где "куются" технологии. Тогда атаку быстро заметили, так как в нашей инфраструктуре проходило тестирование нового решения для защиты от целевых атак и кибершпионажа.

А второй раз, два года назад, одна из самых сложных за историю кибершпионская операция "Триангуляция" показала, что даже iOS со всей своей закрытой экосистемой не застрахована от уязвимостей, встроенных прямо в архитектуру операционной системы. У некоторых наших сотрудников в айфоне сидел вирус. Наши эксперты обнаружили, что процессор на устройствах Apple фактически находился в режиме отладки, что открывало полный доступ к памяти аппарата. Это закладка еще на уровне железа. Скорее всего, это было на всех устройствах, но активировать уязвимость можно было, точно зная особенности реализации. Авторы операции "Триангуляция" обладали этими знаниями и использовали их в своей атаке. Вирус сливает всю информацию вплоть до геопозиции, скорости и направления движения, какие устройства вокруг есть по Bluetooth, кто рядом с вами находится.



- Вы поэтому не пользуетесь техникой Apple?

- Не поэтому, я просто не люблю Apple. Тот же айфон - это черный ящик.

- А к вам обращались из других стран с просьбой поделиться отчетами по тому, как вы обнаружили зараженные телефоны?

- Да, мы рассылаем технические отчеты, это отдельное направление нашего бизнеса, называется Threat Intelligence, кибербразведка по-русски. Такие отчеты не для широкой публики, потому что там слишком много информации. Негодяи же тоже читают, учатся, мы не хотим их учить. Более подробную техническую информацию мы рассылаем по подписке, а некоторыми данными делимся со всем рынком. Недавно, например, выпустили отчет на 300 страниц по 14 хакерским группам. Там есть и финансово мотивированные злодеи, мы относим их к кластеру Ghouls, и группировки, которые занимаются кибершпионажем, их мы называем Likho. Этот отчет доступен всему рынку и будет полезен всем специалистам по информационной безопасности.

- На китайском рынке вы тоже работаете?

- Через партнеров и в основном с малым и средним бизнесом. Китайское правительство обязывает крупных игроков использовать только отечественные продукты, тем не менее даже эти компании интересуются нашими индустриальными решениями и уже упомянутой кибербразведкой.

"Теперь главное - бежать быстро"

- Если говорить про тренд на импортозамещение и независимость продуктов - такой же ли он в других странах, как в России?

- Главный тренд, который сейчас есть, - это "киберзаконодательство", которое принимается или в разработке. Когда все данные находятся на территории страны - никаких внешних облаков. И это сейчас заботит абсолютно всех. Те страны, которые могут себе позволить собственные продукты по кибербезу, - запрещают использовать продукты из других стран. Но собственные продукты по кибербезу могут себе позволить несколько стран, крупнейшие - США, Китай и Россия.

- Какие продукты в России нужно импортозаместить в первую очередь?

- В сфере ИБ - все. Но главный упор - это NGFW, файрвол. Мы начали заниматься этой темой с 2020 г., за это время инвестировали в проект несколько десятков миллионов долларов. Я считаю, что у нас лучшее положение в этой нише, потому что мы уже очень давно работаем с этими решениями, но не как производители, а как поставщики технологий. Соответственно, мы знаем, как это работает, технологии у нас есть, опыт есть. Мы объединили все это и оформили в виде железки. Недавно мы прошли последний этап сертификаций - ФСТЭК. К 2026-2027 гг., полагаю, мы станем полностью конкурентоспособными на российском рынке.

- В конце 2024 г. под эгидой Центробанка банки тестировали российские файрволы. В закрытом отчете говорилось, что банки остались не удовлетворены ни одним из существующих отечественных решений.

- Есть такие решения, я не буду называть их. Нам сказали следующее: у Kaspersky NGFW очень хорошая перспектива выйти на конкурентоспособный уровень в ближайший год. Теперь главное - бежать быстро.

- То есть ваши продукты уже тестируются заказчиками? Уже работают?

- Мы вывели на рынок коммерческую версию NGFW в августе. До этого заказчики и партнеры почти год тестировали две беты. Это и банки, и транспорт, были гиганты отечественного энтерпрайза, чья инфраструктура гораздо больше нашей. Всего было около полусотни пилотов.

"Мобильная операционка сейчас на стадии исследовательского проекта"

- У вас есть продукт KasperskyOS. Заявлялось, что это будет в том числе и мобильная операционная система. Что сейчас происходит с решением?

- Операционная система работает на тонком клиенте (упрощенный вариант рабочего компьютера, который не обрабатывает данные локально, а подключается к серверу или облачной инфраструктуре. - "Ведомости"). Это то, что уже есть, то, что работает и продается.

Похвастаться большими объемами продаж я пока не могу, но в этом году мы провели более 100 пилотных проектов и в России, и за рубежом. Это госсектор, энергетика, образование, промышленность и финансы. Два ключевых партнера по тонким клиентам: российский "ТОНК" и китайский Centerm - первый наш зарубежный партнер по операционке. Помимо Китая партнерства есть еще в Индонезии, Малайзии и Европе. Помимо обозначенных выше это еще разработчики отечественных VDI-платформ (Virtual Desktop Infrastructure - технология виртуализации, которая позволяет запускать операционные системы, приложения, файлы на централизованных мощных серверах в дата-центре, а не на локальных компьютерах сотрудников. - "Ведомости") Basis, Veil, Termidesk и Space. У меня в планах, чтобы таких компаний было много, чтобы на нашей операционке выпускалось как можно больше разных девайсов. Мобильная операционка сейчас на стадии исследовательского проекта. **Прототип есть, но он сырой пока.**

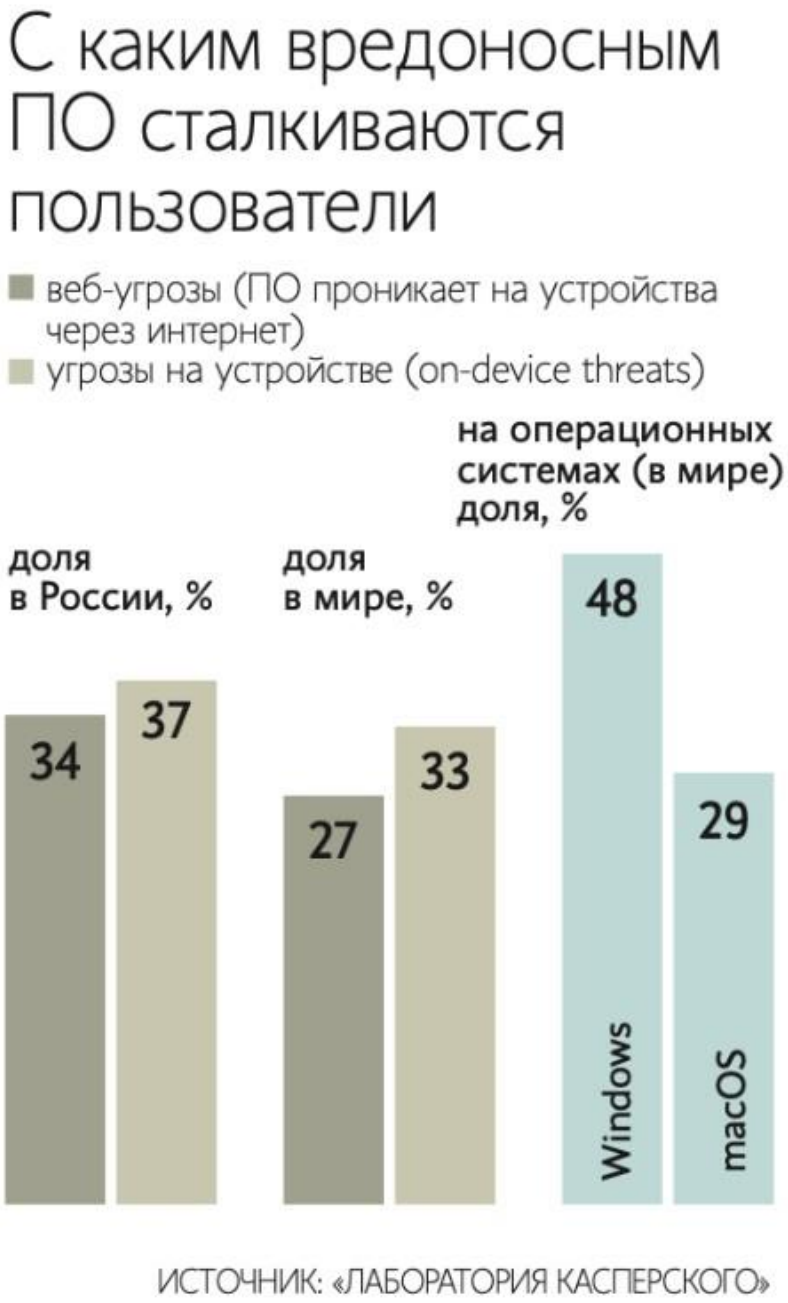
- Почему сейчас нельзя купить телефон на KasperskyOS?

- Пока не готово, нет достаточного количества приложений. Сейчас важно работать в двух направлениях. Первое - привлекать производителей железа (смартфонов и планшетов), которые заинтересованы, чтобы устройство было невозможно взломать. Потенциально сейчас это азиатские и российские компании.

Второе направление - это привлечение разработчиков. У нас есть обучающие курсы, мы работаем с университетами, например с академией наук и МАИ. В МАИ в 2023 г. мы выпустили шесть человек по программе

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

по операционной системе. В Петербургском политехе делают свои решения, студенты экспериментируют с разными проектами на нашей операционке. Эти проекты нужны для работы над архитектурой. Она должна работать не на дырявых системах, а на правильных. И мы надеемся, что оба эти направления будут развиваться, к ним присоединится больше участников.



ИСТОЧНИК: «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- У нас довольно большой выбор отечественных десктопных операционных систем. Почему не получилось так же сделать большой выбор потребительских или корпоративных мобильных ОС?

- В России много чего не получилось сделать. На Луну тоже не получилось человека отправить.

- Мне кажется, мобильную операционку сделать проще, чем на Луну слетать.

- Чуть проще и дешевле, согласен.

"Большую часть решений мы могли импортозаместить еще в 2015 г."

- Минцифры вас как-то привлекает к разработке регулирования в сфере ИБ?

- Конечно, наши сотрудники участвуют во многих рабочих группах и комиссиях.

- Связан ли рост продаж в России с требованиями регулятора по переходу на отечественный софт?

- И да и нет. На это повлияли два фактора, которые сложились вместе.

Первый - в России в целом за последние несколько лет повысился уровень зрелости компаний в вопросах ИБ. Этому способствовали и взрывной рост кибератак, и изменения законодательства, и цифровизация, которая помогла существенно повысить эффективность бизнеса.

Второй - мы сильно расширили свою линейку начиная с 2015 г. В 2012 г. мы начали разработку KICS (Kaspersky Industrial CyberSecurity - комплексная платформа для мониторинга промышленной безопасности. - "Ведомости"), нашего индустриального решения, в 2015 г. оно вышло, пошли первые индустриальные продажи. Потом мы сделали не только продукт для защиты промышленных рабочих мест, но и сети. Потом пошли EDR, XDR, начали делать свою SIEM-систему (Endpoint Detection and Response - решение для мониторинга угрозы на конечных устройствах, Extended Detection and Response - объединенная платформа для обработки информации об инцидентах в сфере информбезопасности, Security Information and Event Management - система управления событиями, которая централизованно собирает, анализирует и коррелирует данные о безопасности со всех устройств в IT-инфраструктуре. - "Ведомости"). Иными словами, мы начали делать не только традиционный антивирус.

В 2022 г. не только фактор импортозамещения сыграл роль. Сегодня больше 90% компаний в России используют различные наши решения, причем не для галочки, а чтобы обеспечить стабильность своих бизнес-процессов. При этом большую часть решений мы могли импортозаместить еще в 2015 г., качество уже позволяло. И на зарубежные рынки мы вышли тоже исключительно по причине качества.

"У нас есть два больших серьезных инвестпроекта"

- И все-таки в 2022 г. был какой-то скачок по финансовым показателям именно в России или все у вас просто планомерно растет из года в год?

- В 2022 г. продажи в России увеличились в полтора раза, в 2023-м - больше чем на треть, в 2024-м - больше чем на четверть. Это отличные результаты!

- А если говорить про финансовые показатели и прогноз на 2025 г.?

- В мире в долларах целимся в рост выручки примерно на 3%. Как глобальная компания, мы считаем наши показатели традиционно в долларах.

- Компания сохраняет чистую прибыль с учетом того, что вы сейчас много вкладываетесь в развитие в Азиатском регионе? Вы всю прибыль перенаправляете?

- Не всю. У нас есть два больших серьезных инвестпроекта. Это операционка, во-первых, которая дорого стоит. Второе - это "Мойофис", они пока не прибыльны.

- Планируете ли вы продавать "Мойофис"?

- Если кто-то заинтересуется инвестициями в компанию, захочет стать соучредителем, совладельцем - мы не исключаем, что рассмотрим такой вариант.

- Сейчас вы ведете какие-то переговоры об этом? Есть ли интересы?

- Периодически да. Но до стадии "меморандума" не дошло.

- Почему у "Мойофиса" плохие финансовые результаты? (В 2021 г. выручка компании составила около 841,8 млн руб. В 2022 г. показатель резко вырос - примерно до 3,4 млрд руб., компания тогда получила чистую прибыль в размере около 386 млн руб. В 2023 г. выручка сократилась на 43,8%, примерно до 1,9 млрд руб. В пресс-релизе за 2024 г. говорилось, выручка "МойОфис" увеличилась порядка до 2,01 млрд руб., показав рост по сравнению с 2023 г., однако так и не вернувшись к пиковым значениям 2022 г.)

- Очень просто. Во-первых, несмотря на то что международные компании якобы ушли с рынка, клиенты продолжают использовать их продукты. Чаще всего бесплатно. Или переходят на опенсорс. В итоге реальный спрос сжался более чем на порядок.

Во-вторых, пока функциональность не доходит до продуктов Microsoft, но динамика очень хорошая. Наши клиенты говорят, что они пользуются решениями "Мойофиса", и им нравится скорость, с которой мы обновляем продукт.

Мы верим, что ребята справятся. Не можем не верить: там половина топ-менеджмента - это наши бывшие сотрудники. Просто дайте время компании. У нас тоже был период, когда "Лаборатория" тормозила, научились же. Если мы зависим от процессора, то мы постоянно должны что-то менять, и мы это делаем, в то время как Microsoft изначально разрабатывался под Windows - он на ней и существует.

- Есть ли сейчас какой-то антикризисный сценарий для "Мойофиса"?

- Нам нужен нормальный отечественный софт, отечественный офисный пакет. Все остальное, что есть на рынке, - чистый опенсорс. А это небезопасно. В 2022 г., когда в опенсорс-пакетах начали массово появляться "закладки", мы создали отдельный сервис, позволяющий их выявлять, - на текущий момент в нем содержится информация примерно о 22 000 "протрояненных" пакетах.

"Мне комфортнее владеть частной компанией"

- Нужен ли вам сейчас стратегический партнер?

- Наверное, будет зависеть от условий. Вы знаете, я немножко консервативен. Мы долго не покупали никаких компаний, потому что у меня был негативный опыт покупки антиспама. Но тогда это был достаточно большой коллектив, у них были свои принципы разработки, свои архитектуры продуктов, это все пришлось перемолоть. 50% [сотрудников ушло в результате, а заняло это год. А если бы мы создавали собственное с нуля - три года и инвестиции в собственный продукт.

Потом немножко поменялась моя точка зрения. Сейчас условия импортозамещения таковы, что нужно как можно быстрее выпускать продукты, "допиливая" необходимое "вчера". Но все-таки, что касается выхода на биржу и привлечения инвесторов, если потребуется - выйдем, хотя мне комфортнее владеть частной компанией.

- Сколько сейчас совладельцев у компании и кто они?

- Я и Вадим Богданов, один из разработчиков. Все остальные продали свои акции. (Доли совладельцев Касперский раскрывать не стал. - "Ведомости".)

- Вас продолжают звать на международные конференции?

- Конечно. Раньше было еще чаще - Европа, Штаты. Одно время было девять кругосветок просто по бизнесу, рекордная командировка - два месяца, это было почти бесконечно.

- Вы жалуетесь или хвастаетесь?

- Хвастаюсь.

- Честно?

- Да. Я счастливый человек.

АО "Лаборатория Касперского" IT-компания

Основные акционеры (данные "СПАРК-Интерфакс"): ООО "Группа компаний Касперского" (100%, бенефициар - Kaspersky Labs Limited (99,99%).

Финансовые показатели (РСБУ, 2024 г.):

выручка - 55,9 млрд руб.,

чистая прибыль - 7,4 млрд.

Основана в 1997 г. Занимается разработкой программных решений для обеспечения IT-безопасности. Портфолио компании включает в себя комплексную защиту цифровой жизни и личных устройств, ряд специализированных продуктов и сервисов, а также кибериммунные решения для борьбы со сложными и постоянно эволюционирующими киберугрозами.

По данным компании, в 2024 г. глобальная выручка "Лаборатории Касперского" составила $822 млн.

Для справки: Название компании: *Лаборатория Касперского, АО* Адрес: *125212, Россия, Москва, Ленинградское шоссе, 39, литера А, стр.3, БЦ «Олимпия Парк»* Телефоны: *+74957978700* Факсы: *+74957978709* E-Mail: *info@kaspersky.com* Web: *https://www.kaspersky.ru/* Руководитель: *Касперский Евгений Валентинович, генеральный директор* (Ведомости 15.12.25)

К СОДЕРЖАНИЮ

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Цифровой двойник

В АГИКИ будут создавать цифровые двойники северных поселений.

Ректор Арктического государственного института культуры и искусств (АГИКИ) Саргылана Игнатьева анонсировала крупные проекты вуза в 2026 году на юбилейном XV Международном форуме "Арктика: настоящее и будущее" имени А. Н. Чилингарова. Она подчеркнула, что благодаря участию в программе технологического лидерства "Приоритет-2030" фокусом образовательного учреждения стали технологии, основанные на культурном коде Арктики.

"Мы четко видим свою нишу – это культурное наследие коренных народов, которых сегодня насчитывается более 500 миллионов человек, живущих в 90 странах мира. Культурный код, унаследованный от предков, сейчас проявляется в современных продуктовых решениях: в мастер-планах и дизайн-кодах территорий, в музейных и библиотечных проектах по сохранению наследия, в цифровизации культурных фондов, в ювелирных изделиях, музыке, кино и анимации. В 2026 году стартуют два крупных направления: создание цифровых двойников северных поселений и дизайн-инжиниринг для Арктики", - отметила ректора АГИКИ, выступая на сессии "С опорой на культурный код: экономический потенциал креативных индустрий".

На сессии "В Арктику по любви: инструменты просвещения" ректор АГИКИ привела несколько реальных примеров того, как Север становится "второй родиной" для талантливых молодых людей, одержимых своей профессией. По ее словам, чтобы полюбить Арктику, нужно узнать её через свой личный опыт, понять через смыслы и ощутить через эмоции и сообщество.

Оргилбаяр Нямжав – студент из Монголии, талантливый хореограф, амбассадор, который, как он считает, навсегда связан с институтом. Именно он "проторил" дорогу из Монголии в АГИКИ другим молодым людям, желающим творчески самореализоваться.

Другой студент – Адилет Каримов из Кыргызстана приехал в институт, почувствовав в нем атмосферу творчества, миссионерских задач и современных возможностей. Вслед за ним ежегодно в институт приезжают выпускники Ошского музыкального училища, чтобы построить не просто карьеру, а насыщенную жизнь, которой будут гордиться.

"Современный мир стал очень мобильным, и у Арктики есть возможность стать "Северным фронтиром" – территорией свободы, творчества, миссии и больших возможностей. А любовь возникает там, где есть личная история, положительные эмоции и точка приложения своих сил. И наша задача – дать молодым людям возможность написать такую историю в Арктике!" - заключила Саргылана Игнатьева. (INFOLine, ИА (по материалам Администрации Республики Саха (Якутия)) 10.12.25)

К СОДЕРЖАНИЮ

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

Системы передачи данных

МТС укрепляется на рынке pLTE в 2025 году.

Лидером по реализации проектов в этом сегменте, эксперты Telecom Daily называют компанию МТС. С 2018 по 2025 годы, по данным агентства, компания запустила 69 коммерческих и пилотных сетей, что составляет 43% рынка. На втором месте, согласно исследованию Telecom Daily, расположился Мегафон, запустив 56 проектов (35%), а на третьем - Ростелеком с 7 проектами (4%). Еще 30 запусков были реализованы другими участниками отрасли (18%). По общему количеству коммерческих проектов, эксперты Telecom Daily также отдали лидерство МТС - на долю компании приходится 39 запусков (43%).

По итогам внедрений в 2025 году, эксперты Telecom Daily отмечают преимущество МТС по общему числу запусков, в 2025 году, по данным аналитиков, запущено 42 проекта, из которых 19 реализовано МТС, 17 из них - коммерческие (45% от общей суммы проектов), 18 проектов реализовала компания Мегафон (43%) и еще 5 - другие поставщики pLTE-решений (12%).

Среди основных отраслей-заказчиков горнодобывающая промышленность (46%), нефтегазовый сектор (16%), транспорт (12%), энергетика (11%) и нефтехимия (8%).

Средняя стоимость проектов заметно колеблется от года к году, отмечают эксперты.

В 2021-2023 годах цена могла варьироваться от нескольких десятков миллионов до более чем 150 млн руб., а в 2024 году диапазон стал шире: от компактных сетей стоимостью 50-90 млн руб. до крупных инфраструктурных решений, превышающих по цене 200 млн руб. Отдельные комплексные проекты стоили свыше 500 млн руб.

Согласно исследованию, трендом рынка является активное импортозамещение и переход на российское оборудование и ПО, стимулируемый государственной политикой технологического суверенитета и включением pLTE в национальные программы цифровизации. Сети все чаще интегрируются с ИИ и edge-решениями для обработки данных в реальном времени, а с переходом к p5G частные сети станут платформой для запуска новых индустриальных сценариев.

Кроме того, аналитики отмечают рост популярности модульных решений и гибридных архитектур, сочетающих pLTE со спутниковой связью в отдаленных регионах. Рынок также смещается в сторону модели "сеть как услуга" (SaaS), что делает технологии доступными для среднего бизнеса, и формируются предпосылки для вторичного рынка оборудования. При этом сохраняются такие вызовы, как дефицит квалифицированных кадров, рост затрат и повышенные требования к надежности и безопасности сетей.

Эксперты отмечают, что основной спрос на pLTE формируют отрасли с высокой операционной зависимостью от надежной связи. Рынок постепенно переходит от пилотных испытаний к серийным внедрениям. Прогнозируется, что в ближайшее время сегмент pLTE/5G будет стабильно расти на 25-30% в год.

Для справки: Название компании: *МТС, ПАО* Адрес: *109147, г. Москва, вн.тер.г. муниципальный округ Таганский, ул. Воронцовская, д. 1/3, стр. 2А* Телефоны: *+78002500890* E-Mail: *pr@mts.ru; mrm.pressa@mts.ru* Web: *https://mts.ru* Руководитель: *Минин Михаил Владимирович, генеральный директор; Николаев Вячеслав Константинович, президент* (ComNews.ru 12.12.25)

К СОДЕРЖАНИЮ

Маломобильная связь: в России появится стационарный интернет на базе 5G. "Известия". 10 декабря 2025

В России легализуют технологию фиксированного доступа в интернет на базе стандарта 5G, узнали "Известия" из материалов Госкомиссии по радиочастотам. Она позволяет подключать к сети квартиры и офисы на скорости до 1 Гбит/с. В Минцифры считают, что технология 5G FWA пригодится там, где заводить отдельный кабель в каждый дом сложно и нерентабельно. Речь может идти о подключении к интернету коттеджных поселков, окраин городов, других малоэтажных населенных пунктов с небольшой плотностью застройки, говорят эксперты. По их мнению, технология может быть востребована на фоне периодических отключений мобильного интернета и роста спроса на фиксированный доступ в Сеть.

Чем стационарный 5G отличается от мобильного

В России могут разрешить использование технологии фиксированного беспроводного доступа в интернет на базе радиопротокола 5G (5G FWA). Это следует из материалов Госкомиссии по радиочастотам (ГКРЧ), с которыми ознакомились "Известия". Ее заседание должно состояться в конце декабря.

Госкомиссия намерена выделить неопределенному кругу лиц частоты в диапазоне 27,8-28,4 ГГц и 28,8-29,4 ГГц - на них должны работать средства связи, использующие временной дуплекс (метод разделения каналов, позволяющий более экономно использовать частоты), говорится в документах.

Этим требованиям как раз отвечает 5G FWA, указал один из специалистов по частотному планированию. Не следует путать ее с мобильным 5G - FWA и характеристики, прописываемые в проекте решения ГКРЧ, предназначены именно для стационарной связи, уточнил он.

По словам собеседника "Известий", радиус действия базовых станций этого стандарта может достигать нескольких километров при наличии прямой видимости и использовании внешней антенны, а скорость доступа по этой технологии - до 1 Гбит/с. 5G FWA хорошо подходит для подключения к интернету коттеджных поселков, окраин городов, других малоэтажных населенных пунктов, где плотность застройки невелика, отметил собеседник "Известий". Переход на современный радиоинтерфейс позволяет использовать высокие полосы частот, которые сейчас простаивают, поскольку изначально выделялись для устаревших фиксированных технологий, утверждает он.

Также 5G FWA позволяет подключать к интернету на высокой скорости квартиры и офисы, в которые интернет был проведен десятки лет назад, и где инфраструктура доступа устарела физически и морально и не обеспечивает нужные скорости передачи данных, добавил специалист.

Актуальна технология и в свете периодических отключений мобильного интернета, и как следствие - роста интереса к фиксированному доступу. Дело в том, что сигнал при подключении по 5G FWA хоть и передается по воздуху, но на частотах, которые не используются для массовой мобильной связи. В силу малого радиуса действия их бессмысленно использовать для управления дронами, объяснил источник на рынке связи. Соответственно, даже в случае отключений мобильного интернета для защиты от БПЛА, эти частоты глушиться не будут.

Частоты, о которых идет речь в материалах ГКРЧ, были переданы для гражданского использования еще в конце 2010-х годов. Но и в России, и за рубежом они оказались практически невостребованными сотовыми компаниями - из-за того, что радиус действия базовых станций при подключении со смартфонов очень невелик, строить сети, покрывающие города, нерентабельно и неэффективно, рассказывали "Известиям" участники рынка.

Вопрос о выделении этих частот для FWA вынесли на ГКРЧ, потому что отрасль телеком решила опробовать их для разработки отечественных решений, а также проработки бизнес-модели оказания услуг, отметили в Минцифры, курирующем работу госкомиссии.

- Эта технология находит применение в тех районах, где заводить отдельный кабель в каждый дом сложно и нерентабельно. FWA набирает популярность в мире, но на территории России пока не получила распространения, - объяснили в ведомстве.

Будет ли востребован в РФ фиксированный беспроводной интернет

ГКРЧ рассмотрит вопрос о частотах для 5G FWA по заявке "Эр-Телеком Холдинга", одного из крупнейших в РФ операторов фиксированной связи, говорится в материалах комиссии. При этом в случае положительного решения госкомиссии сети FWA могут быть запущены и другими интернет-провайдерами.

В "Эр-Телекоме" и МТС отказались от комментариев. "Известия" также направили запрос в "Вымпелком".

В "Мегафоне" считают выделение частот для 5G FWA заделом на будущее. Использование беспроводных решений для организации фиксированного доступа может рассматриваться как один из вариантов развития сетевой инфраструктуры, считают в компании.

- Однако необходимость и конкретные параметры применения таких технологий зависят от утвержденных нормативных требований, доступности частотного ресурса и экономической эффективности. Мы внимательно отслеживаем потребности рынка и оцениваем окупаемость подобных проектов - именно эти факторы определяют целесообразность внедрения новых технологических решений, - добавили в "Мегафоне".

По словам партнера ComNews Research Леонида Коника, сети 5G в формате FWA успешно внедряются в США.

- В стране до сих пор огромное количество частных домов в небольших городах - так называемая "одноэтажная Америка" - имеют выход в интернет по медным телефонным проводам. Для того чтобы разом дать таким пользователям быстрый интернет и при этом не проиграть во времени кабельным операторам, сотовые компании пошли по пути развития FWA, - рассказал он.

Вопрос о выделении российским связистам частот для новой технологии доступа поднят в то время, когда начали случаться отключения мобильного интернета и пользователи начали сильнее интересоваться фиксированным. Во второй половине 2025 года спрос на его услуги возрос как со стороны частных пользователей, так и малого и среднего бизнеса, отметил сотрудник одного из операторов. Люди стали чаще заказывать подключения квартир и домов, хотя до недавнего времени базовые потребности удовлетворяла именно мобильная связь - многие даже смотрели ТВ, подключаясь по мобильному трафику, утверждает собеседник "Известий".

Интерес к фиксированному доступу в интернет вне городов повышается с 2020 года, отметили в Минцифры. Этот тренд неизменный и связан с миграцией пользователей за город в летний период и ростом сегмента удаленной работы, объяснили в ведомстве.

Только в июне-июле 2025 года спрос на Wi-Fi-роутеры в РФ по сравнению с аналогичным периодом 2024 года вырос вдвое, рассказывали "Известиям" продавцы и операторы. Покупают их как граждане, так и малые и средние предприятия, утверждали они. В частности, на Wildberries реализация проводных Wi-Fi-роутеров летом этого года выросла на 134%.

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

Любое выделение частот - позитивное событие для отрасли связи, считает гендиректор TelecomDaily Денис Кусков. Внедрение 5G FWA позволило бы в перспективе решить многие вопросы, связанные с подключением к интернету не только труднодоступных районов, но и прилегающих к крупным городам территорий. В коттеджных поселках и селах зачастую действительно проблематично провести кабель, признает эксперт. Более того, там, где он есть, доступ зачастую обеспечивают морально устаревшие технологии, добавил Денис Кусков. (Известия 10.12.25)

К СОДЕРЖАНИЮ

Программное обеспечение

Российские энергетические компании направляют 90% цифрового бюджета на отечественное ПО.

В 2024 компании топливно-энергетического комплекса потратили около 150 млрд рублей, из которых более 90 млрд — на закупку российского ПО в нефтегазовой отрасли

На Международном энергетическом форуме Energy Space 2025 замминистра энергетики Эдуард Шереметцев сообщил, что компании российского энергетического сектора тратят 90% своего цифрового бюджета на закупку отечественного программного обеспечения. Об этом передает ТАСС.

По словам чиновника, отрасль уже несколько лет целенаправленно работает над достижением технологического суверенитета России. Речь идет о формировании способности самостоятельно разрабатывать, производить и внедрять критически важные технологии — именно они призваны обеспечить устойчивость и безопасность отечественной энергетики.

Шереметцев подчеркнул, что энергетический сектор входит в число лидеров по темпам импортозамещения и демонстрирует ощутимые результаты. В качестве примера он привел показатели по ПО: в целом по отрасли 90% цифровых расходов приходится на российские решения, а в атомной энергетике доля отечественного ПО достигает 85%.

Кроме того, Шереметцев напомнил, что в 2024 году компании топливно-энергетического комплекса потратили около 150 млрд рублей, из которых более 90 млрд рублей пришлось на закупку российского ПО в нефтегазовой отрасли. (Реальное время 09.12.25)

К СОДЕРЖАНИЮ

Участники IT-рынка указали на ограничения из-за новых правил допуска в реестр ПО.

Собеседники "Ъ" опасаются, что новые правила допуска в реестр российского ПО могут ограничить доступ к льготам для малых и средних разработчиков. Правительство 9 декабря утвердило изменения в порядок формирования реестра, дающего право на налоговые преференции и отсрочку от армии.

Теперь производители программно-аппаратных комплексов для генеративных ИИ должны иметь не менее 1 эксабайта хранения данных, не менее 1 тыс. GPU для машинного обучения и собственный ЦОД в России мощностью от 10 МВт.

Также введены требования к чипам "с матричными умножителями" с производительностью от 8,75 PFLOPs FP4, а также сетевым адаптерам от 400 Гбит/с с RDMA. В аппарате вице-премьера Дмитрия Григоренко утверждают, что постановление "не отсекает возможности по попаданию в реестр" и вводит лишь "дополнительную категорию" для ИИ-ПАК, не ужесточая условий для других разработчиков.

Основатель WMT AI Игорь Никитин отмечает, что российский рынок пока не производит такие чипы: "Эксабайт хранилища и сетевые подключения на 400 Гбит/с — это уровень крупных технологических компаний". По его оценке, инфраструктурные затраты вырастут на 40–70%. Независимый эксперт Алексей Лерон предупреждает, что концентрация ресурсов у нескольких игроков может поднять цены и снизить гибкость B2B-сегмента.

По словам источника "Ъ" в ИТ-компании, наличие мощностей "никак не гарантирует качества конечного ИИ-продукта": более логично оценивать итоговое ПО. Он считает требование о собственном ЦОДе искусственным барьером. (КоммерсантЪ 12.12.25)

К СОДЕРЖАНИЮ

Личная ответственность за чужой код. "КоммерсантЪ". 10 декабря 2025

Уголовные риски нарушения прав на ПО: что нужно знать бизнесу?

Гражданские иски о нарушении авторских прав на ПО — довольно привычная практика для IT-рынка. Однако уголовные дела, вменение легализации средств и персональные риски для руководства становятся новой реальностью. Управляющий партнер Criminal Defense Firm Алексей Новиков и советник практики интеллектуальной собственности ЮК ЭБР Артем Евсеев предупреждают: слабым звеном в деле может оказаться экспертиза, а главной угрозой — неверная оценка стоимости "нарушенных" прав, которая и превращает правонарушение в преступление.

Программное обеспечение сегодня — один из ключевых нематериальных активов бизнеса. Правообладатель программного продукта получает исключительные права на использование программы: от установки и воспроизведения до модификации, распространения и предоставления доступа в облаке (SaaS). Охрана возникает автоматически с момента создания кода, а значит, любое несанкционированное использование ПО влечет риски нарушения авторских прав.

Традиционно основным инструментом защиты таких прав остаются гражданские споры в арбитражных судах: взыскание денежной компенсации за нарушение прав, изъятие контрафактных копий ПО и прочее. Для многих компаний эти инструменты являются управляемым коммерческим риском — вопрос лишь в цене урегулирования спора и перестройки бизнес-процессов. Однако практика последних лет показывает, что споры вокруг ПО все чаще

выходят за рамки гражданских исков и переходят в уголовно-правовую плоскость, затрагивая уже не только финансовые активы компании, но и персональную ответственность менеджмента.

Не так давно совместная работа двух юридических компаний, Criminal Defense Firm и ЭБР, помогла защитить гражданина России от обвинения в нарушении авторских прав и легализации денежных средств, полученных преступным путем, с которым он столкнулся на территории государства—члена Совета Европы. Наработанный опыт позволяет нам последовательно разобрать, как доказать или опровергнуть наличие прав на ПО, в каких случаях могут возникнуть уголовно-правовые споры о ПО, какую роль играют экспертизы и позиция правоохранительных органов и что должен знать бизнес для минимизации собственных рисков.

Наличие прав на ПО

Права на ПО возникают в силу факта создания продукта, однако на практике правообладателю нужно доказать, что ему действительно принадлежит исключительное право на конкретный продукт. В России и большей части стран ЕАЭС и СНГ доказательства принадлежности авторских прав можно разделить на две категории в зависимости от того, кем был создан продукт — собственное ПО и ПО, полученное от иных лиц. В первом случае правообладатель должен показать, что в трудовую функцию его работников входило создание соответствующих продуктов. Для доказывания прав на ПО могут потребоваться трудовые договоры, должностные инструкции с работниками, служебные задания, локальные акты по вопросам создания служебных произведений и другие документы. Если же речь идет о ПО, полученном от иных лиц, то компания может приобрести исключительное право на уже готовый продукт либо заказать его разработку у подрядчика. В таком случае для доказывания своих прав компании необходимо будет предоставить такие договоры.

Доказывание нарушения

Для того чтобы подтвердить наличие нарушения, потребуется обратиться к эксперту за проведением компьютерно-технического исследования на предмет возможных заимствований и незаконных модификаций в спорном ПО. Такая экспертиза назначается правоохранительными органами после возбуждения уголовного дела. Однако для того, чтобы добиться возбуждения, потерпевшему рекомендуется подготовить внесудебное исследование для подтверждения обоснованности своих требований. В свою очередь, будучи подозреваемым, необходимо занять не менее проактивную позицию, подготовить собственное исследование, поручив его опытному эксперту, а также провести рецензирование экспертизы, назначенной следствием, чтобы подтвердить наличие в них существенных методологических ошибок.

Сложность современных программных продуктов и методологий выявления совпадений между их функциональными компонентами зачастую приводит к тому, что следователи испытывают затруднения при постановке вопросов экспертам и последующей оценке содержания заключения. Экспертиза по уголовным делам в сфере авторских прав, где предметом преступления являются IT-продукты, превращается для защиты в обоюдоострый меч: ее можно использовать как довод невиновности или непричастности доверителя. Одновременно с этим она же становится препятствием для проведения полноценного расследования в условиях обвинительного уклона, когда сторона защиты в своих доводах об отсутствии состава преступления опирается на изначально порочную экспертизу.

Более того, наличие большого объема совпадений в сравниваемых продуктах само по себе не может являться основанием для подтверждения нарушения. Так, современное ПО во многом состоит из различных open source компонентов, которые любой разработчик может включить в свой продукт. Однако далеко не каждый сотрудник правоохранительных органов будет углубляться в последние тренды в области защиты интеллектуальной собственности, чтобы разглядеть нюансы в вопросах вины разработчика. В результате следствие часто может принимать позицию потерпевшего, изложенную в заявлении, хотя в рамках спора о нарушении интеллектуальных прав суд мог бы с ней не согласиться.

Нарушение перерастает в преступление

Одна из многих проблем в правоприменении, особенно свойственная законодательству стран СНГ,— отсутствие понимания того, какие именно последствия должны наступить, чтобы незаконное использование авторских прав перестало быть лишь гражданско-правовым нарушением и приобрело черты преступного посягательства. Водоразделом является "размер" правонарушения, который определяется исходя из стоимости нарушенных прав.

Можно предположить, что один лишь размер доходов разработчика, нарушившего авторские права, не позволяет сделать вывод, что содеянное является преступлением. Зачастую при расследовании уголовных дел на первый план выходит вопрос об упущенной выгоде, но даже стоимость реализованных продуктов необходимо правильно посчитать, что требует от следователей познаний в области IT и бизнес-процессов конкретного потерпевшего.

Следствие часто ориентируется на результаты внутреннего расследования потерпевшего, что приводит к парадоксальной ситуации: для определения преступления учитывается суммарная стоимость каждого экземпляра контрафактной продукции, но не по цене, по которой она была реализована обвиняемым, а по цене, установленной правообладателем, даже если таковая противоречит рынку. Возникает логичный вопрос: почему следствие назначает экспертизу по установлению факта нарушения, но не проводит аналогичное исследование для определения действительной стоимости нарушений?

Вменение легализации

INFOLine информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

Следующая проблема заключается в том, что при установлении состава преступления по нарушению прав на ПО следствие зачастую вменяет обвиняемому совершение еще одного преступления — легализации денежных средств, приобретенных преступным путем. При этом финансовые операции с доходами от реализуемого ПО вменяются разработчику как самостоятельное преступление — отмывание денежных средств.
Чем подобная неопределенность в правоприменении грозит добросовестным разработчикам на рынке IT-продуктов? В экстремальных случаях можно увидеть, что некоторые компании способны использовать уголовное преследование по этой статье как способ агрессивной борьбы с конкурентами или даже как обоснование собственных финансовых потерь.
В такой ситуации важно заранее понимать, как минимизировать уголовно-правовые риски в своей операционной деятельности. Опыт позволяет прийти лишь к одному выводу — необходимости применения упредительных мер и осуществления комплексной защиты вместе с IT-юристами и адвокатами по уголовным делам. Упредительными мерами могут стать проверка "чистоты" прав на программный продукт, анализ использованных сторонних компонентов, проведение тренингов для разработчиков по алгоритму действий в случае инициирования уголовного преследования и ряд других. Именно такие действия в тандеме позволяют предупредить возможные риски и сохранить бизнес разработчика и его свободу. (КоммерсантЪ 10.12.25)

К СОДЕРЖАНИЮ

Главные драйверы российского DevOps - ИИ и безопасность. "ComNews.ru". 10 декабря 2025

По словам директора дивизиона платформы "Сфера" АО "Т1" Евгения Косиненко, главными драйверами российского DevOps в ближайшие годы станут кибербезопасность и искусственный интеллект. При этом он отметил, что импортозамещение для российских компаний станет фоном, а на первые роли выйдут конкуренция за эффективность, скорость инноваций и построение интеллектуальных платформ.
Так он прокомментировал выводы ИТ-холдинга Т1 в отчете "ИТ-рынок в России 2025-2026: импульсы, энергия и потенциал". Согласно ему, от 80% до 90% корпоративного софта разрабатываются на базе сторонних библиотек и open-source-компонентов. С одной стороны, это ускоряет вывод цифровых решений, с другой - делает внешний код точкой потенциальной угрозы. Из-за этого крупные компании переходят к безопасным конвейерам разработки.
Евгений Косиненко добавил, что отчет основан на публичной информации, данных авторитетных источников и аналитического агентства компании и экспертизе ИТ-холдинга Т1.
С этими выводами согласился технический директор платформы GitFlic ООО "Ресолют" (Входит в "Группу Астра") Максим Козлов. Он назвал их общемировым трендом и отметил, что он задается не столько революцией на рынке искусственного интеллекта, сколько грядущей индустрией 5.0, к которой мир шел с середины 1980 гг. Ее основой является автоматизация процессов и принятия решений, безопасность автоматизации - ее естественное следствие.
"Я бы не ставил на использование ИИ в вопросах разработки, поскольку по тем же отчетам компаний ИИ лишь алгоритмизирует ранее неавтоматизированный труд, который человек выполнял за машину. Все же важными аспектами в разработке продуктов является принятие оптимальных решений (ранжирование среди нескольких вариантов) и учитывание противоречий в работе - на это способен лишь интеллект и процесс размышления, к коим генеративные модели или LLM, сугубо, отнести нельзя, ввиду отсутствия, как это ни странно, собственно интеллекта. В связи с этим главным драйвером считаю процессы обеспечения ИБ и их стандартизация", - заявил ведущий инженер группы систем защиты АСУ ТП ООО "Газинформсервис" Никита Фокин.

Будущее за платформами с ИИ

"Те компании, на которых регуляторные требования не давят напрямую, предпочли остаться на зарубежных решениях без обновлений и поддержки, в то время как остальные постепенно завершили импортозамещение. За несколько лет на российском рынке появилось множество полноценных инструментов разработки, которые не уступают зарубежным аналогам, а в отдельных нишах - превосходят их гибкостью и адаптацией под инфраструктуру заказчиков. Тем не менее миграция остается сложным и инерционным процессом: корпоративные специалисты привыкли к интерфейсам западных инструментов, смена пайплайнов требует глубокого пересборки архитектурного конвейера, а эффект образовательных программ проявится только через поколение молодых DevOps кадров, для которых локальные продукты будут "родными", - говорится в сообщении компании.
Помимо этого, по данным Т1, искусственный интеллект превращается в полноценный инструмент разработки. Использование нейросетей в корпоративных процессных конвейерах снижает порог входа для начинающих разработчиков, компенсирует кадровый дефицит и высвобождает время для решения сложных задач. Согласно сообщению Т1, гибридные платформы не ограничивающие свободу разработки и рекомендующие лучшие практики - будущее DevSecOps-решений.
По словам Евгения Косиненко, многие российские платформы для разработки ПО уже содержат ИИ-инструменты, оптимизирующие затраты на тестирование, ускоряющие кодинг и выявляющие ошибки на ранних этапах. Он отметил, что если уровень зрелости измерять именно по ИИ, то отечественные платформы могут отставать от западных, но в целом они активно используются крупнейшими компаниями, а это свидетельствует об их высокой состоятельности.

"ИИ, как и ожидалось, стал хорошим помощником для оптимизации деятельности и фактически может выполнять роль второго пилота, но только когда оператор сам является экспертом в нужном вопросе. Однако ИИ в ближайшие годы не заменит полностью человека, кроме того, бездумное использование ИИ может сильно навредить компании и сотрудникам в виде недостоверных результатов и утечек данных", - отметил архитектор информационной безопасности, vCISO ООО "Юзергейт" (UserGate) Дмитрий Овчинников.

Спрос на DevSecOps растет

"Недоверие к SaaS и облачным сервисам делает корпоративную разработку по настоящему локальной: все - от CI/CD и DevOps инструментов до специализированных ИИ - должно быть развернуто внутри корпоративного периметра. Бизнес требует отчуждаемых систем, которые обучаются и дорабатываются на площадке заказчика, не передавая данные вовне. Это формирует модель, сравнимую с "автоматизированной кабиной авиалайнера", где рутинные действия делегируются системе, а разработчик управляет направлением и стратегией. Такая универсальная интеллектуальная "надстройка" для DevSecOps-платформ - тренд, который будет определять структуру ИТ-рынка в ближайшие годы", - гласит сообщение Т1.

Евгений Косиненко отметил, что не последнюю роль в общем интересе к DevSpecOps в 2025 г. играло огромное количество кибератак. По его словам, они заставили бизнес пересмотреть подходы к безопасности и сосредоточится на проверке программного обеспечения на этапе разработке для минимизации рисков и повышения защиты от угроз.

"В 2025 г. DevOps в России проходит этап зрелости - команды переходят от механической автоматизации к стратегическому управлению жизненным циклом продуктов. Главным трендом является интеграция безопасности на всех этапах разработки, то есть полноценный переход к DevSecOps. Если раньше безопасность рассматривалась как завершающий этап, то теперь она встроена в CI/CD-пайплайн: автоматизированные проверки, анализ зависимостей и мониторинг инфраструктуры стали обязательными элементами. Второе направление - активное использование ML и ИИ для оптимизации работы DevOps-инженеров: от анализа логов и выявления аномалий до автоматического подбора конфигураций и прогнозирования отказов систем. Это помогает командам не просто ускорять релизы, но и снижать долю человеческих ошибок", - рассказал руководитель отдела администрирования и DevOps MD Audit АО "Фабрика ПО" (SL Soft FabricaONE.AI, акционер - ГК Softline) Александр Демин.

О тенденции, когда затраты на информационную безопасность увеличиваются, а количество уязвимостей в корпоративных продуктах растет, рассказал директор по техническому консалтингу АО "Аксиом" (Axiom JDK) Алексей Захаров. По его мнению, многие компании совершают ошибку, делая упор на защиту периметра без контроля уязвимостей внутри, но сегодняшние атаки почти всегда начинаются с фишинга или социальной инженерии. По его словам, организациям нужно постоянно обновлять компоненты, проводить внутренние тесты на проникновение и так далее.

"Невозможно построить безопасный контур, если фундамент системы зависит от иностранных технологий, чьи обновления, репозитории, ключи подписи и механизмы доставки могут быть недоступны или изменены в любой момент. Речь идет не только о специализированных средствах защиты, но также о среде исполнения и серверах Java-приложений, операционных системах, контейнеризации, CI/CD-платформах, гипервизорах и системных библиотеках", - отметил он.

Рост спроса на DevSecOps отметил лидер продукта Nova Container Platform ООО "Орион" (Orion Soft) Александр Фикс. По его словам, потребность формируется не только через требования регуляторов, но и со стороны команд разработки, которым нужен предсказуемый и безопасный процесс поставки ПО.

С ним согласился директор департамента по инструментам и технологиям выпуска версий и тестированию ООО "Диасофт" Александр Захаров. Он отметил, что требования безопасного производства и эксплуатации ПО - типовое как для финансовых организаций, так и для компаний из других отраслей экономики. По его словам, требования обычно делятся на несколько разделов, такие как "управление рисками", "безопасная разработка и сборка", "всесторонняя проверка" и другие.

"Запрос на DevSecOps-практики есть, и он только растет. Подтверждение этому - рост количества обучающих курсов и материалов в интернете. Безопасная разработка всегда начинается с базы: безопасной инфраструктуры сборочной среды, настройки доступов и обучения персонала безопасным приемам работы. Одновременно с этим необходимо быть внимательными к заимствованным компонентам, отсутствию паролей, токенов и ключей в открытом виде, а также применению продуктов класса SAST и DAST. Финальным этапом является обучение разработчиков правильному проектированию ПО с точки зрения безопасности. Все это в итоге и делает продукт максимально защищенным, но при этом экономически выгодным для разработчиков", - заключил Дмитрий Овчинников. (ComNews.ru 10.12.25)

К СОДЕРЖАНИЮ

Иван Мыздриков: "Рынок корпоративного ПО входит в фазу упорядочивания". "Ведомости". 15 декабря 2025

Директор по продуктам VK Tech - о промежуточных итогах импортозамещения, предпочтениях бизнеса в софте и технологических трендах

После волны импортозамещения основным драйвером рынка корпоративного программного обеспечения стала цифровизация бизнес-процессов. Об этом в интервью изданию "Ведомости. Инновации и Технологии" заявил директор по продуктам VK Tech Иван Мыздриков. Также он рассказал о том, какие задачи сейчас в приоритете у компаний, как решаются проблемы безопасности в условиях растущего числа кибератак и как искусственный интеллект меняет отрасль.

- Продолжается ли рост российского рынка корпоративного программного обеспечения (ПО)? Какие наблюдаются тенденции?

- Рост рынка до 2024 г. был во многом обусловлен продолжающимся импортозамещением. Сегодня основной фактор роста - цифровизация и сопутствующие процессы, например увеличение объемов данных, которые бизнесу нужно хранить, обрабатывать и анализировать. На первый план выходят задачи, связанные с созданием эффективной инфраструктуры, закрывающей ключевые потребности бизнеса, - от продвинутых облачных платформ до удобных сервисов коммуникаций и продуктивности, это и стимулирует спрос. Например, за девять месяцев 2025 г. наша клиентская база выросла в четыре раза - до 26 800 компаний.

- Можно ли считать, что импульс импортозамещения исчерпан?

- Ряд крупных российских организаций, в частности, госучреждения и объекты критической инфраструктуры, действительно прошли этот этап и сейчас фокусируются на повышении эффективности за счет внедрения отечественных цифровых решений.

Однако не во всех отраслях сроки импортозамещения прошли: согласно национальному проекту "Экономика данных", у российских организаций в ключевых отраслях экономики есть время до 2030 г. Для сегмента малого и среднего бизнеса вопрос перехода на отечественные системы ранее не стоял так остро, но сейчас зарубежные вендоры прекратили поддержку своих решений в России, эти решения каждый день неизбежно устаревают. В свою очередь, российские компании давно предлагают конкурентоспособные альтернативы, которые учитывают локальную специфику и потребности клиентов.

"Безопасность становится во главу угла"

- С какими запросами приходят клиенты?

- Большой запрос на безопасность продуктов: шифрование хранимых и передаваемых данных, тщательную проверку безопасности конечного продукта, процесса разработки и сервиса, гарантированную работоспособность, резервное копирование данных, запись и хранение истории действий для разбора инцидентов.

Разработчики, реагируя на этот запрос, усиливают защиту своих решений, в том числе за счет интеграции сервисов в единые платформы с офлайн-доступом и шифрованием. Например, одно из основных обновлений платформы для корпоративных коммуникаций VK WorkSpace также было направлено на усиление безопасности. В его рамках мы вывели все сервисы: почту, мессенджер, календарь, видеозвонки, диск с документами, оргструктуру и опросы - в единый суперапп. Он теперь работает в офлайне с почтой и календарем, есть шифрование и дополнительные функции безопасности на устройствах пользователей. Также в этом году мы выпустили линейку новых сервисов информационной безопасности (ИБ).

- Как в целом решается вопрос с безопасностью корпоративного ПО, особенно при его использовании компаниями с широкой сетью филиалов в разных точках и офисах по всей стране?

- Вопрос безопасности предельно важный и актуальный. В 2025 г. только за первые восемь месяцев количество кибератак, направленных на российские облачные и гибридные сервисы, согласно экспертным оценкам, достигло 105 млн. Таким образом, за январь - август 2025 г. было зафиксировано больше инцидентов, чем за 2023 г. и 2024 г. вместе. Поэтому мы внимательно следим за безопасностью корпоративного ПО и постоянно ее совершенствуем.

Безопасность становится во главу угла для большинства разработчиков. Например, мы регулярно сканируем информационную инфраструктуру, привлекаем независимых исследователей проверять наш код и сообщать об уязвимостях в рамках программы Bug Bounty. Проводим внутренние и внешние аудиты, тесты на проникновение. Исходный код нашего ПО на постоянной основе подвергается статическому и динамическому анализу, то есть мы смотрим на него в состоянии покоя и во время работы. Все требования к ИБ задокументированы и доступны сотрудникам, они постоянно совершенствуют навыки безопасной разработки.

"Цифровизация и импортозамещение остаются актуальными для бизнесов из всех отраслей"

- Насколько сфера отечественного корпоративного ПО сейчас конкурентна? Можно ли назвать рынок установившимся или его ждут изменения?

- Российский рынок корпоративного ПО входит в фазу упорядочивания и консолидации: крупные разработчики будут укреплять свои позиции, повышая зрелость своих продуктов и расширяя линейки новыми решениями. Нишевым игрокам в такой рыночной ситуации будет все сложнее соперничать с лидерами по функциям.

- Кто в первую очередь формирует спрос: госструктуры, крупный бизнес или малый и средний бизнес?

- В отечественных решениях заинтересованы все. Средний или малый бизнес предпочитают разворачивать сервисы в облаке, так как у этих компаний зачастую нет своей инфраструктуры и требуется быстрое подключение. Госсектор и крупный бизнес, наоборот, предпочитают внедрять решения в своем периметре по подписке. Таким клиентам важнее держать все в собственном дата-центре, в соответствии с собственными политиками безопасности.

"Облачные сервисы будут одним из главных драйверов рынка в ближайшие годы"

- В большинстве технологических направлений сейчас применяется ИИ. Как нейросети и машинное обучение используются в сегменте корпоративного ПО?

- ИИ - безусловно, главный технологический тренд, а также один из приоритетов национального развития. Мы в VK Tech внедряем ИИ во внутренние процессы, в том числе используем в разработке, реализуем соответствующие возможности в продуктах. Например, LLM-сервис помогает нашим менеджерам продукта быстро и структурировано формулировать, уточнять и проверять бизнес-требования, превращая сырые идеи в четкие концепции. Кроме того, ИИ применяется для автоматической проверки кода и умного поиска по документации.

Мы активно развиваем сервисы с применением ИИ в области клиентской поддержки. В VK Cloud, VK HR Tek и VK WorkSpace часть обращений обрабатывается автоматически с помощью сервисов на базе языковых моделей. В дальнейшем мы планируем расширять пользовательский опыт на базе ИИ-инструментов.

- Согласно базовому прогнозу Strategy Partners, в течение ближайших пяти лет рынок корпоративного ПО в России будет расти в среднем на 24 % в год и в 2030 г. составит 727 млрд руб. За счет каких сегментов и направлений возможен такой рост?

- В целом облачные сервисы - и частные, и публичные - будут одним из главных драйверов рынка в ближайшие годы, в том числе за счет спроса на инфраструктуру для ИИ и машинного обучения. Решения для управления данными как базовый слой в пирамиде потребностей ИИ тоже будут динамично развиваться.

В сегменте офисного ПО будут продолжать действовать факторы импортозамещения и отложенного спроса.

Одно из самых быстрорастущих направлений VK Tech - HR Tech и бизнес-приложения. Так, у нас за девять месяцев 2025 г. почти в два раза выросла выручка по бизнес-приложениям: Tax Compliance для управления финансами и операционного менеджмента, Process Mining для управления операционными процессами и рисками и HR Tek для автоматизации функций отдела кадров. (Ведомости 15.12.25)

К СОДЕРЖАНИЮ

Координационный центр по доработке ПО в ТИМ выбрал главную цель. "ComNews.ru". 16 декабря 2025

К 2028 г. Координационный центр развития по доработке программного обеспечения в области технологий информационного моделирования (ТИМ) определил главную цель - разработать решение, которое позво-лит формировать и развивать информационную модель на всех этапах - от прединвестиционного этапа до эксплуатации.

12 декабря состоялась стратегическая сессия Координационного центра, посвященная итогам работы в 2025 г. и формированию стратегических задач на 2026-2028 гг. Цели сессии подвел заместитель начальника департамента ПАО "Газпром" Сергей Буторов. По совместительству он является председателем координационного центра по доработке программного обеспечения в области ТИМ.

По итогам встречи участники определили следующие задачи:

1. Упростить процесс проектирования для инженеров.
2. Организовать эффективное взаимодействие с государственными регуляторами.
3. Получить от строительного подрядчика пожелания и требования к информационной модели. Обеспечить синхронизацию на этапе строительно-монтажных работ.
4. Интегрировать ООО "Нанософт разработка" в структуру Координационного центра по доработке программного обеспечения в области ТИМ.

Сергей Буторов напомнил, что 23 января 2025 г. на сессии ТИМ в топливно-энергетическом комплексе (ТЭК), организованной ПАО "Газпром", участники обсудили обмен опытом и развитие сотрудничества. Итогом той встречи стало единогласное решение по созданию координационного центра.

Инициатором создания Координационного центра развития (КЦР) по доработке программного обеспечения в области ТИМ выступило ПАО "Газпром", в проект вошли такие компании, как АО "МХК ЕвроХим", ПАО "Сибур Холдинг", ГК "СиСофт", а также ГК "Росатом". Основная задача центра - развитие отечественного программного обеспечения на основе обратной связи с пользователями.

Исполнительный директор АО "СиСофт Девелопмент" Игорь Орельяна Урсуа заявил, что при создании Координационного центра развития не верилось, что ГК "СиСофт" сможет выровнять требования от разных заказчиков: "У крупных заказчиков есть видение развития, поэтому мы корректируем планы по развитию продукта, синхронизируя их с этим видением. Итогом взаимодействия в Координационном центре развития стало позитивное движение, благодаря которому нам удалось улучшить управляемость процессами и оптимально выстроить работу команд".

На вопрос корреспондента ComNews, возможно ли участие в Координационном центре для компаний не из ТЭК, и какие экспертизы были бы полезны для центра, Сергей Буторов ответил, что внутри Координационного центра обсуждалась возможность расширения состава центра за пределы ТЭК: "С одной стороны, у нас есть своя специфика, с другой - мы ограничены рамками отрасли и не видим полной картины. Поэтому мы рассматривали возможность включения в состав центра компаний из других отраслей. Что касается критериев отбора, то мы

информационное агентство | information agency | 199155 Санкт-Петербург пр. КИМа 28 | +7-812-322-6848 +7-495-772-7640 | mail@advis.ru

обсуждали этот вопрос. Важно найти баланс между пересечением интересов и смежными вопросами. Даже если компания не из ТЭК, но ее деятельность пересекается с нашими интересами, мы будем рады ее видеть в составе центра".

Сергей Буторов пояснил, что все, что находится за пределами опыта ТЭК, представляет интерес, так как это новые подходы и мышление. "Например, мы общаемся с другими компаниями, и нам интересны их идеи по использованию информационного моделирования в различных циклах работы, очень ценны для нас", - сказал председатель Координационного центра ТИМ.

Сергей Буторов отметил, что Координационный центр развития ТИМ также рассматривает возможность сотрудничества со стартапами и студенческими разработками: "Хотя члены нашего центра - крупные компании и холдинги, иногда именно молодые проекты предлагают нестандартные решения, на которые мы, возможно, не обратили бы внимания. В этом есть потенциал для развития".

Заместитель генерального директора по информационным технологиям ООО "Газпром проектирование" Вячеслав Гурьянов рассказал о достижениях компании в работе с участниками Координационного центра. Он отметил, что главным результатом стала организация процесса по систематизации задач и выработке алгоритмов взаимодействия специалистов - участников КЦР. Это позволило четко определить, как выстраивать коммуникацию и ставить задачи, чтобы специалисты вендора могли их эффективно решать.

Вячеслав Гурьянов отметил, что если говорить о новых компаниях, которые могли бы стать членами центра, интерес есть к еще одному отечественному вендору: "Мы уже обсудили этот вопрос в рабочем порядке и даже согласовали приглашение. Очень надеюсь, что они официально акцептуют его, так как на рабочем уровне они уже подтвердили участие в Координационном центре".

Руководитель отдела комплексных решений ГК "СиСофт" Александр Белкин рассказал про статус исполнения пунктов дорожной карты развития программных продуктов ГК "СиСофт": "Мы внедрили в последние версии программного обеспечения около 5000 задач. Они касались доработки, оптимизации и улучшения функционала. Что касается портала Stakeholders (проект участников Координационного центра - прим. ComNews), то к нему подключено 140 пользователей. Мы создали 765 задач, из которых 135 уже выполнены, а 65 закрыты. Остальные задачи находятся в процессе выполнения".

Александр Белкин напомнил, что в июне 2025 г. на базе ООО "Газпром проектирование" в Саратове технические координаторы провели встречу: "На ней мы отобрали 74 приоритетные задачи и разделили их на блоки. Первый и второй блоки разработаны на основе дорожной карты. В них входит 51 задача. Из них 15 уже выполнены, а 36 находятся в работе. Третий блок составили задачи, выбранные техническими координаторами. Мы добавили их на портал Redmine. На данный момент восемь задач решены, а 15 находятся в процессе выполнения".

Александр Белкин отметил, что кроме работы с порталом Stakeholders "СиСофт" провел семь демонстраций реализованного функционала во флагманских продуктах: генплан, стройка, трубы, кабельные хозяйства. "Мы также познакомили пользователей с комплексной методологией работы в системах Model Studio (MS) и XLib (X library - библиотека функций клиента системы X Window, написанная на языке Си - прим. ComNews), включая передачу заданий между отделами", - сказал Александр Белкин. (ComNews.ru 16.12.25)

К СОДЕРЖАНИЮ

Мультимедиа

На связи с облаком: как сервисы коммуникаций повышают эффективность бизнеса. "Ведомости". 10 декабря 2025

Решения Telecom API позволяют сократить расходы на работу колл-центра на 18%

По мере того как IT-системы, используемые для управления бизнесом, становятся все сложнее, у компаний появляется потребность интегрировать их с телекомсоставляющей. Простой пример такой интеграции - это возможность в один клик позвонить клиенту, записанному в CRM-системе. С технической точки зрения за подобные возможности отвечает Telecom API. Так называют набор интерфейсов, которые телекомоператоры предоставляют разработчикам, чтобы те напрямую использовали возможности сетей в своих приложениях и сервисах.

Рынок растет

Mordor Intelligence оценивает мировой рынок Telecom API в $353,87 млрд в 2025 г. с потенциалом роста к 2030 г. до $687,83 млрд. По доле выручки с показателем 35,7% на этом рынке в 2024 г. лидировали API-интерфейсы обмена сообщениями. Почти половина услуг телекоммуникационных API (49,85%) предоставлялась в 2024 г. с помощью "гибридного облака" - IT-инфраструктуры, совмещающей публичные и частные облачные сервисы. По прогнозам Mordor Intelligence, такой тип инфраструктуры будет расти на 15,5% ежегодно до 2030 г.

В России похожая динамика. По данным "TMT консалтинга", объем российского рынка Telecom API в 2023 г. увеличился на 26% до 5,8 млрд руб. Более поздних данных нет, но есть прогнозы. Они предусматривают ежегодный рост рынка на 23-25% в 2024-2025 гг.

По данным разработчика коммуникационных решений для бизнеса МТС Exolve, 100%-ной "дочки" МТС, рынок Telecom API продолжает сохранять двузначные темпы роста. Он составляет около 25% в год - такую оценку дает генеральный директор МТС Exolve Рамиль Биккужин.

Среди основных драйверов рынка управляющий партнер "TMT консалтинга" Константин Анкилов называет стремление компаний к омниканальности и персонализации общения с клиентами, автоматизацию и роботизацию каналов общения, развитие средств защиты персональных данных, а также внедрение аналитических инструментов и речевых технологий на базе искусственного интеллекта (ИИ).

Нарастить функционал

По данным рейтинга провайдеров Telecom API, составленного CNewsMarket, в топ-3 российских провайдеров по функционалу, включая как базовые функции, так и продвинутые возможности сервиса с использованием инструментов ИИ, входят облачные платформы от МТС Exolve, Voximplant и "Телфин".

Telecom API прошла путь от предоставления базовых функций до создания полноценных экосистем, таких как CPaaS (Communication Platform-as-a-Service - коммуникационная платформа как услуга), рассказывает Биккужин. Эти платформы объединяют голосовые вызовы, SMS, мессенджеры, социальные сети и электронную почту, помогая бизнесу строить омниканальные стратегии и улучшать клиентский опыт, говорит он.

Так, летом 2025 г. МТС Exolve сообщила о запуске на своей платформе сервиса синтеза речи в режиме реального времени. Также ее функционал позволяет проверить базу контактов на актуальность и телекоммуникационную доступность - это нужно для того, чтобы обращаться исключительно к активным клиентам. А возможность распознавания автоответчиков и автоинформаторов снижает затраты на связь и позволяет избежать простоя операторов колл-центров.

Таким образом, бизнес получает единую точку входа для всего общения, объединяющую голос, SMS, мессенджеры, чаты и видео в одно пространство. Сервисы не просто обеспечивают коммуникацию, но и анализируют сам контекст общения, предоставляя выводы и рекомендации при помощи ИИ и роботизации. "Также выросли требования к аутентификации, безопасности в коммуникациях, расширяются сценарии применения Telecom API. В том числе этот сервис используется для идентификации и верификации пользователей", - сказала генеральный директор телекомкомпании "Телфин" Мария Тюрина.

Защитить данные

Одним из популярных сценариев использования Telecom API для бизнеса является защита персональных данных. Этот сценарий применяется, когда платформе нужно, например, связать водителя такси и пассажира или покупателя и продавца, но при этом не раскрыть их номера телефонов. Ритейлер Ozon использует эту технологию для организации взаимодействия специалистов курьерской службы с покупателями. За счет ее применения он смог сократить количество нецелевых звонков и повысить доверие пользователей к своей платформе, сообщала ранее компания.

Ритейлер "Магнит" применяет Telecom API от МТС Exolve для связи с соискателями в восьми регионах, в том числе в Москве, Волгограде и Санкт-Петербурге. Решение позволяет обеспечить конфиденциальность и быстрее обзванивать кандидатов. Они также могут самостоятельно перезвонить и автоматически через API связаться с нужным подразделением по найму. В результате внедрения коммуникационных сервисов компании удалось

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

сократить расходы на работу колл-центра на 18%, а эффективность взаимодействия с кандидатами повысить на 21%, указывала компания.

Внедрение системы речевой аналитики помогло клиентской поддержке "Атомэнерго" оперативнее выявлять запросы пользователей электрозарядных станций и максимально быстро на них отвечать. Все разговоры анализируются с помощью нейросети, а интеграция с CRM-системой предоставляет удобный инструмент для формирования отчетов и визуализации данных.

Таким образом, развитие Telecom API приводит бизнес к более комплексной модели общения - от использования отдельных услуг, например телефонных звонков и SMS, к применению коммуникационных экосистем, которые помогают вести с клиентом уважительный и персонализированный диалог, резюмирует Биккужин. (Ведомости 10.12.25)

К СОДЕРЖАНИЮ

информационное агентство information agency 199155 Санкт-Петербург пр. КИМа 28 +7-812-322-6848 +7-495-772-7640 mail@advis.ru

Прочие новости IT-компаний

"Базис" проводит IPO по верхней границе диапазона, объем сделки - 3 млрд рублей.

Цена размещения в рамках IPO ПАО "ГК "Базис" составила 109 рублей за акцию, сообщила компания.

Это соответствует верхней границе объявленного ранее ценового диапазона (103-109 рублей) и рыночной капитализации эмитента в 18 млрд рублей.

В рамках IPO миноритарии компании продают 27,52 млн акций, и, таким образом, базовый объем сделки составил, как и планировалось, 3 млрд рублей.

Сама компания средств не привлекает.

По результатам IPO продающие акционеры, которых "Базис" пока не назвал, сохранили участие в акционерном капитале группы. Миноритарии также передали 5% капитала "Базиса" под программу мотивации ключевых сотрудников и топ-менеджмента.

Согласно проспекту ценных бумаг, неназванным акционерам перед IPO принадлежало 26,7%, 8,1% и 5% акций "Базиса".

Мажоритарный акционер "Базиса" - РТК-ЦОД (контролируется ПАО "Ростелеком") - не продавал принадлежащие ему акции и сохранил свою долю в 50,3%, продолжит принимать участие в развитии бизнеса группы.

По итогам IPO free-float составит 16,7% от акционерного капитала.

"Базис" и основные акционеры берут на себя стандартное обязательство lock-up сроком на полгода. Также действует механизм стабилизации в размере около 10% от объема размещения (2,75 млн акций) на срок 30 дней после начала торгов. Агентом по стабилизации выступает ООО "ВТБ Капитал Трейдинг".

Торги акциями компании под тикером BAZA и ISIN RU000A10CTQ0 начнутся на "Московской бирже" 10 декабря, бумаги включены в котировальный список второго уровня.

Как говорится в сообщении, в структуре аллокации 39% пришлось на институциональных инвесторов, 61% - на розничных. Аллокация определялась независимо от брокера, через которого происходило участие в IPO, уточняет компания.

Средняя аллокация розничным инвесторам составила около 48% от размера заявки. Розничные инвесторы, подавшие более 10 заявок, не получили аллокации. Значения минимального и максимального размера аллокации для институциональных инвесторов не устанавливались.

IPO позволяет компании усилить мотивацию команды, повысить прозрачность корпоративного управления и расширить возможности для неорганического роста, приводятся в сообщении слова гендиректора "Базиса" Давида Мартиросова. "Наш фокус - импортоопережение и международная экспансия: мы видим значимый потенциал на рынках Латинской Америки и Африки, где востребованы надежные и конкурентоспособные технологические платформы", - сказал он.

"Первое в истории IPO компании группы "Ростелеком" - для нас знаковое событие. Публичный статус "Базиса" позволит рынку по достоинству оценить масштаб и качество его бизнеса, а также будет способствовать раскрытию справедливой стоимости "Ростелекома". Мы сохраняем долгосрочную приверженность этому активу, и уверены в его способности укреплять лидерство в сегменте инфраструктурного ПО", - отметил президент "Ростелекома" Михаил Осеевский.

"Базис" был образован в 2021 году за счет объединения активов "Ростелекома", ООО "КНС Групп" (Yadro) и "Рубитеха" (структура "ГС-Инвест"). Уставный капитал ПАО "ГК "Базис" составляет 165 млн рублей и состоит из 165 млн обыкновенных акций номиналом 1 рубль.

"Базис" - крупнейший разработчик ПО управления динамической инфраструктурой в России по итогам 2024 года, лидер в крупнейшем сегменте этого рынка - ПО виртуализации IT-инфраструктуры, включающий серверную виртуализацию и VDI. Также по результатам 2024 года группа являлась вторым крупнейшим игроком в сегменте ПО контейнеризации.

По итогам 9 месяцев 2025 года выручка ГК "Базис" по МСФО составила 3,5 млрд рублей, что на 57% больше, чем за аналогичный период 2024 года. Показатель OIBDA вырос на 42% - до 1,9 млрд рублей. Рентабельность по OIBDA снизилась до 54% с 59% годом ранее. Показатель OIBDAC (OIBDA, скорректированная на сумму капитализированных расходов) вырос на 40% - до 0,9 млрд рублей. Рентабельность по OIBDAC снизилась до 26% с 29%.

Чистая прибыль составила 1 млрд рублей, увеличившись на 35%. Показатель NIC (чистая прибыль за вычетом капитализированных расходов, увеличенная на величину расходов по программам долгосрочной мотивации и величину амортизации нематериальных активов) составил 0,9 млрд рублей, прибавив 42% г/г.

Для справки: Название компании: *ГК Базис, ПАО (ИНН 9722103241)* Адрес: *129085, Россия, Москва, ул. Годовикова, 9, ст. 17* Телефоны: *+74956456889* E-Mail: *info@basistech.ru; pr@basistech.ru* Web: *https://basistech.ru* Руководитель: *Мартиросов Давид Игоревич, генеральный директор* (Интерфакс 10.12.25)

К СОДЕРЖАНИЮ

Основатель "Лаборатории Касперского" Евгений Касперский не исключил продажу "Мойофиса".

Основатель "Лаборатории Касперского" Евгений Касперский не исключил возможность продажи разработчика офисного ПО "Мойофис" или привлечения в компанию нового совладельца.

"Если кто-то заинтересуется инвестициями в компанию, захочет стать соучредителем, совладельцем, - мы не исключаем, что рассмотрим такой вариант", - рассказал Касперский в интервью "Ведомостям".

По его словам, переговоры с потенциальными инвесторами ведутся периодически, однако до подписания меморандума дело пока не доходило.

Комментируя финансовые результаты "Мойофиса", Касперский указал на сокращение реального спроса на рынке. В 2021 г. выручка компании составляла около 841,8 млн руб., в 2022 г. выросла до примерно 3,4 млрд руб., а чистая прибыль достигла около 386 млн руб. В 2023 г. показатель снизился на 43,8% - до порядка 1,9 млрд руб. По итогам 2024 г. выручка увеличилась до 2,01 млрд руб., однако не вернулась к пиковым значениям 2022 г.

По словам Касперского, несмотря на уход международных компаний, многие клиенты продолжают использовать их продукты, часто бесплатно, либо переходят на опенсорс-решения. При этом функциональность "Мойофиса", по его оценке, пока уступает продуктам Microsoft, но развивается быстрыми темпами.

"Нам нужен нормальный отечественный софт, отечественный офисный пакет. Все остальное, что есть на рынке, - чистый опенсорс. А это небезопасно", - подчеркнул он. По его словам, в 2022 г. из-за роста числа уязвимостей в опенсорс-пакетах был создан специальный сервис для их выявления, в базе которого сейчас содержится информация примерно о 22 000 зараженных пакетах.

Для справки: Название компании: *Лаборатория Касперского, АО* Адрес: *125212, Россия, Москва, Ленинградское шоссе, 39, литера А, стр.3, БЦ «Олимпия Парк»* Телефоны: *+74957978700* Факсы: *+74957978709* E-Mail: *info@kaspersky.com* Web: *https://www.kaspersky.ru/* Руководитель: *Касперский Евгений Валентинович, генеральный директор* (Ведомости 15.12.25)

К СОДЕРЖАНИЮ

Цифровизация в странах СНГ

На заводе "СарыаркаАвтоПром" запущен пилотный ИИ-проект по реагированию на инциденты безопасности (Казахстан).

На крупные промышленные предприятия Казахстана активно внедряют технологии искусственного интеллекта. 25 сентября в Astana Hub прошел Demo Day, организованный QazIndustry при поддержке Министерства промышленности и строительства Республики Казахстан. В ходе мероприятия была утверждена Дорожная карта по внедрению практических решений искусственного интеллекта в производственные процессы крупных предприятий на 2025-2026 годы.

Карта уже демонстрирует свои результаты. Например, на автомобильном заводе ТОО "СарыаркаАвтоПром", входящем в состав группы компаний Allur, запущен пилотный ИИ-проект - оперативный центр реагирования на инциденты безопасности. Современная интеллектуальная платформа анализирует данные с камер, датчиков и IT-систем, что позволяет мгновенно выявлять и фиксировать производственные риски, аварийные ситуации, аномалии в работе оборудования и оперативно устранять их.

"Искусственный интеллект обрабатывает данные в реальном времени. При выявлении отклонений в поведении персонала и работе механизмов система отправляет сигнал о нарушении и запускает процедуру реагирования", - пояснил исполнительный директор ТОО "СарыаркаАвтоПром" Аргулан Майконов.

К примеру, система незамедлительно реагирует на задымления, открытое пламя, падение груза, движение техники вблизи персонала, протечки жидкостей, а также на отсутствие у работников защитных касок и жилетов, остановку оборудования, падение давления воздуха, скопление людей, превышение скорости транспортом, загромождение проходов, аномальные климатические условия.

Помимо этого, на заводе внедрен ряд умных решений, чтобы сделать процессы прозрачными, управляемыми и предсказуемыми.

К примеру, система ERP объединила производство, закупки, склад, финансы и управление персоналом.

С помощью MES (Manufacturing Execution System) управляют производственными операциями в режиме реального времени: принимает и распределяет заказы по цехам и отслеживают этапы производства.

QLS (Quality Leadership System) занимается проверкой качества материалов на входе, фиксирует брак, анализирует его причины и принимает корректирующие меры.

WMS (Warehouse Management System), или "умный" склад, ведет автоматический прием и размещение товаров, онлайн-учет остатков и занимается комплектацией заказов и маршрутов погрузки.

Качество продукции автомобильных заводов играет огромную, критически важную роль, ведь речь идет о безопасности людей - водителей, пассажиров, пешеходов. Для обеспечения контроля качества Allur внедрил Hexagon Toro Performance - лазерное и оптическое 3D-сканирование кузовов и автоматический диагностический комплекс, который проверяет все системы автомобиля перед отгрузкой.

Также на предприятии задействовано более 24 промышленных роботов. Они помогают в сборке, окраске, сварке и подготовке кузовов автомобилей.

Внедрение технологий искусственного интеллекта в работу предприятий в рамках Дорожной карты стало стратегическим решением, направленным на оптимизацию, автоматизацию и повышение эффективности производственных процессов. Теперь контроль всех ключевых процессов происходит в режиме онлайн, сокращены простои и браки, повышена скорость и точность производства, улучшены условия труда, повышена безопасность.

Отметим, в разработке Дорожной карты приняли участие такие ведущие промышленные предприятия страны, как "Allur", "Казахмыс", "Казфосфат", "Qarmet", "Казцинк", "ERG", "АК "Алтыналмас", группа "KAZ Minerals", "Solidcore Eurasia", "Кайнар-АКБ" и "Astana Motors Manufacturing Kazakhstan". Участие столь значимых компаний обеспечило комплексный охват отраслей и позволило создать практическую платформу для системного внедрения современных цифровых решений.

Карта объединяет 41 проект по внедрению ИИ на 11 крупных промышленных предприятиях. В перечень технологий входят компьютерное зрение, предиктивная аналитика, роботизированная техника, беспилотный транспорт, цифровые двойники, Big Data, генеративные ИИ-ассистенты. Такой широкий спектр направлений демонстрирует стратегический подход к цифровой трансформации, направленной на повышение производительности, безопасности и инновационного потенциала предприятий.

Для справки: Название компании: *СарыаркаАвтоПром, ТОО* Адрес: *110006, Республика Казахстан, Костанай, ул. Промышленная, 41* Телефоны: *+77142391001; +7(7142)391002; +7(7142)391003* E-Mail: *marketing.sap@list.ru; inform@sap.kz; akhmedova.ds@sap.amh.kz* Web: *http://sap.com.kz* Руководитель: *Семейбаев Сырым Сайранбекулы, директор* (Министерство промышленности и строительства Республики Казахстан 09.12.25)

Предприятия России и Беларуси заменяют на тяжелых производствах людей роботами. "Российская газета". 10 декабря 2025

Российские и белорусские предприятия переживают новую индустриальную революцию, связанную с активным внедрением роботизированных технологий. Автоматизация производства становится способом повысить конкурентные преимущества и производительность труда.

Россия и Беларусь ставят перед собой схожие планы по роботизации производств. "Президент РФ Владимир Владимирович Путин в 2024 году в ходе послания Федеральному собранию поставил цель: к 2030 году по числу промышленных роботов Россия должна войти в число 25 ведущих стран мира", - напоминает доцент Финансового университета при Правительстве РФ Петр Щербаченко. Это означает, что количество роботов в экономике должно составить 145 единиц на 10 тысяч человек, на предприятиях с госучастием на то же количество сотрудников количество роботизированной техники должно составить не менее 230 единиц.

В Беларуси также запланирована масштабная модернизация и роботизация производств. Правительство поставило задачу к 2040 году достичь среднемирового уровня роботизации в промышленности. Это означает, что на 10 тысяч работников должно быть около 150 роботов. Причем в приоритете роботы, произведенные на территории Беларуси.

Схожие планы по роботизации производств рождают и совместные инициативы. Так, этим летом премьер-министр Беларуси Александр Турчин на выставке "Иннопром. Беларусь" предложил создать России и Беларуси "союзного промышленного робота" в рамках совместной программы.

В 2025 году спрос на внедрение роботизированных систем растет как среди крупных предприятий, так и среди малого и среднего бизнеса - особенно в отраслях машиностроения, металлообработки, энергетического машиностроения, пищевой промышленности, электроники и логистики, отмечает Павел Сучков, первый заместитель генерального директора АНО "Центр промышленной роботизации".

"Если оглянуться на последние два-три года, интерес к роботизированным системам в России стал куда более предметным. Это уже не эксперимент крупных корпораций, а прагматичный запрос самых разных производств, - считает Андрей Тян, генеральный директор компании "Аметист Логистика". - Предприятия приходят к роботизации не из моды, а из необходимости закрыть дефицит квалифицированных кадров, повысить стабильность процессов и снизить издержки за счет цифровой управляемости".

Сегодня российские предприятия выпускают промышленных роботов, которые сильнее и быстрее людей. И могут работать в условиях, которые для людей опасны. А значит, их использование способно сберечь человеческие жизни. Большой вес - около 120 килограмм - поднимают челябинские промышленные машины. А одна из моделей уральского "Завода Роботов" умеет работать с заготовками температурой до 1300 °С, что позволяет автоматизировать производственные операции в машиностроительных и металлургических производствах, рассказывает Петр Щербаченко. Компании роботизируют сварочные цеха. Например, на одном из автомобильных производств сварочная ячейка позволила сократить такт сварки с 75 до 57 секунд и высвободила трех специалистов для более сложных задач, где без участия человека не обойтись. Экономический эффект составил около 15 млн руб. за три года. О сходных результатах внедрения автоматизированной сварки говорят и на других предприятиях, многие из них сегодня устанавливают второй-третий роботизированный сварочный комплекс.

На уже действующих предприятиях зачастую автоматизируют сварочные, сборочные, покрасочные, упаковочные и логистические процессы. Однако наиболее эффективна роботизация, если она заложена на стадии проектирования предприятия.

Внедрение роботизированных систем требует аудита действующих производств. Специалисты помогают провести анализ производственных процессов, выявить те участки, которые могут быть автоматизированы, рассчитать выгоды от внедрения роботизации. В рамках нацпроекта "Средства производства и автоматизации", который курирует Минпромторг России, до конца 2030 года Федеральный центр компетенций проведет диагностику и предложит решения по роботизации 1,5 тысячи российских компаний, сообщили "СОЮЗу" в центре.

Работа ведется и на уровне региональных центров. Кроме того, российские специалисты выходят на международный уровень. Так, специалисты из Челябинской области наладили сотрудничество с белорусской свободной экономической зоной "Могилев". Идею привлечь специалистов АНО "Центр промышленной роботизации" для проведения технологических аудитов на предприятиях союзного государства предложил в ходе визита в Беларусь губернатор Челябинской области Алексей Текслер. В ближайшее время будут проведены два экспресс-аудита на предприятиях свободной экономической зоны (Завод горного машиностроения и "Могилевлифтмаш"), по итогам которых определят точки роботизации, подготовят дорожные карты внедрения роботов.

Сегодня технологии позволяют создавать так называемые темные фабрики - полностью автоматизированные производства с минимальным участием людей. Пример таких решений есть и в Беларуси, и в России. В Минске в холдинге "Горизонт" заработал безлюдный завод, где основную работу выполняют роботы. Предприятие выпускает бытовую технику и электронику. В России "темными" могут стать производства с опасными для людей условиями

труда, в том числе атомные объекты. Соответствующие проекты сейчас находятся в стадии разработки. (Российская газета 10.12.25)

К СОДЕРЖАНИЮ