



Хождение за три чипа

Технологические санкции 2022 года сначала ввергли в шок российских производителей электроники, которых лишили возможности сотрудничать с зарубежными партнерами в части производства и разработки компонентов, а затем заставили их искать партнеров в дружественных странах. В первом квартале текущего года ряд крупных российских производителей электроники, разработчиков микроэлектроники, вендоров программного обеспечения, а также отраслевые ассоциации совершили несколько деловых поездок в Индию в поисках возможностей развития. „Ъ“ разбирался в том, чем индийский рынок привлекает российские IT-компании.

— сотрудничество —

Растущий и амбициозный

Международные аналитические агентства видят индийский IT-рынок перспективным и имеющим большой потенциал роста. Так, согласно прогнозу Gartner от ноября 2022 года, расходы индийских компаний и госсектора на цифровизацию в 2023 году вырастут на 2,6% год к году, до \$112 млрд, устойчивый рост в этом сегменте продолжается как минимум последние три года. Аналитики Gartner предполагают, что наиболее существенный рост будет в сегменте программного обеспечения (+13% год к году, до \$13,35 млрд) и сегменте IT-услуг (+7,1% год к году, до \$22 млрд). Причиной роста рынка аналитики видят интерес индийских предприятий и госсектора к цифровизации производств и жилищно-коммунального хозяйства.

Международные аналитические агентства позитивно оценивают не только софтверный, но и полупроводниковый рынок Индии. Так, согласно февральскому отчету Deloitte, к 2026 году объем индийского рынка полупроводников составит \$55 млрд, при этом 60% рынка будет приходиться на три сегмента: компоненты для смартфонов, носимых устройств и автоэлектронику (по итогам 2021 года MMR оценивал объем индийского рынка полупроводников в \$21,75 млрд). В прогнозах на 2030 год Deloitte идет еще дальше, оценивая потенциальный объем рынка полупроводников к этому времени в \$85 млрд.

Индия — одна из самых быстро развивающихся экономик мира. Размеры территории и численность населения этой страны требуют массового внедрения IT-услуг, среди которых банковские услуги, услуги доставки товаров, технологии «умного города» и другие, добавляют в Минцифры. В министерстве подчеркивают, что перспективы сотрудничества с Индией связаны с совместными разработками и созданием российско-индийских компаний, производящих компоненты и платформенные IT-решения для применения в Индии и поставок в другие страны.

Полупроводниковые грезы

В декабре 2021 года правительство Индии одобрило программу Semicon India, которая ставит целью развитие производств в стране дисплеев и микроэлектроники. Про-

грамма предполагает, что правительство Индии предоставит 50-процентную субсидию от стоимости проектов, бюджет программы составил примерно \$10 млрд.

Уже в феврале 2022-го Министерство электроники и информационных технологий Индии сообщило, что получило пять заявок в рамках этой программы общей стоимостью около \$20 млрд. Три из них (от CIP Vedanta и Foxconn, IGSS ventures pte и ISMC) предполагают строительство полупроводниковых фабрик для выпуска микроэлектроники по технологическим нормам от 28 до 65 нм и общей производственной мощностью до 120 тыс. кремниевых пластин в месяц. Совокупный объем инвестиций в проекты составит приблизительно \$13,6 млрд. Компании Vedanta и Elest, следует из сообщения правительства, подали заявки на строительство фабрик по выпуску дисплеев с совокупным объемом инвестиций \$6,7 млрд.

Судя по публичным заявлениям официальных лиц Индии, планы развития полупроводникового сектора не ограничиваются строительством заводов на территории страны, а также подразумевают создание индустрии, которая в дальнейшем исключит риски нарушений цепочек поставок, наблюдавшихся в 2020–2022 годах во время пандемии.

Летом 2022 года глава ассоциации «Индия—Тайбэй» Гурангалал Дас в интервью Nikkei говорил, что совокупно власти Индии хотят направить до \$30 млрд на перезапуск своей технологической индустрии и выстраивание цепочек поставок чипов. «Нам нужны некоторые гарантии, что наш спрос на полупроводники не окажется в заложниках нестабильности цепочек поставок, что мы иногда видели во время пандемии», — сказал в интервью господин Дас. Он также отмечал, что к 2030 году на Индию будет приходиться более 10% всего мирового спроса на полупроводники, что оценивается в \$110 млрд.

Нынешней весной Индия вновь активизировала усилия по привлечению инвестиций в полупроводниковый сектор. 10 мая агентство Bloomberg со ссылкой на источники сообщило, что правительство Индии планирует провести еще один раунд подачи заявок на получение субсидии, чтобы израсходовать до конца \$10 млрд, заложенных на финансирование программы. «Но сейчас полупроводниковых производств в Ин-



дии нет, и не факт, что они появятся в ближайшее время. Так что в этой части сотрудничать пока негде», — подчеркивает топ-менеджер российского производителя микроэлектроники.

У Индии действительно большие амбиции по запуску полупроводниковых производств в стране, но они буксуют, утверждает топ-менеджер российской IT-компании: «Плюс нужно понимать, что Индия — крайне бюрократизированная страна и большие проекты там в любом случае будут буксовать».

К проектированию чипов ищут подход

Но даже при отсутствии возможности производства в Индии микроэлектроники одним из потенциальных вариантов для кооперации может стать сотрудничество российских и индийских дизайн-центров (по данным Invest India, в стране их насчитывается 1,14 тыс.), говорят опрошенные „Ъ“ профильные ассоциации.

В «АКРП — Консорциум дизайн-центров» (в него входят 73 производителя и разработчика электроники, в том числе «Микран», «Элвис», «Миландр» и т. д.), „Ъ“ сказали, что уже видят взаимный интерес российских и индийских разработчиков микроэлектроники к кооперации. «По нашим данным, такой взаимный интерес однозначно есть. Позитивный момент в том, что многие контакты были установлены и развиваются уже давно», — уточняют в АКРП.

«Мы пытаемся выйти на индийский рынок, ищем точки соприкосновения с местными компаниями. Наиболее перспективным мы видим проектирование приборов учета электроэнергии. У российских компаний есть опыт в разработке таких приборов, а у индийских — потребность в их выпуске», — говорит топ-менеджер российского разработчика электроники. По его словам, компания сейчас работает над «трансфером технологий» совместно с индийскими партнерами.

Потенциально, говорит собеседник, это может быть организация совместного предприятия, в котором российские компании помогают проектировать компоненты и конечные изделия, а индийские — обеспечивают их производство на мощностях местных заводов. По его словам, индийским центрам проектирования электроники и микроэлектроники «не хватает опыта разработки всего продукта от начала и до конца».

В Индии большой объем разработок предназначен для американских корпораций: Intel, Qualcomm и т. д. Это десятки тысяч высококвалифицированных специалистов, отмечают исполнительный директор Ассоциации российских разработчиков и производителей электроники (АРПЭ) Иван Покровский: «Но при этом в стране практически нет дизайн-центров микроэлектроники, разрабатывающих собственные решения».

В России, напротив, накоплен большой опыт проектирования собственной электроники и микроэлектроники, говорит эксперт: «И индийская сторона проявляет большой интерес к запуску совместных проектов. Наиболее интересны проекты, в рамках которых производство российских разработок было бы локализовано в Индии, и стороны совместно инвестируют в развитие технологий».

Однако топ-менеджер российского разработчика электроники настаивает, что при сотрудничестве, подразумевающем создание СП с индийским партнером, нельзя говорить о перспективах экспорта российских решений. «Индийские инвесторы, без условно, рады сотрудничеству с российскими компаниями, у которых есть готовый продукт, особенно если мы говорим про интернет вещей. Но такое сотрудничество предполагает передачу в СП прав на интеллектуальную собственность», — объясняет он. В таком случае, добавляет собеседник, российские компании совершают трансфер технологий, выгода от которого в дальнейшем неочевидна.

Топ-менеджер российского разработчика микроэлектроники также смотрит на планы кооперации российских и индийских дизайн-центров скептически, называя перспективой подобного сотрудничества не такими радужными для российских компаний: «Индийским дизайн-центрам такой опыт просто не зачем — они хорошо работают в качестве аутсорс-разработчиков».

Ряд российских дизайн-центров действительно предлагал индийским компаниям свои услуги как в части продажи собственных IP-блоков, так и в части кооперации при проектировании микроэлектроники, говорит топ-менеджер крупной российской IT-компании. По его словам, в этом был заинтересован МЦСТ (разрабатывает процессоры линейки «Эльбрус»): «Но вопрос в том, насколько самим индийцам это необходимо. Зачем им наработка условий МЦСТ, учитывая, что экосистема вокруг „Эльбрусов“ развита слабо. Да и в целом предполагать, что индийским компаниям нужна помощь дизайн-центров, — смешно». В самом МЦСТ от комментариев отказались, в «Байкал Электроникс» (проектирует процессоры Baikal) не ответили.

Софт с местным колоритом

Пока представители наших дизайн-центров спорят о перспективах разработок совместно с индийскими партнерами, российские разработчики ПО уже сегодня видят индийский рынок однозначно перспективным с точки зрения экспорта российских решений. Интерес к российским IT-решениям резко обострился в Индии после начала СВО и санкционной кампании против России в США и ЕС, говорит президент «Руссофта» Валентин Макаров.

В марте ассоциации «Руссофт» (объединяет разработчиков ПО) и АРПЭ (объединяет разработчиков и производителей компонентов) организовали бизнес-миссию в Ин-

дию, рассказывает Валентин Макаров. «Наши компании приняли участие в выставке IndiaSoft, в российско-индийском деловом форуме „Сотрудничество во имя развития и роста“, где мы подписали соглашение о сотрудничестве с ассоциацией RISING», — рассказывает господин Макаров, добавляя, что после окончания миссии члены организации поддерживают «углубленные контакты с теми индийскими компаниями, бизнес-результатов этих переговоров можно ожидать на горизонте трех-шести месяцев».

Опрошенные „Ъ“ разработчики софта отмечают, что наибольший интерес у индийских заказчиков как из частного, так и из госсекторов вызывают решения, позволяющие обеспечить технологическую и информационную независимость. «Это решения в области кибербезопасности, компьютерного зрения, Data Science, искусственного интеллекта», — говорит глава направления мобильной разработки компании SimbirSoft Ринат Шамшутдинов. Стремление к независимости и автономии от санкционных IT-решений подстегнуло спрос, в том числе на российские продукты за рубежом, добавляет директор по развитию TrueConf Дмитрий Одинцов.

Интерес к российскому ПО проявляют индийские промышленные предприятия, в частности компании горнорудной отрасли, говорит директор департамента горнодобывающих решений «Рексофта» Дмитрий Карамышев: «Горнодобывающая промышленность Индии развивается высокими темпами. Это значит, что в отрасли будут вовлекать все больше кадров и ресурсов, которым будет необходимо повышать эффективность бизнеса. Сейчас горнодобывающий сегмент в Индии только выпускает первые зарубежные IT-компании и делает шаги в промышленной автоматизации».

Впрочем, не все российские IT-компании видят выход на индийский рынок простым. В стране «довольно плотно и эффективно» работают практически все глобальные IT-вендоры, и прямые иностранные инвестиции в ПО и оборудование по своим объемам занимают лидирующие позиции, одновременно с этим каждый год число внутренних стартапов серьезно растет, перечисляет глава дирекции внедрения и сопровождения ГК «Астра» Ярослав Богомолов: «Поэтому любой российский производитель в Индии столкнется с очень высоким уровнем конкуренции. Более того, несмотря на численность 1,4 млрд человек, в стране присутствует серьезное финансовое расслоение, что значительно сужает круг платежеспособного населения».

Он добавляет, что индийцы в подавляющем большинстве случаев ориентированы только на долгосрочное сотрудничество, поэтому рассматривают проекты с реализацией в перспективе пяти лет и больше: «Однозначно выход на данный рынок требует серьезной проработки как с точки зрения бизнес-стратегии, так и адаптации продуктов под его специфику».

Никита Королев

Оборудование ждет помощи

— инфраструктура —

В России вырос спрос на партнерскую поддержку (аутсорсинг) собственного IT-оборудования компаний на фоне ухода западных производителей (Nokia, Ericsson, SAP), которые ранее оказывали вендорскую поддержку вычислительной техники. Для сохранения и поддержки парка уже закупленного оборудования российские организации привлекают интеграторов, у которых есть компетенции и возможность закупить необходимые для ремонта комплектующие. Это приводит как к росту цен на IT-аутсорсинг, так и к появлению на рынке новых участников.

Отказ в обслуживании

По данным IT-интегратора «Крок», после ухода из России иностранных вендоров почти 70% компаний столкнулись с проблемами при обслуживании IT-систем. И в первую очередь это отразилось на работе парков оборудования, которые бы-

ли зависими от поддержки зарубежных производителей. Их отказ от обслуживания и останова контрактов с российскими фирмами стали драйвером роста спроса на услуги IT-аутсорсинга (установка, поддержка, техобслуживание).

Основная динамика увеличения числа заказов на услуги сервисной поддержки и аутсорсинга пришлась на прошлый год, добавляют в «Кроке». Бизнесу, который раньше пользовался услугами международных компаний, было необходимо в сжатые сроки найти нового партнера, способного быстро перевести на себя весь объем требуемых услуг без потери качества. В текущем году темпы роста сохраняются. Востребованность услуг сервиса и аутсорсинга растет пропорционально потребностям заказчиков, прогнозируют аналитики.

Наибольшим спросом в России сейчас пользуются услуги по обслуживанию телекоммуникационного и промышленного IT-оборудования, центров обработки данных (ЦОД) и другой специализированной вы-

числительной техники, рассказывает собеседник „Ъ“ (см. „Ъ“ от 22 апреля). Большую часть этого рынка занимали зарубежные производители оборудования: Nokia, Ericsson, SAP, Siemens, ABB, GE и другие.

Уход компаний в прошлом году не означал полного отключения уже закупленного оборудования. Некоторые вендоры частично сохранили поддержку или передали этот функционал локальным юристам, которые остались на рынке. По словам директора по сервису ESA PRO Михаила Назарова, если оборудование использовалось соответствующим образом и регулярно поддерживалось, то его срок службы может быть продлен до пяти-семи лет: «Однако любое оборудование со временем становится устаревшим и нуждается в замене».

Некоторые виды оборудования можно поддерживать бесконечно, заменяя части и обновляя ПО, соглашается руководитель направления «Системная интеграция» MONS (входит в ГК «КОРУС Консалтинг») Владислав Бахаудинов. В среднем

оборудование используется от трех до десяти лет, уточняет он.

Наиболее зависимыми от бесперебойной работы оборудования ожидаемо стали компании, которые активно занимались цифровизацией как внутренних процессов, так и оказания услуг клиентам. По оценке «Рексофта», в их числе представители финансовой, телекоммуникационной отраслей, а также промышленных производств, где возможные издержки и риски от прекращения работоспособности предприятий ведут к прямым финансовым потерям и риску возникновения техногенных катастроф. На компании этих отраслей и приходится наибольший рост спроса на IT-аутсорсинг парков оборудования, говорит директор по развитию бизнеса группы «Рексофт» Дмитрий Ретюнский.

Услуги IT-аутсорсинга подходят как небольшим компаниям, так и крупным корпорациям, считает заместитель генерального директора «Сервионики» Артем Спинул: «Чем крупнее компания и критичнее стабильная работа ее IT-инфраструкту-

ры, тем выше требования к экспертизе и опыту сервисной компании».

Но применимость услуг аутсорсинга зависит от типа технологических платформ организации, объясняет господин Спинул: «Внешний IT-сервис актуален для компаний, использующих решения среднего класса (mid-range), но еще более критичен сервисный партнер для бизнеса, связанного со сложными технологическими цепочками, высоконагруженными системами, аппаратными платформами уровня enterprise». Для поддержки таких решений, говорит эксперт, необходимы не только высокая экспертиза и квалификация IT-специалистов, но и налаженные цепочки поставок запасных частей и встроенного программного обеспечения (ПО) для зарубежного оборудования. «Моментальный переход на российские аналоги невозможен в существующих условиях, но переход на них обязательно должен быть предусмотрен в стратегиях компаний», — добавляет господин Спинул.

IT-ландшафт крупных корпораций представляет собой совокуп-

ность технических сложных, взаимосвязанных информационных систем, и многие из них являются бизнес-критичными, говорит директор управления реализации сервисов Softline Алексей Филиппук: «В связи с этим любого рода миграции, в том числе на отечественное оборудование, могут рассматриваться только при наличии четкого плана, в котором одним из важнейших является вопрос технической поддержки как самого мероприятия, так и формируемой целевой архитектуры».

Ситуация на рынке заставляет участников пересматривать отношение к стратегии потребления услуг. «Например, у компании остался обширный парк программно-аппаратной инфраструктуры, но требует развития, поддержки со стороны производителей и экспертизы в области эксплуатации. Передача этого направления на IT-аутсорсинг помогает заказчикам сосредоточиться на ключевых бизнес-задачах и оптимизации вспомогательных направлений», — объясняет господин Филиппук.

информационные технологии



«Главный принцип — иметь четкое понимание того, что и от кого мы защищаем»

Прошлый год стал зоной турбулентности для российского IT-рынка: если ранее он развивался по аналогии с глобальным, ориентируясь на мировые тренды и технологии, то события 2022 года холодным душем смыли все прошлые ориентиры. IT-директорам пришлось в экстренном порядке выстраивать процессы в новых условиях, не полагаясь на зарубежных вендоров, учитывая рост цен на оборудование и снижение числа кадров. В 2023 году перестройка процессов продолжается, рассказал „Ъ“ директор по сервису «Кросс технологжис» **Михаил Назаров**: если ранее в приоритете была скорость решения проблем, обеспечивающая выживание бизнеса в новых условиях, то теперь пришло время пересмотреть стратегии и исправить недоработки.

— мнение —

Из-за сбоев цепочек поставок усилился дефицит оборудования, его стоимость выросла — так, например, стоимость услуг по IT-аутсорсингу оборудования в 2023 году выросла на 15–40%, писал „Ъ“ 22 апреля. Тотальные запретительные меры и ограничения доступа к интернету привели к удорожанию систем информационной безопасности и увеличению затрат на нее. Многие инструменты киберзащиты подорожали более чем на 40%. Например, из-за проблем с логистикой и компонентной базой подорожали такие аппаратные средства защиты, как криптошлюзы (ПО, шифрующее трафик) и firewall (межсетевой экран, обеспечивающий защиту IT-периметров).

Такую ситуацию многие молодые специалисты восприняли в штыки, поэтому число человеческих ресурсов стало стремительно сокращаться. В 2023 году спрос на IT-кадры увеличился на 63%, а срок поиска кандидатов вырос в два раза, писал „Ъ“ 21 апреля. Требования к квалификации специалистов также изменились — так, в кибербезопасности стали менее востребованы специалисты по законодательству и методологиям. «Бумажный» firewall не защитит от реальных кибератак, число которых в прошлом году выросло: в октябре 2022 года вице-премьер РФ Дмитрий Чернышенко докладывал президенту о росте атак на 80%.

В компаниях растет спрос на инженеров, которых на рынке всегда было немного. Причиной нехватки кадров стал не только отъезд многих IT-специалистов, но и рост спроса на отечественные решения. Внедрение отечественного софта и Open Source-решений требует большого количества разработчиков в стране. Волшебной палочки для решения этих проблем нет, и было бы излишне оптимистично утверждать, что кому-то удалось окончательно с ними справиться. Я вижу три основных направления, которые помогают IT-директорам.

Во-первых, это использование квалифицированно-го аутсоринга для восполнения недостатка кадров и закрытия пика по нагрузкам на своих сотрудников. Экономить на персонале позволяло облачные сервисы: согласно прогнозу Gartner, к 2026 году 75% организаций перейдут на модель цифровой трансформации, в которой облако является фундаментальной базовой платформой.

Во-вторых, сегодня особенно важна тотальная пропаганда «цифровой гигиены» в компании. Персонал — это, как правило, самое слабое звено, через которое можно проникнуть в инфраструктуру организации. Поэтому нужно доносить важность кибербезопасности до каждого сотрудника, проводить постоянные тестирования. Например, можно поддерживать бдительность с помощью тестовых фишинговых рассылок, при которых IT-департамент отправляет сотрудникам электронные письма, имитирующие фейковые рассылки мошенников. Те сотрудники, которые перейдут по ссылке из письма или откроют вложенный файл, должны будут пройти дополнительное обучение по мерам цифровой гигиены.

Кроме того, компания может справиться с нехваткой специалистов путем повышения квалификации уже имеющихся сотрудников. Инвестирование в обучение сотрудников — глобальный тренд. IDC в прогнозе для мировой IT-отрасли на 2023 год отмечал, что «большинству компаний будет трудно удержать и найти специалистов с нужными навыками. Компаниям и поставщикам IT нужно будет инвестировать в развитие требуемых навыков использования IT».

Наконец, более актуальным становится использование комплексных решений от одного поставщика. В сфере кибербезопасности стоит обратить внимание на комплексные предложения вендоров — например, у «Лаборатории Касперского» есть защитные решения для бизнеса, которые можно подобрать в зависимости от потребностей и бюджета.

При комплексном подходе к защите компания тратит намного меньше усилий на поддержание взаимной интеграции систем. Внедрение таких решений не настолько трудозатратно, как переход на Open Source-решения, и позволяет избежать появления зоопарка технологий. Да и принцип «одного окна», при котором за поддержку по всем вопросам отвечает один вендор, всегда удобен. Кроме того, обучение сотрудников работе в новых программах проходит проще и быстрее благодаря меньшему количеству итераций и однородности логики интерфейсов.

Главный принцип при создании экосистемы безопасности — иметь четкое понимание того, что и от кого мы защищаем. Важно определить, актуальны вам только обычные угрозы или еще и скрытые и какие сложные атаки могут произойти. Далее начинаем выстраивать за-



щитную систему, определив базу: с защитой от обычных угроз справится IT-отдел компании, при появлении рисков скрытых угроз может потребоваться команда кибербезопасности, а в случае с защитой от сложных атак стоит говорить о создании службы ИБ или центра мониторинга и реагирования на инциденты. Таким образом мы создаем стержень системы, на который будут нанизаны дальнейшие защитные продукты. Набор продуктов может варьироваться в зависимости от размера и типа компании, ее бизнес-процессов, важности ее данных и других факторов. Как правило, комплексные решения уже включают все необходимое для компаний того или иного типа. На таком подходе основаны защитные решения «Лаборатории Касперского».

Например, для небольших организаций, которые только начинают выстраивать цифровые процессы, пока не обладают собственной экспертизой в вопросах безопасности и существенным бюджетом на эти задачи, подойдет «Kaspersky Endpoint Security для бизнеса Стандартный». Продукты, включенные в этот уровень, позволяют защитить бизнес от массовых киберугроз, которые составляют до 90% от всех атак на компании. В решение включена защита, в том числе от бесфайловых вирусов, которые наиболее сложно выявить и заблокировать. Например, в 2022 году был обнаружен бесфайловый троян, который «прячется» в журналах событий Windows. Всеми продуктами можно управлять из единой консоли, что позволяет упростить процесс контроля.

Безопасное извлечение клиентов

— конъюнктура —

Спустя более года после того, как Microsoft объявила об остановке продаж в России, клиенты розничных магазинов и корпоративные заказчики свыкаются с новыми способами покупки ее продуктов. Источники „Ъ“ и представители крупного бизнеса говорят, что на рынке нет прямых замен Microsoft Exchange, а продление существующих лицензий в отсутствие поддержки не имеет смысла. При этом они утверждают, что в большинстве случаев российские компании справляются с услугами вендорской поддержки.

Решение Microsoft о сокращении деятельности в РФ вследствие военной операции на Украине выдвинулось даже на фоне прочих подобных заявлений, сделанных в 2022 году. Компания, представившая локализованное системное ПО на территории России еще во времена Советского Союза, впоследствии стала предлагать программы и услуги в самых разных категориях: от облачных технологий до видеопир.

Microsoft, как говорил в июне 2022 года ее президент Брэд Смит, планировала сокращать присутствие в России до тех пор, пока от него «совсем ничего не останется». Сокращение штата российских юристов Microsoft до одного-двух человек уже нашло отражение в опубликованных в апреле бухгалтерских отчетности. „Ъ“ оценил, как решение компании оставить бизнес в стране сказало на тех сегментах рынка, где она представлена.

Ключик повернулся

Прямые продажи потребительного ПО и сервисов Microsoft были сокращены еще до полномасштабных военных действий. В 2018 году компания перестала продавать на своем сайте цифровые копии Windows 10 и подписки на Office — последнее компания объясняла решением «переориентировать продажи Office на розничных партнеров», а также отключила рублевые платежи в цифровом магазине Microsoft Store. Microsoft также не продавала в России компьютеры под собственным брендом Surface, за исключением первого поколения планшетов в 2013 году.



Остановка деятельности Microsoft в России привела к тому, что в течение 2022 года коды активации Windows и Office были практически недоступны в крупных розничных сетях и магазинах. Ключи периодически появлялись в специализированных магазинах, но те уточняли, что речь идет о складских запасах (см. „Ъ“ от 9 ноября 2022 года). С тех пор некоторые магазины наладили поставки — так, «М.Видео» стал продавать подписки и коды активации офисного и системного ПО от Microsoft в комплекте с подпиской на публичный VPN-сервис. К моменту появления этих предложений крупные ритейлеры уже объединяли аналогичным образом коды пополнения цифровых кошельков в одну позицию с сервисными пакетами (см. „Ъ“ от 8 ноября 2022 года).

О каких-либо ограничениях активации программ от Microsoft в России или получении регулярных обновлений не сообщалось. При этом Microsoft закрыла доступ из России к средствам создания установочных носителей Windows 10 и 11, размещенных на ее сайте. Эксперт по кибербезопасности «Лаборатории Касперского» допускает, что в связи с блокировкой в перспективе может вырасти количество вредоносного ПО, маскирующегося под средства установки Windows: «Злоумышленники постоянно используют актуальные темы, связанные с различными ситуациями в мире, для реализации своих атак».

Крупные российские сборщики компьютеров закупили предназначенные для них лицензии напрямую у Microsoft, говорит источник „Ъ“ на рынке дистрибуции. Речь идет о лицензиях канала ODR (OEM Distribution & Reseller) — их можно использовать только для установки производителем ПК и нельзя перепродавать: «Такие же лицензии есть и в Китае, они предназначены для китайских производителей. Если Microsoft увидит использование таких лицензий не по назначению и в другой стране, то в теории может заблокировать все неактивированные лицензии». Раньше Microsoft продавала в России OEM-лицензии, которые могли быть активированы хоть через десять лет хранения, сейчас же на рынке появились лицензии с ограничениями по времени, говорит он.

Поддержки мою инфраструктуру Microsoft запретила покупку новых корпоративных лицензий на ПО, но текущие контракты действуют и могут быть продлены, говорит директор управления развития продаж ГК Softline Андрей Благоразумов. Источники „Ъ“ ранее сообщали, что компания сама обратилась к ряду российских представителей международных компаний, не попавших под санкции, с предложением о продолжении сотрудничества (см. „Ъ“ от 28 апреля). Господин Благоразумов добавил, что «любой контракт от 500 рабочих мест невозможен

но продолжить без прямого взаимодействия с Microsoft».

По его словам, раньше корпорация предлагала корпоративным заказчикам два стандартных варианта лицензирования своего ПО: или аренда лицензий с продлением, или покупка постоянной лицензии с докупкой новых версий. «Смысла продлевать выкупленные лицензии нет, так как нет доступа к новым версиям и техподдержке», — говорит господин Благоразумов, уточняя, что Microsoft прекратила поддержку заказчиков с 1 июля 2022 года.

Помимо продаж ПО Microsoft оказывала услуги премьер-поддержки. Этот план «включал в себя инцидентную и проактивную поддержку продуктов вендора с высоким уровнем SLA (уровнем поддержки. — „Ъ“», объясняет вице-президент по развитию инфосистем «Ростелекома» Дарий Халилов. В 2021 году эти услуги, согласно финансовой отчетности основного российского юрлица Microsoft («Майкрософт Рус»), принесли тому 1,3 млрд руб., составив пятую часть его выручки. В 2022-м выручка от реализации премьер-поддержки упала до 462,5 млн руб. и до 9% в структуре выручки «Майкрософт Рус». Остальная выручка приходится на поступления от дочерних компаний Microsoft в Ирландии.

Российские компании, по словам господина Халилова, способны предоставлять вневедомскую поддержку с уровнем сервиса, сопоставимым с премьер-поддержкой Microsoft, «но не смогут обеспечить часть поддержки, связанной с исправлением специфических ошибок, для которых нет готовых общедоступных исправлений». При этом в двух крупных заказчиках продуктов Microsoft сказали „Ъ“, что прекращение премьер-поддержки не стало большой проблемой. «Ключевые игроки отечественного рынка обладают экспертизой и обходятся в вопросе поддержки собственными ресурсами», — заверил источник в одной из них.

Письма со старого адреса

У таких базовых продуктов Microsoft, как сервис корпоративной почты Microsoft Exchange и служба управления ресурсами Active Directory, «сегодня нет адекватных замен на рын-

ке», говорит источник „Ъ“ в одном из крупных заказчиков: «Большинство крупных российских бизнесов будет готово отказаться от этих продуктов лишь в том случае, если появятся полноценные аналоги, не уступающие решениям от Microsoft ни с точки зрения клиентского опыта, ни с точки зрения требований безопасности». Большинству других решений Microsoft можно найти альтернативы, «но их точно не будет разом у одного игрока», что усложняет процессы интеграции и ценообразования: «К тому же качество таких продуктов в деталях все равно будет уступать».

По всем классам ПО от Microsoft, используемого в «Ростелекоме», есть российские аналоги, и с 2016 года компания реализовывает программу его замены, говорит господин Халилов. Но компаниям со сложной инфраструктурой, переходящим с одного решения на другие, нужно, чтобы новые решения поддерживали интеграции и типовые паттерны совместимости: «У того же Microsoft существует способ миграции почтового ящика пользователя с одного почтового сервера на другой, в то время как у российских почтовых приложений такого рода опция пока отсутствует». Такие функции нужны компаниям, чтобы обеспечить «бесшовный переход в течение замены используемых технологий», причем этот процесс сложен сам по себе вне зависимости от страны происхождения ПО, добавил он.

Переход компаний на решения не от Microsoft будет зависеть как от правовой возможности использования их в России, так и от технических причин, полагает директор Ассоциации поставщиков программных продуктов Дмитрий Соколов: «Если окажется, что в тех или иных классах ПО будет легче перейти на аналоги — перейдут на аналоги, если решат, что легче перевести средства на спецсчет — будут переводить на спецсчета». Ранее глава Минцифры Максим Шадоев сообщил, что готовится способ легализации использования ПО из недружественных стран без российских аналогов (см. „Ъ“ от 20 апреля). Господин Соколов при этом заявляет, что представители крупных компаний зачастую усугубляют в своих заявлениях невозможность замены софта.

Корпоративные клиенты часто руководствуются «желанием получить все и сразу», но даже Microsoft не сразу начала удовлетворять этот запрос, говорит господин Соколов: «Если мы внимательно посмотрим на то же офисное ПО, то мы увидим, что его пакеты представляют собой лоскутные одеяла. Многие из продуктов Microsoft — исторически разработки других компаний».

Россия не может отобразить эту страницу

Поисковая система Microsoft Bing, несмотря на интеграцию в интерфейс операционной системы Windows, привлекала ничтожную аудиторию в России: по данным Statcounter и «Яндекс Радар», она составляла менее 1%. Интерес к поисковику повысился в феврале 2023 года, когда в Bing внедрили чат-бот на основе генеративных нейросетей. После запуска функции выяснилось, что Microsoft сделала ее неактивной для пользователей из России. Блокировка пересекается с недоступностью в РФ бота ChatGPT: оба ассистента полагаются на разработки OpenAI, привлеченной инвестициями Microsoft.

Американская компания, однако, уже вскоре после объявления об остановке продаж в России стала сворачивать региональные варианты своих информационных продуктов. Речь, в частности, идет о портале MSN со встроенным агрегатором новостей. В большинстве стран мира портал установлен по умолчанию как главная страница в браузерах от Microsoft (в России в качестве умолчаний используются сервисы «Яндекса»), а его новостная лента интегрирована в гаджеты Windows.

В ноябре 2022 года депутат Госдумы Антон Горелкин называл интеграцию MSN с Windows одним из доказательств того, что в России не наступил «цифровой суверенитет». «Ход компаний не означает, что люди перестали пользоваться их продуктами», — написал он в своем Telegram. Региональный сегмент MSN, однако, прекратил работу еще в марте, и на сайте отображаются только поисковая строка Bing. Ссылки на старые статьи, размещавшиеся на MSN, еще доступны на отдельных страницах сайта, но при этом не работают.

Юрий Литвиненко

информационные технологии

■ positive technologies

Тяжело в учении, легко в кибербою

К 2023 году ландшафт киберугроз заметно изменился: по последним исследованиям информационной безопасности (ИБ), экспертам удалось подтвердить реализацию 89% недопустимых событий в организациях ключевых отраслей экономики. Постоянное развитие угроз в IT-пространстве изменило «бумажный» подход компаний к кибербезопасности на результативный, заточенный на защиту инфраструктуры от недопустимых последствий атак. Это привело к росту спроса организаций на специальные тренировки ИБ-специалистов на киберполигонах для повышения готовности специалистов. „Ъ“ разобрался, как работает киберполигон, возможно ли столкнуться там с реальными угрозами и как отрабатывают навыки профессиональные защитники кибербезопасности.

— информационная безопасность —

Активная цифровизация российской экономики и ужесточение ситуации в IT-среде еще в прошлом году выявили уязвимости в защите инфраструктуры даже крупнейших отечественных компаний. Рост кибератак неоднократно приводил к остановке работы сервисов и даже целых ведомств — так, например, произошло с Федеральной таможенной службой в текущем году и, по неофициальным данным, с Росавиацией весной прошлого года. Обе структуры после атаки злоумышленников были вынуждены приостановить работу и перейти на бумажный документооборот. Страдал от кибератак и бизнес. Реализованные злоумышленниками события в российских организациях почти во всех случаях являются недопустимыми для них: именно такие сценарии должны предотвращать внутренние подразделения компаний, отвечающих за ИБ. Но в единичных случаях компаниям удавалось отразить нападение без потерь независимого от количества установленных средств защиты.

Все примеры показывают одно: за каждой системой кибербезопасности стоят люди, которые ею управляют и реагируют на инцидент, и нередко в первую очередь от них зависит защищенность организации. Для постоянного «поддержания в тонусе» специалисты и понимания самых современных угроз компании участвуют в киберучениях, чтобы погрузиться в реальные условия хакерской атаки.

Киберучения — это практическая, но безопасная для участников тренировка на реальных кибератаках этических, или, как их называют в отрасли, «белых» хакеров, которые не отличаются от реального инцидента и позволяют отточить навыки командной работы ИБ-специалистов. Для проведения профессиональных учений необходим киберполигон, который представляет собой цифровые копии типовых инфраструктур предприятий и объектов важнейших отраслей экономики со специфическим оборудованием и софтом.

Один из таких киберполигонов — Standoff — был развернут с 17 по 20 мая и представляет собой модель виртуального Государства F (так организации называют цифровую копию взаимосвязанных отраслей на своем киберполигоне), где есть вся присущая реальной стране инфраструктура.

«За последний год практически все отечественные компании подверглись кибератакам, причем во многих случаях злоумышленникам удавалось достичь своей цели и нанести ущерб бизнесу», — рассказал директор экспертного центра безопасности Positive Technologies (PT Expert Security Center) Алексей Новиков. — Киберучения позволяют проверить на прочность систему кибербезопасности, стек технологий, а также узнать, хорошо ли в компании выстроены процессы реагирования на угрозы».

Киберполигон Positive Technologies работает для атакующих 24/7, но ежегодно в рамках мероприятия он открывается для всех команд и зрителей, в нынешнем году — в 11-й раз. Само мероприятие Positive Hack Days проводится компанией—вендором ИБ-решений и лидером в области результативной кибербезопасности Positive Technologies уже 12-й год подряд, и в текущем году — как единственный в России открытый фестиваль кибербезопасности. В компании отмечают, что новый формат и площадка в парке Горького выбраны неслучайно: важно привлечь к участию не только ключевых специалистов отрасли, но и людей, которые только знакомятся с кибербезопасностью на бытовом уровне. Поэтому часть PHDays 12 была доступна всем посетителям парка бесплатно.

Основано на реальных событиях
В 2023 году наблюдается прирост доли инцидентов, затронувших веб-ресурсы организаций: с 17% до 22% относительно итогов 2021 года. Наибольший удар пришелся на государственные: количество успешных атак, направленных на сайты, выросло более чем в два раза. По словам Алексея Новикова, компании чаще всего взламывались с помощью фишинга, эксплуатации уязвимостей на пе-



риметре, взлома веб-приложений или просто в результате перебора паролей для сервисов удаленного доступа. При этом государственные, медицинские учреждения и промышленность чаще всего находятся в топе интересов злоумышленников.

Представители крупнейших российских организаций указывают, что при проведении киберучений должны быть учтены особенности инфраструктуры. «Идеальный киберполигон — тот, где учтена специфика деятельности организации», — считает заместитель начальника департамента мониторинга информационной безопасности Газпромбанка Евгений Горбачев. Например, для банка это могут быть платежи или другие бизнес-процессы, угрозы которым важно отработать, перечисляет он.

Главной особенностью киберполигона Standoff можно назвать реалистичность кибератак. В первую очередь это настоящий постоянный вредоносный трафик, направленный на инфраструктуру жертвы, который в этом году может стать любой участник независимой от размера его собственной инфраструктуры. Например, на киберучениях Standoff 11 представлены объекты компании финансового блока (Central Bank of the Standoff), промышленного (Big Bro Group), транспортного (контролирующая все пути сообщения города) и других значимых секторов экономики. В режиме реального времени команды могут наглядно увидеть последствия атак на свою инфраструктуру.

В Positive Technologies отмечают, что всем специалистам необходимо понимать возможность и масштаб сценариев атак любого типа, которые приводят к недопустимым для организации событиям. В текущем году на киберполигоне возможно реализовать более 140 недопустимых событий. Например, в случае с аэропортом, который должен работать постоянно и обслуживать как грузовые перевозки, так и пассажирские, от-

ключение электроэнергии может привести к сбою в работе диспетчеров и других критически важных специалистов, что влечет за собой последствия от транспортного коллапса до крупной аварии.

На Standoff недопустимые события реализуются через поиск уязвимостей в инфраструктуре жертвы, атакующие могут использовать любые — и самые современные, и уже исследованные — сценарии нападения. «Победит та команда „белых“ хакеров, которая сможет реализовать наибольшее количество недопустимых событий», — рассказывают в компании. Так защитники смогут убедиться в серьезности последствий разных атак и, конечно, отработать их командное отражение, объясняют в Positive Technologies.

Во время киберучений отрабатываются основные сценарии работы службы информационной безопасности, рассказывает Евгений Горбачев. Первое — это анализ IT-инфраструктуры, определение возможных векторов атак и изучение доступных средств защиты. Затем следует настройка сбора логов событий и разработка правил корреляций. И третье: определение мер предполагаемого реагирования исходя из векторов атак, говорит эксперт. Важным навыком, отрабатываемым на киберполигоне, является оперативное обнаружение и реагирование на атаки в стрессовых условиях. Изучение тактик и техник проведения атак на практике, а также командная работа защитников являются преимуществом участия в киберучениях, уверены в Газпромбанке.

Сила в команде

В киберучениях Standoff в нынешнем году приняли участие 22 команды атакующих и 7 команд защитников. Самыми зрелыми и понимающими важность киберучений в формате полигона оказались банки, убедили «Ъ» больше половины команд-защитников были представлены именно ими. Вто-

рые по количеству — представители энергетики и добывающей отрасли. На предстоящих открытых киберучениях в рамках PHDays размер команды был ограничен 10 участниками, но развитие площадки подтолкнуло организаторов к масштабированию команд до 15 человек: события происходят очень быстро, интенсивность атак высока, к тому же в идеале работать должна связка из защитников нескольких специализаций, поясняет бизнес-лидер киберполигона Standoff 365 Елена Молчанова.

На открытом киберполигоне как участники, так и зрители, получают ценный опыт: наблюдая за работой команд, все видят, как могут действовать злоумышленники, на что направляют ресурсы и как строят атаку. «Только за первый день Standoff, в рамках PHDays 12, атакующим командам удалось реализовать более 25 недопустимых сценариев, в том числе хакеры проникли в инфраструктуру завода по обогащению урана, созданную в этом году на полигоне», — рассказал CPO Standoff 365 Ярослав Бабин. За четыре дня атакующим удалось реализовать недопустимые события 204 раза. Чаще всего были реализованы утечка конфиденциальной информации (32 раза) и распространение вируса-шифровальщика (31 раз).

Также за все время кибербитвы в Государстве F атакующие сдали 209 отчетов об уязвимостях, из них 58% — об уязвимостях критического уровня риска, 24% — высокого и 17% — среднего. Наиболее популярным типом выявленных уязвимостей стало удаленное выполнение кода (Remote Code Execution). «Для команд защитников это огромный опыт: за несколько дней изучить самые актуальные и серьезные методы атак», — считают организаторы Standoff 11. Команды защитников подготовили более 200 отчетов о выявленных инцидентах и расследовали 11 атак, которые привели к недопустимым событиям. Для мониторинга и расследования инцидентов участникам были предоставлены продукты Positive Technologies.

Standoff 11 показал на практике последствия самых актуальных в 2023 году киберугроз для объектов, которые в первую очередь подвергаются нападениям реальных хакеров. Спрос на экспертизу со стороны специалистов по информационной безопасности подтверждает рост рынка центров мониторинга и контроля кибербезопасности (SOC) — в сравнении с первым кварталом 2023 года интерес к ним со стороны российского бизнеса составил 25%, а к концу года динамика может достигнуть 70%, отмечают исследователи рынка. Это связано с постоянно растущим напряжением в киберпространстве — так, объем персональной информации граждан, незаконно попавшей в сеть за первый квартал, превысил 118 млн уникальных записей, что в 2,3 раза выше, чем за аналогичный период прошлого года. Киберполигон уже стал необходимым для специалистов местом тренировок и обмена опытом, спрос на который растет пропорционально росту киберугроз.

Татьяна Исакова

Безопасности добирают ума

— инновации —

ChatGPT, чат-бот на основе искусственного интеллекта (ИИ), набрал популярность во всем мире всего за несколько месяцев благодаря простому интерфейсу и многозадачности программы. С ее помощью и подключением других инструментов на основе ИИ IT-специалисты стараются решить большое количество задач, оптимизировав собственные ресурсы и упростив работу. Но, как и любую другую технологию, нейронные сети можно использовать как во благо, так и в преступных целях. „Ъ“ разобрался, как влияет развитие ИИ на работу хакеров и защитников информационных систем.

Глобальный рынок искусственного интеллекта в сфере кибербезопасности аналитическая компания Research and Markets в 2022 году оценивала в \$14,1 млрд. К 2027-му, считают исследователи, рынок может достигнуть \$41,9 млрд при среднегодовом темпе роста 24,4%. К драйверам роста этого направления Research and Markets относят распространение технологии интернета вещей (IoT), в том числе увеличение количества подключенных устройств по всему миру, повышение уязвимости Wi-Fi и рост числа киберинцидентов во всем мире.

Начало 2023 года в России продемонстрировало изменения ландшафта кибератак на отечественные IT-системы: по данным компании по защите от интернет-угроз Qrator Labs, по сравнению с первым кварталом 2022-го длительность DDoS-атак сократилась более чем в шесть раз. В компании объясняют это более тщательным выбором жертв хакерами, а также применением злоумышленниками современных инструментов анализа трафика и систем защиты атакуемых. В качестве примера эксперты по кибербезопасности приводят распространяющиеся в даркнете вредоносные коды и программы на основе нейросетей, способных самостоятельно мониторить инфраструктуру жертв.

Также сам ИИ все чаще становится жертвой кибератак: по данным исследования Gartner, выпущенного летом 2022 года, 41% опрошенных организаций столкнулись с нарушением конфиденциальности организации через внутренний ИИ. При этом 60% инцидентов были связаны с компрометацией данных внутренним злоумышленником (инсайдером), в то время как 27% атак были атаками на нейросети извне. Эксперты по

итогам исследования пришли к выводу, что при внедрении моделей искусственного интеллекта компаниям пора предусматривать защиту алгоритма от внешнего воздействия.

Качай оружие

Условия работы OpenAI (разработчик ChatGPT) для чат-бота прямо запрещают создание вредоносных программ, вирусов и других инструментов хакеров. Однако, по данным международных СМИ, практически сразу после появления последней версии бота злоумышленники начали тестировать на нем написание вредоносного ПО.

Да, условия работы для ChatGPT действительно запрещают боту сообщать опасную и неправомерную информацию, однако технология несовершенна, и даже не злоумышленники, а обычные любознательные пользователи придумали несколько способов обхода этого запрета, говорит коммерческий директор «Кода безопасности» Федор Дбар: «Например, они представляют чат-боту преподавателя и просят его сделать код фишингового письма, чтобы показать студентам, как он может выглядеть».

Хакеры и до появления последней версии ChatGPT использовали в своих целях искусственный интеллект. «ИИ — это инструмент оптимизации усилий, поэтому его используют те, кто хочет добиваться своих целей эффективнее, быстрее, с меньшими затратами», — объясняет замдиректора «Гарда Технологии» Рустэм Хайретдинов. Средства для создания и обучения инструментов ИИ, в том числе вредоносного, находятся в открытом доступе, поэтому неудивительно, что преступники, которых не сдерживают ни законы, ни вопросы морали при использовании ИИ, идут на шаг впереди защитников. «Библиотеки нейросетей и обучающие датасеты активно используются злоумышленниками», — добавляет эксперт.

Ведущий инженер CorpSoft24 Михаил Сергеев выделяет несколько категорий кибератак, в которых уже используются нейронные сети:

фишинговые атаки — хакеры используют ИИ для создания более реалистичных фишинговых писем и веб-страниц, которые могут обмануть даже опытных пользователей. Также ИИ может анализировать данные из социальных сетей и создавать персонализированные фишинговые письма, которые выглядят более убедительно, чем стандартная рассылка;

атаки на пароли — использование нейронных сетей для создания и тестирования словарей паролей может ускорить и улучшить процесс их взлома;

социальная инженерия — ИИ может использоваться для анализа и сбора информации о целях атаки, что может помочь хакерам реализовать их более персонализированно; фальсификация информации — ИИ может использоваться для создания фальшивых новостей и информации.

Использование ИИ в хакерских атаках — это тренд, который наблюдается во всем мире, а не только в России, добавляет господин Сергеев. Атаки с элементами ИИ могут быть проведены любыми киберпреступниками независимо от их местоположения. Нейронные сети сильно повышают эффективность атаки, благодаря этому в том числе удалось успешно совершать различные атаки на российскую инфраструктуру, уверен он.

Разнообразие использования ИИ в хакерских атаках огромно: начиная от фишинговых рассылок и заканчивая разработкой зловредов и эксплоитов, соглашается эксперт по кибербезопасности Axenix Евгений Качуров. Конечно, необходимо иметь базовые знания и обладать опытом обхода ограничений ИИ в части разработки зловредов и эксплоитов, но это не является непосильной задачей — с ней сможет справиться любой, добавляет он: «Поэтому можно ожидать появления армии так называемых script kiddie (хакеры, использующие скрипты и программы) с минимальным набором знаний и опыта, но с жизнеспособными инструментами». С этим согласны и зарубежные эксперты в области кибербезопасности: исследователь группы Check Point по анализу угроз Сергей Шикевич напоминает в диалоге с ZDNET, что «невозможно свести злоупотребление новыми технологиями к нулю».

Умный щит

Специалисты в области кибербезопасности, в свою очередь, тоже начинают использовать обучение нейронных сетей для выстраивания защиты IT-систем. Например, по словам собеседников „Ъ“ на IT-рынке, алгоритмы машинного обучения уже используются для обнаружения аномального поведения в сети, а также для автоматизации процессов анализа уязвимостей и создания решений для защиты от них.

Средства защиты активно внедряют ИИ, особенно там, где нет четкого понимания, что

это атака, рассказали в «Гарда Технологии». ИИ хорош для обнаружения и быстрого анализа аномалий в цифровых системах, отделение ошибок от злонамеренных действий, то есть там, где нужно быстро проанализировать большое количество данных и взаимосвязей без наличия четких правил. Такие технологии используются в средствах защиты от сетевых атак, DDoS-атак, межсетевых экранов прикладного уровня, межсетевых экранов нового поколения, решениях UEBA, DBF и многих других, перечисляет Рустэм Хайретдинов.

Наиболее распространенная сфера применения ИИ — поведенческий анализ, говорит Федор Дбар: «По большому счету есть два способа понять, что такое-то ПО или, скажем, трафик в сети носит вредоносный характер. Первый способ — сравнение с сигнатурами, то есть с некими слепами каких-то сущностей, которые когда-то были признаны вредоносными». По этому принципу работают антивирусы, объясняет он: у них есть база вирусов, которые были отловлены ранее, и по ней они проверяют, нет ли совпадений: «Это похоже на работу прививки, когда у пациента берут небольшое количество образца, а затем передают их другим людям, чтобы они вырабатывали иммунитет».

В России, считают собеседники „Ъ“, есть несколько факторов, стимулирующих развитие технологии нейронных сетей в целом и ИИ в кибербезопасности в частности. Например, внимание государства к развитию технологии: Минэкономразвития планирует в ближайшее время «ускорить процесс широкомасштабного внедрения отечественных ИИ-решений в экономику и социальную сферу». Мероприятия, направленные на развитие технологии, закреплены в «дорожной карте» «Развитие высокотехнологичного направления „Искусственный интеллект“ (ИИ) до 2030 года».

Еще одним фактором является усиливающийся в России кадровый дефицит: компании за неимением достаточного количества специалистов начинают тестировать нейронные сети для написания простых кодов и других прикладных задач. Среди сдерживающих факторов развития технологии собеседники „Ъ“ называют дефицит вычислительных мощностей и кадров для развития самой технологии.

«Существует множество потенциальных вариантов использования ИИ в сфере кибербезопасности: его можно использовать в IoT для повышения безопасности, за-

щиты активов и снижения уровня мошенничества», — считают эксперты компании «Информзащита». В долгосрочной перспективе искусственный интеллект выйдет за рамки предотвращения мошенничества и злонамеренных действий, так как он будет использоваться для предоставления расширенной аналитики и принятия решений. Это особенно актуально для решений IoT, использующих данные в реальном времени, уверены в компании.

Игра на опережение

Развитие информационных технологий, и искусственного интеллекта в частности, постепенно будет менять отрасль кибербезопасности, считают эксперты. Сергей Шикевич в разговоре с ZDNET поделился мнением, что «в краткосрочной перспективе тот же ChatGPT не создаст совершенно новые типы атак, но основное внимание разработчиков будет уделяться тому, чтобы сделать их повседневные действия более рентабельными».

С помощью ИИ можно быстро строить новые векторы атак, автоматизировать их, уменьшать время от обнаружения уязвимости до атаки — делать все вредоносное, что человек делает медленнее машины, прогнозирует Рустэм Хайретдинов.

С развитием нейронных сетей возможности для создания новых типов хакерских атак могут увеличиваться, согласен Михаил Сергеев. Например, могут появляться новые атаки на IoT-устройства, на автомобили, а также новые методы обхода сетевых защитных механизмов, но с ростом количества средств обнаружения и предотвращения кибератак злоумышленникам также придется создавать более сложные алгоритмы и использовать более продвинутые методы, уверен он.

«Вряд ли ИИ сможет создавать новые типы атак, но однозначно может модернизировать уже имеющиеся. Направление развития ИИ может варьироваться в зависимости от целей, которые преследуют мошенники», — считает руководитель отдела анализа и оценки цифровых угроз Infosecurity а Softline Company Константин Мельников. Эксперты «Информзащиты» прогнозируют, что вендоры решений в области информационной безопасности также будут наращивать компетенции в сфере искусственного интеллекта: в перспективе на рынке могут появиться сделки и партнерства разработчиков с компаниями, производящими решения в области нейронных сетей.

Татьяна Исакова

информационные технологии

«Параллельный импорт — игра в лотерею»

Уход зарубежных компаний из России заставил отечественные организации усиленно заниматься импортозамещением. Технологические проблемы коснулись и сферы информационной безопасности, где корпорациям с масштабными IT-инфраструктурами требуются межсетевые экраны нового поколения — NGFW. Коммерческий директор ИБ-вендора «Код Безопасности» **Федор Дбар** объяснил, что, почему импортозамещение — наше единственное будущее, почему переход на российские решения должен быть быстрым и что ожидает Россию в ближайшие годы.

— мнение —

— **Федор Анатольевич, в любой сфере есть свои лидеры. А какие компании главенствуют на рынке NGFW?**

— Здесь также есть своя «большая четверка»: Cisco, Fortinet, Check Point и Palo Alto. Каждая из них существует 20–40 лет, и все это время в качестве тестового полигона для них открыт весь мир — даже когда NGFW этих компаний не были идеальными, альтернатив им не было. На сегодняшний день «большая четверка» имеет высококачественные NGFW, которыми пользовалось большинство компаний России. В 2022 году установленное оборудование насчитывало 30–40 тыс. единиц, но после ухода зарубежных вендоров этот объем превратился в громадную дыру, которую необходимо оперативно закрыть российскими решениями. — **Импортозамещение у нас часто ругают. Обыватели считают, что, кроме вооружения, в России ничего сделать не могут, особенно если речь идет о высокотехнологичных решениях. Насколько это справедливо?**

ЧТО ТАКОЕ NGFW

NGFW (Next-Generation Firewall — межсетевой экран нового поколения) представляет собой устройство с большим количеством функций, обеспечивающих централизованное управление и комплексную защиту масштабных IT-инфраструктур. В NGFW входят межсетевые экран для фильтрации сетевого трафика, система предотвращения вторжений, система обнаружения приложений и Extra Firewall Intelligence, которая обеспечивает постоянную актуализацию механизмов защиты.

— Эта точка зрения далека от реальности, потому что в большинстве отраслей проблема создания альтернатив западным решениям зависит не от способностей, а от банального жизненного цикла любой компании и ее продуктов.

— **Что вы имеете в виду?**

— Доступность современных технологий открывает большие возможности, поэтому начинающие компании без проблем создадут рабочий продукт. Можно сделать качественный антивирус, приготовить вкуснейший гамбургер, даже построить и запустить в небо небольшую ракету, но приблизит ли это к созданию корпорации уровня «Лаборатории Касперского», «Роскосмоса» или McDonald's? Нет, потому что появление таких компаний зависит от самых разных факторов, главный из которых время.

Та же «Лаборатория Касперского» стала одной из ведущих не сразу, а лишь пройдя через сложные времена — кто помнит, первые версии их антивируса в целом уступали другим предложениям. Со временем технические проблемы были решены, но сам по себе продукт — лишь малая часть успеха, ведь любая крупная компания представляет огромную машину со своей экосистемой из тысяч сотрудников, подрядчиков, поставщиков и клиентов. Эта машина создает множество простых и понятных в эксплуатации и поддержке решений, работающих на всевозможных платформах и любых языках.

— **Почему при доступности технологий и возможности привлечения инвестиций нельзя построить эту машину в короткий срок?**



ФОТО: АЛЕКСАНДР КОД БЕЗОПАСНОСТИ

— Существуют естественные процессы роста, требующие времени, например переход с одного уровня управления на другой. Одно дело — разрабатывать нишевой продукт с командой единомышленников в гараже, и совершенно иное — руководить сотнями сотрудников. Это

«гражданского» человека, в реальности бизнеса и государства параллельный импорт — временная мера.

— **Почему?**

— Для крупных структур критически важен стабильный приток запчастей и прочих расходников, а параллельный импорт — это игра в ло-

24 миллиарда рублей составит объем рынка NGFW в 2023 году, по данным «Кода Безопасности»

задача не из тривиальных, и непонимание важности грамотного менеджмента погубило многие компании. — **Так ли необходимо импортозамещение NGFW и других технологий, ведь есть же параллельный импорт?**

— Скепсис по отношению к импортозамещению частично вызван пристрастной надеждой, что скоро все будет как прежде, а пока можно перебраться параллельным импортом. И он действительно спасает, ведь автомобили не разваливаются на ходу, промышленность не останавливается, а в магазинах по-прежнему есть ограниченные деликатесы. Но это взгляд

терею, так как всегда существует вероятность, что на границе задержат важную партию и ты останешься ни с чем. В 2022 году ушли зарубежные IT-вендоры, но, как бы громко они ни хлопали дверью, их оборудование продолжило работать и критических проблем не возникло. Однако это породило иллюзию, что искать альтернативу нет необходимости, к тому же можно схитрить с параллельным импортом — и никто не заметит. В действительности таких хитрецов много, поэтому никакие уникальные логистические пути нет — рано или поздно их найдут и перекроют. Те, кто еще в прош-

Бизнес берет GPT-4 в оборот

— инновации —

В марте OpenAI представил новое поколение алгоритма по обработке естественного языка GPT-4. В отличие от своих предшественников, нейросеть научилась анализировать изображения и способна обрабатывать более сложные инструкции. «Б» разбирался, как GPT-4 может использоваться бизнесом, на какие отрасли технологии сильнее всего повлияет в перспективе нескольких лет и каких специалистов может или не может заменить.

GPT-4: точность и анализ изображений
GPT-4 стал самой обсуждаемой технологией в сфере искусственного интеллекта (ИИ) нынешней весной. Система основана на принципе языковой модели: алгоритм, обученный на огромных массивах текстов — от классики мировой литературы до постов в соцсетях, определяет статистическую вероятность того, что после того или иного слова будет то или иное другое слово, и таким образом создает новый текст. Ключевое отличие GPT-4 от предыдущих версий ChatGPT и GPT-3.5 состоит в том, что она может анализировать изображения. Также, по данным самой OpenAI, она превосходит GPT-3.5 на 40% по достоверности, а ее склонность к запрещенному контенту снижена на 82%: модель шесть месяцев учили ориентироваться в этике.

Возможность обработки изображения в теории значительно расширяет применение модели в бизнес-процессах, говорят эксперты. «Так, теперь клиентские решения могут быть основаны на единой модели, которая помимо текстовых запросов сможет обрабатывать и изображения, что значительно повысит качество обслуживания», — говорит вице-президент Сбербанка Максим Еременко. Помимо генерации текстов важное свойство GPT-4, которое уже сейчас используется многими на практике, — умение преобразовывать

текст и данные из одного формата в другой, отмечает директор по развитию прикладных проектов Института искусственного интеллекта AIRI Манвел Аветисян: «В среднесрочной перспективе я ожидаю, что GPT-4 и похожие нейросетевые модели от других компаний поменяют то, как мы организуем и ищем информацию в интернете: этот процесс станет более быстрым и нативным». С нейросетью в новой версии в целом стало гораздо легче взаимодействовать, она лучше работает с изображениями и стала более точной, резюмирует Артем Чистяков, преподаватель направления Data Science «Нетологии»: «А для бизнеса именно точность работы нейросети и сложность решаемых ею задач важнее всего».

Проблема надежности

Несмотря на то что Microsoft встроила GPT-4 в свой поисковик Bing, мы пока не можем судить, насколько на самом деле будет актуальным ответ сети: не выдает ли она в ответ устаревшие факты, говорит директор по RnD Центра Big Data МТС Никита Зелинский. «Проблемы актуальности, правильности и надежности ответов по-прежнему остаются. Хотя сильная сторона GPT-4 — мультиязычность, максимальных результатов сеть достигает в задачах на английском, качество генерации русского текста существенно хуже. Пока я лично не вижу каких-то отличий применения GPT-4 от ChatGPT», — говорит он.

Обработка изображений в языковой модели пока недоступна широкой публике и находится на стадии тестирования: нет даже приблизительной даты, когда ее можно будет попробовать, отмечает управляющий партнер аналитического агентства SpektR Николай Седашов. Он считает, что пока наиболее значимым кажется появление API ChatGPT, который позволяет встраивать функционал чат-бота в сторонние сервисы и бизнесы, а также запуск плагинов — расширений, выполняющих обратную функцию по интеграции сторонних приложений в ChatGPT: «Эти две вещи в перспективе превра-

щают ChatGPT в платформу наподобие App Store и открывают возможность как для монетизации бота, так и для создателей приложений».

Чем может помочь GPT-4: тексты и анализ данных

Хотя и GPT-4, и ChatGPT, который на ней работает, находятся пока в довольно сыром виде, некоторые компании уже используют их для создания презентаций, написания почтовых рассылок. «Чат-бот достаточно хорошо справляется с большими текстами, может создавать идеи для проектов и рекламных кампаний, написать сценарий видео», — говорит Николай Седашов.

Компании могут использовать GPT-4 для создания чат-ботов и виртуальных помощников, которые взаимодействовали бы с клиентами и оказывали мгновенную помощь: они могут обрабатывать рутинные запросы и обеспечивать круглосуточную поддержку, освобождая сотрудников поддержки для решения более сложных вопросов, говорит сооснователь VitoBox Александр Вученович: «Применение GPT-4 в генерации контента для социальных сетей и email-рассылок сильно снизит нагрузку копирайтеров в компании и даст им возможность сконцентрироваться на создании более экспертных материалов».

Копирайтинг, написание самых разных текстов: от документации до рекламных баннеров — это самое очевидное, говорит сооснователь United Investors Александр Горный: «Психологически сложнее, но, возможно, даже более полезно сделать нейронные сети помощником в менеджменте, прогонять через них все решения хотя бы в режиме брейншторма».

Компании, которые работают в сегменте дополнительного образования, могут использовать нейросети для развития виртуальных ассистентов, рассказал Георгий Бабаян, руководитель и основатель школы программирования «Эльбрус Буткемп»: «Например, в нашей школе студенты обращаются к GPT-4 для поиска развернутых ответов на вопросы по

разработке. Если у них возникают трудности с кодом, прежде чем обратиться к преподавателю, они пробуют справиться сами с помощью нейросети». По его словам, около 25% выпускников буткемпа используют ChatGPT в разработке для написания определенных фрагментов кода: «Правда, для проверки технических заданий и вступительных экзаменов ChatGPT пока не применяется».

Какие сферы меняет GPT-4

Уже сейчас есть ряд профессий, которые пользуются ChatGPT ежедневно: это основатели стартапов на ранних стадиях, продавцы — особенно там, где нужно вести коммуникацию на неродном языке, говорит Никита Зелинский. Корпоративное же использование сервиса пока затруднено — мешает блокировка российских адресов, непонятная политика конфиденциальности, говорит Роман Янковский, преподаватель образовательной платформы Moscow Digital School: «Но с появлением аналогов (того же Copilot от Microsoft), приспособленных под задачи крупных компаний, все процессы будут включать работу с ИИ. В первую очередь это все, что касается менеджмента: составление писем, презентаций, других материалов, распределение задач и т. п.». Генеративные нейросети начали с рынка копирайтинга, но это всего лишь «проба пера», считает Александр Горный.

Максим Еременко отмечает, что GPT-4 создает новый подход к веб-поиску: «Уже сейчас существуют плагины, которые позволяют языковой модели осуществлять поиск информации из специфичных источников, например базы данных компании, которая использует языковую модель в своих приложениях или веб-сайтах, в который она интегрирована». Сфера, на которую уже повлияли ChatGPT и GPT-4, — программирование, добавляет он: «Несмотря на то что существуют отдельные модели для обработки кода, наличие сильной универсальной модели, которая поможет исправлять код из единой точки, — большой шаг вперед».

лом году начал обкатывать российские решения, поступили наиболее дальновидно.

— **Но есть же альтернативы, например продукты Китая или других дружественных стран?**

— Наш мир не перестает жить: работают банки, открываются госучреждения, внедряются различные информационные системы. Для всего этого нужны софт и оборудование, которые периодически требуют перенастройки или ремонта. Если мы хотим, чтобы страна развивалась, должна развиваться и ее IT-инфраструктура, а это нельзя сделать, если разработчик находится за пределами России. Как показывает общемировая практика, независимость и безопасность возможны только через тяжелый путь импортозамещения. Нам придется его пройти, как бы мы ни хотели этого избежать.

— **Почему путь импортозамещения такой непростой?**

— В первую очередь потому, что объем IT-инфраструктуры, который требует перестройки, колоссален. Во-вторых, альтернативные решения, имеющиеся на рынке, подходят не всем компаниям: им хотелось бы идти своим путем, но государство не может сделать разные правила — они должны быть унифицированы. Как со скоростным режимом на дорогах: везде действует одинаковое ограничение, уравнивающее лихачей, новичков, уставших, бодрых и любых других. Да, для каких-то компаний законодательные требования станут тяжелым компромиссом, однако это данность, которую не изменить.

— **Почему создание отечественных NGFW не началось задолго до 2022 года?**

— Во-первых, не было необходимости: потребитель все равно предпочитал решения «большой четверки». Во-вторых, две компании все же решили делать свой продукт, несмотря на присутствие Cisco, Fortinet, Check Point и Palo Alto. Это «Код Безопасности» и UserGate, которые на сегодняшний день уже преодолели те проблемы роста, о которых мы говорили, и в итоге создали качественные решения, заняв определенную нишу. Конечно, у них есть свои минусы и плюсы, однако NGFW «Кода Безопасности» и UserGate зарекомендовали себя на рынке и ими пользуются тысячи компаний, в том числе крупные государственные организации и корпорации с госучастием.

— **Если уход «большой четверки» образовал на рынке NGFW вакуум, то смогут ли две компании его заполнить?**

— Естественно, рынок пополняется и будет пополняться другими вендорами. Из крупных игроков, которые разрабатывают NGFW, стоит выделить две компании: Positive Technologies и «Ростелеком-Солар». У каждой из них есть свои конкурентные преимущества, и я думаю, что они сыграют важную роль в формировании рынка NGFW, поскольку конкуренция всегда оказывает позитивное влияние на качество продуктов всех игроков.

Единственная проблема в том, что работать «новичкам» приходится в сжатые сроки: чтобы внедрить NGFW к 2025 году, провести «пилот» рабочей версии на IT-инфраструктуре заказчика нужно уже в мае 2024-го. И это крайний срок, потому что любые инфраструктурные проекты готовятся и обкатываются долго.

— **Есть ли возможность подождать и начать полномасштабное импортозамещение NGFW и других IT- и ИБ-решений позже?**

— Если говорить конкретно об этих сферах, то нет — переход нужно делать как можно быстрее, особенно в части NGFW, потому что эти устройства обеспечивают безопасность объектов критической информационной инфраструктуры.

Как я уже отмечал, объем рынка NGFW огромен — 30–40 тыс. единиц оборудования, к тому же благодаря 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» к 2025 году, по самым скромным оценкам, востребованность NGFW вырастет еще на 20–30%. Чтобы удовлетворить все нужды и успеть вовремя, потребуются приложения сил не только от вендоров, но и всех участников рынка: интеграторов, заказчиков, поставщиков.

Интервью взял Матвей Соколов

ИЗ ИСТОРИИ NGFW

Появление NGFW стало ответом ИБ-специалистов на расширяющийся ландшафт киберугроз, нехватку квалифицированных кадров, а также усложнение IT-инфраструктур. Первые NGFW появились в 2009 году, а спустя семь лет компании выпустили второе поколение NGFW, в которых были добавлены новые механизмы защиты. На 2021 год, по оценкам Gartner, 95% компаний мира используют NGFW для защиты периметра сети.

доверяют только ограниченный объем задач, в основном технических, вполне может: «Но GPT-4 не разработает стратегию защиты интеллектуальной собственности для клиента».

На горизонте десяти лет сокращения коснутся вообще всех слоев воротничков, пессимистичен Александр Горный: «Прямо сейчас под явной угрозой еще далеко не все, но и у копирайтеров, и у редакторов, и у специалистов служб поддержки, и у младших юристов, например, потери будут уже в 2023–2024 годах». Заведующий Центром трансформации юридического образования факультета права НИУ ВШЭ Роман Янковский ожидает, что использование ИИ «упозволит высвободить значительное количество специалистов, занимающихся малопродуктивным ручным трудом».

В целом перспективы сокращения могут коснуться скорее наименее квалифицированных сотрудников, считает Манвел Аветисян: «Но вырастет ценность высококлассных и узкопрофильных специалистов, которые будут уметь пользоваться инструментами на основе GPT-4». Николай Седашов считает, что в будущем интеграция чат-ботов в рабочие процессы может повлиять на наем персонала на начальные должности: «Сейчас чат-бот не сможет заменить собой настоящих профессионалов. Сегодняшние модели ограничены теми знаниями, на которых они натренированы. Ближе к истинной концепции, которую продвигает Microsoft, где искусственный интеллект — «второй пилот», который всего лишь помогает быть продуктивнее и производительнее».

Всю информацию, получаемую с помощью ChatGPT, нужно внимательно проверять, напоминает Никита Зелинский: «Поэтому я бы не опасался сокращений специалистов, но ожидал бы, что производительность труда маркетологов, рекламщиков, редакторов, программистов, аналитиков, презентаторов и многих других специалистов повысится».

Валерия Лебедева

информационные технологии

«IT лучше всего развивается в изменчивых индустриях»

Сегодня CRM-системы — это главный инструмент, который позволяет бизнесу выстраивать работу по взаимодействию с клиентами. Потребность в российских CRM-системах растет как из-за политики импортозамещения и требований регуляторов, так и из-за необходимости модернизировать уже существующие системы для решения новых задач, в числе которых детальное понимание потребностей клиентов. Первый заместитель генерального директора холдинга T1 **Кирилл Булгаков** рассказал, Ё о состоянии рынка, перспективах экспорта российских решений в Юго-Восточную Азию и Латинскую Америку, а также о том, какой технологический скачок предстоит совершить компаниям-разработчикам для того, чтобы вывести рынок на новый уровень развития.

— мнение —

— В конце 2022 года мы слышали от чиновников и топ-менеджеров тезис о том, что российские разработчики ПО смогли заместить большую часть зарубежных решений. Как вы думаете, как реально обстоит ситуация с замещением программного обеспечения?

— Не думаю, что нужно обманывать себя завышенными ожиданиями. Замещение иностранного программного обеспечения на текущий момент выглядит неравномерным. Решения, востребованные широким кругом потенциальных заказчиков, замещаются сейчас без больших трудностей. То есть на рынке для таких продуктов есть объем денег, который заказчики готовы потратить, и, с другой стороны, есть компании, которые могут закрыть этот спрос.

Сложнее ситуация в тех нишах, где круг заказчиков очень узкий. Им нужно специфичное программное обеспечение, для разработки которого требуются время и глубокие компетенции. Обычно это ПО необходимо промышленным предприятиям, например системы автоматизированного проектирования или программы жизненного цикла продуктов. В таких случаях компаниям приходится, с одной стороны, использовать зарубежный софт, добавляя к нему собственные страховочные решения, а с другой — готовить программы реализации импортозамещения, закладывая бюджет на миграцию на альтернативное ПО.

— А если говорить о ситуации в разрезе отраслей? Компании каких сегментов лучше адаптируются к текущим вызовам, а каких — хуже?

— Успешность замещения зарубежного софта варьируется от индустрии к индустрии. Так сложилось, что в России IT лучше всего развивается в изменчивых индустриях — в отраслях, которые в силу высокой конкуренции были вынуждены постоянно адаптироваться к новым условиям, быть гибкими. Это финансовый сектор: по уровню цифровизации отечественные банки сейчас самые передовые в мире, транспорт и логистика, а также, как ни странно, государственный сегмент. Сегодня сложно найти в мире такую же качественную с точки зрения цифровизации процессов систему государственных сервисов, как у нас.

Необходимость постоянно модернизировать собственные сервисы и системы привела к тому, что крупные компании и организации в этих сегментах создали собственные департаменты цифровизации, которые разрабатывали ПО для внутренних нужд. Однако есть ряд отраслей, где цифровизация играла менее значимую роль. Это крупные промышленные предприятия, и там уровень развития IT-систем не такой высокий, а гибкость ограничена. Сейчас такие компании находятся в поиске способов замены зарубежного софта. — **Власти с осени прошлого года инициируют переход на российские решения через механизмы ИЦК и ЦКР. Эти инструменты похожи на механизмы ручного управления рынком. Насколько они сегодня оправданны, показывают они эффективность?**

— То, что вы называете ручным регулированием IT-индустрии, не российское изобретение. В Китае, Евросоюзе, США и на других крупных рынках регуляторы так или иначе направляют свои цифровые индустрии по нужному треку, а рынок приспосабливается к пожеланиям регуляторов, подстраиваясь под них.

Если оценивать эффективность механизмов ИЦК и ЦКР, то они превосшли мои ожидания. Они работают ста-

лансированно: с одной стороны, есть пожелания регулятора, а с другой — саморегулирование отрасли. В ИЦК и ЦКР регулярно собираются те участники рынка, которым такой подход интересен и которые хотят и умеют пользоваться такими форматами взаимодействия с регуляторами, определяя наиболее значимые проекты.

Эти механизмы, повторюсь, работают хорошо. Есть возможность получить гранты на разработки, при этом грантовые программы отличаются друг от друга: в одних случаях это средства на разработку, в других — бюджет на внедрение, который реализуется совместно с исполнителем.

Чаще подобную государственную поддержку получают те компании, которые готовы решать значимые для отрасли и государства задачи, и это не обязательно крупнейшие игроки рынка. Резюмируя, я вижу в индустриальных центрах компетенций и центрах компетенций разработки эффективности и пользу: появился поток государственных денег, которые стимулируют частную инициативу.

— **Участники рынка в анонимных беседах со мной несколько раз говорили о том, что в ряде сегментов срочное замещение зарубежных решений невозможно в силу того, что они слишком сложные. Другие же отмечали, что по ряду направлений замещение и вовсе не нужно. Какая у вас на этот счет точка зрения?**

— Насколько бы сложной ни была система, создавать работоспособный аналог можно и нужно. Приведу пример: до санкций некоторые российские авиаперевозчики использовали зарубежную систему бронирования билетов Sabre. Она была глубоко интегрирована в их инфраструктуру, а ее замена виделась многим невозможной. Но когда появилась острая потребность, деньги нашлись, программное обеспечение переписали. Аналогичная ситуация будет и в других сегментах, где замещение сейчас кажется излишне трудоемким.

Однако рынок и регуляторы действительно могут столкнуться с проблемой, когда компании затратили средства на разработку импортозамещающего ПО, которое в итоге останется среди заказчиков невостребованным. Например, брокерские системы.

— **В 2022 году вы в одном из интервью об эволюции CRM-систем говорили, что крупные заказчики, столкнувшиеся с риском потери лицензий на западный софт, оказались на распутье: искать замену среди российских решений либо писать систему под заказ. Это проблема для российских поставщиков решений или нет?**

— Как разработчики T1 CRM мы видим сразу несколько интересных тенденций. Первая заключается в том, что крупные заказчики вошли во вкус цифровизации и разработки и собственными силами создают системы для внутренних нужд. Это осложняет ситуацию для российских поставщиков: крупным клиентам сложно доказывать, что решение, разработанное опытным вендором, который годами занимался подобными проектами, несет в себе больше практической ценности, чем внутренний продукт.

Есть и другая тенденция. Ее можно назвать нестандартной. На рынке стали появляться небольшие компании, которые на волне возросшего интереса к замещению продуктов предлагают потенциальным заказчикам «идеальные» решения с безграничным функционалом. На деле у таких компаний нет ни опыта разработки, ни уникального продукта, ни средств на развитие. В итоге ряд



клиентов в подобной ситуации рискует оказаться обманутыми.

— **Как вы по итогам чуть больше чем года после начала санкций оцениваете готовность российских заказчиков к миграции на российские CRM-решения?**

— Интерес большой, но мы наблюдаем в этом случае неоднозначный процесс. Компании разрабатывают собственными силами продукты, внедряют их, затем осознают, что установка зрелых решений от крупных вендоров будет продуктивнее, и берут продукты и поддержку уже опытных разработчиков.

— **А если говорить о компаниях, которые пока предпочитают использовать решения зарубежных вендоров in house?**

— In house против новой системы — актуальная история. Да, ряд крупных компаний продолжает использовать CRM от зарубежных игроков. Но возможности их развития ограничены, что сдерживает масштабирование бизнеса. Поэтому я уверен, что в течение ближайших двух-пяти лет даже крупнейшие пользователи таких систем перейдут на отечественные решения.

— **Я несколько раз слышал тезис о том, что сейчас заказчики делятся на две категории: одним нужна полная копия западных решений, а другие, напротив, хотят, чтобы замещенные продукты превосходили по функционалу зарубежный софт. Это так?**

— Да, мы также наблюдаем подобное разделение. Одни просто полностью скопировать привычный функционал решений ушедших вендоров, а другие готовы на глубокое переосмысление своего подхода к работе с цифровыми продуктами. Мне ближе второй подход. Дело в том, что, когда ты занимаешься переведением технологического стека, ты получаешь уникальную возможность пересмотреть работу своих процессов с точки зрения автоматизации и получить новые возможности для развития за счет расширения функционала. Но даже в таких ситуациях важно соблюсти баланс: бывают заказчики, которые хотят превратить CRM в универсальную систему с огромным набором функций, большая часть которых рискует остаться невостребованной. Сейчас достаточно просто «повторить» решение «как есть у импортных поставщиков» — необходимо опередить ожидания и требования заказчиков. Недостаточно стать просто быстрым и дешевым — сейчас крайне важно быть безопасным, прогнозируемым и устойчивым решением, позволяющим не только разрешить тактическую задачу, но и заложить стратегию долгосрочного развития.

— **Как крупным компаниям, ранее внедрившим зарубежный софт, даются решения попробовать что-то новое?**

— Я периодически наблюдаю психологическую ловку менеджеров, которые успели потратить несколько миллиардов рублей на внедрение зарубежного ПО, а сейчас им нужно

найти еще несколько миллиардов на новое внедрение. Принять такое решение действительно непросто. Но так или иначе компании идут на замещение иностранных решений, понимая необходимость этого шага.

— **Какие сейчас у заказчиков требования при внедрении CRM?**

— Можно говорить о двух категориях требований: технологических и функциональных. Технологические — это наличие микросервисной архитектуры и лоукода. Сейчас это must have для любых компаний — без возможности удовлетворить такие требования на рынок даже не стоит пытаться выходить. Объясню почему: нехватка специалистов, которые будут адаптировать и дорабатывать систему, приводит к популярности решений-конструкторов. При работе с ними в меньшей степени нужны дорогие программисты и в большей степени — специалисты, хорошо знающие функциональность различных блоков системы и умеющие настроить ее под конкретного заказчика.

Еще среди популярных технологических запросов — включение в CRM-платформы инструментов искусственного интеллекта и внедрение сквозного автоматизированного процесса от предложения до заключения сделки. Согласитесь, совершенно по-другому представит ситуация, когда поставщик, у которого, например, несколько тысяч наименований металлических труб, составляет коммерческое предложение не в ручном режиме, а с использованием алгоритмов.

Команда разработок постоянно находится в поиске инструментов, которые позволят бизнесу экономить и наращивать прибыль — это сегодня основной запрос. Вторая категория требований — функциональные, и здесь все намного интереснее. Дело в том, что рынок CRM-систем исторически развивается по синусоиде.

— **В каком смысле?**

— На заре своего зарождения CRM-системы подавались заказчикам не как технология, которая встраивается в уже существующие процессы и дополняет их, а как универсальный ключ к лидерству, который позволит быстро обойти конкурентов. Затем, когда CRM получает широкое распространение, а компании устают с ним играть, такие решения воспринимаются как часть IT-ландшафта компании. Важная часть, для эффективной работы которой необходимо высокое качество менеджмента. Затем происходит функциональный или технологический скачок, и история повторяется заново. Я наблюдаю движение этой синусоиды достаточно давно.

— **Можете привести пример пика этой синусоиды?**

— Я был одним из тех, кто занимался внедрением CRM-системы в банке «Тинькофф», который уже на старте нацелился на работу с клиентами в цифре. CRM успешно внедрили, и банк получил большое преимущество перед конкурентами именно в

части понимания клиентов и работы с ними. Сейчас же мы наблюдаем как раз второй период отношения к CRM. Это обязательный и неотъемлемый продукт у любой зрелой компании. Следующий пик этой синусоиды мы увидим, когда вендоры решений смогут донести до топ-менеджеров компаний мысль о том, что у них есть некая новая технология или даже подход к использованию уже существующей, которая позволит совершить квантовый скачок.

— **А как может выглядеть этот квантовый скачок? В моем понимании в части работы с большими массивами данных о клиентах и умении таргетированно делать им предложения мы уже достигли потолка.**

— Не соглашусь. Действительно, компании обладают огромными массивами данных о клиентах, но не все умеют с ними работать. То есть обрабатывать данные настолько тонко, чтобы со своими предложениями точно попадать в потребность клиента. Потенциал этой технологии мы сейчас используем в лучшем случае на 45–50%, не больше. То есть первая очевидная точка роста сегодня — умение качественно использовать данные, а не только накапливать их. Для этого нужны аналитики, дата-сайентисты, проверка различных гипотез, проведение исследований. Расти здесь есть куда.

Вторая точка роста — это совместное использование и обогащение данных крупными игроками, что позволит сделать инструменты бизнеса эффективнее. Уже было несколько попыток организовать такую кооперацию, но они не увенчались успехом.

— **В части потенциала развития систем управления взаимоотношениями с клиентами существует, как мне кажется, проблема, которая остается нерешенной. Это настройка частоты коммуникации с клиентом в зависимости от его тревожности и раздражительности. Это может быть точкой роста, реально ли настроить такой параметр?**

— Меня давно интересует этот вопрос: можно ли тонко настроить частоту таргетированных обращений с клиентом, учитывая его психологические особенности, раздражаемость и другие сложные параметры. Это интересная задача, но пока ни одна компания далеко не продвинулась в ее решении, хотя бизнес пытается это сделать: крупнейшие вендоры нанимают аналитиков и психологов, проводят исследования на эту тему, пытаются анализировать и размечать данные с учетом возраста, социального статуса и так далее.

— **У таких исследований есть смысл?**

— С одной стороны, в истории развития каждой крупной компании наступает такой момент, когда ее топ-менеджмент теряет понимание того, как корпорация тратит деньги, а как их зарабатывает. Отсюда появляются команды и сотрудники, которые проверяют необычные гипотезы, проводят странные исследова-

ния и так далее. Но, с другой стороны, такой подход к работе позволяет крупным компаниям проверять самые смелые предположения. Девять из десяти провалятся, а одно окажется перспективным, и на его основе появится уникальный продукт.

Я думаю, что это реализуемая задача, но для ее решения нужна команда квалифицированных специалистов. — **Какие сервисы сегодня можно разрабатывать и внедрять «поверх» CRM-решения?**

— CRM — это конвейер, который позволяет бизнесу взаимодействовать с клиентами, и компании подходят к внедрению дополнительных сервисов в зависимости от задач, которые перед ними стоят. Одна из самых популярных надстроек, характерных для всех бизнесов, — это программы лояльности: они позволяют реализовать множество интересных для заказчика механик. Самый очевидный пример — это когда компании используют различные механизмы в рамках программ лояльности, чтобы получить от пользователей их данные, а взамен предоставить скидки и бонусы.

— **Мы видим, как государство ужесточает правила оборота персональных и обезличенных данных. Это может негативно сказаться на развитии подобных решений в рамках CRM-систем?**

— Здесь я не вижу рисков в части соблюдения законодательства. Новое регулирование, напротив, может создать дополнительные возможности для того, чтобы лучше узнать клиента. Мы, например, видим большие перспективы в использовании биометрических данных, регулированием оборота которых занялось государство.

Вопрос обращения с персональными данными сегодня один из самых острых. Чуть ли не ежедневно приходят сообщения об очередной утрате чувствительной и особо регулируемой информации. Конечно, задача команд разработки сегодня сделать такой IT-инструментарий, который не позволил бы специально или случайно спровоцировать утечку данных. Мы, например, включили модуль для обезличивания в свою платформу производства технологичных продуктов «Сфера». Теперь информация из рабочих систем, которая необходима для тестирования новых IT-сервисов, вне опасности, потому что с вероятностью на 97% нейросеть обнаружит ее и закодирует. Если ИИ и различные алгоритмы, контролирующие весь жизненный цикл ПО, увидят отклонения от нормы, топ-менеджмент оперативно получит тревожный сигнал о возможных правонарушениях.

— **Какие сейчас параметры рынка CRM в России?**

— Текущий объем российского рынка мы оцениваем в 20–25 млрд руб. ежегодно. Это тот бюджет, который компании вкладывают в покупку лицензий, модернизацию и сопровождение существующих систем. При этом 60% от рынка приходится на покупку и внедрение решений, 20% — развитие имеющихся систем, оставшиеся 20% — на их поддержку. — **На ваш взгляд, как в дальнейшем будет развиваться рынок CRM в России и какие факторы будут влиять на спрос?**

— Спрос на CRM будет стабильно расти за счет волнообразной потребности в импортозамещении и апдейте систем. Он будет подогреваться необходимостью перехода на отечественные платформы, на котором настаивают регуляторы.

Если говорить об экспортном потенциале, я вижу перспективы поставок в ближнее зарубежье: Беларусь, Армения, Азербайджан и особенно Узбекистан, который идет по пути цифровизации. У нас есть опыт внедрения решений для компаний в этих регионах.

Однако, выходя на эти рынки, необходимо понимать, что там нет острой необходимости замещения западных продуктов, поэтому российским компаниям придется работать в жестких рыночных условиях и предлагать лучшие по функционалу решения.

Интересная история может сложиться на развивающихся рынках: это Юго-Восточная Азия и Латинская Америка, например Мексика и Филиппины. В этих регионах сложилась благоприятная ситуация для экспорта CRM-систем. С одной стороны, есть явный интерес к решениям, позволяющим обеспечить высокое качество работы с клиентами, с другой — местные регуляторы в сфере персональных данных пока не припустили к контролю этого сегмента. К тому же как раз эти регионы восприимчивы к внедрению новых решений и сервисов.

Интервью взял Никита Королев

информационные технологии

«Российские решения могут занять до 98% рынка»

По итогам года, истекшего после начала технологических санкций, российские разработчики систем информационного моделирования говорят о кратном росте спроса на собственные продукты и видят перспективы в развитии не только на внутреннем, но и на внешних рынках. Исполнительный и технический директор АО «СиСофт Девелопмент» (CSoft Development) **Игорь Орельяна Урсуа** рассказал, „Б“, какие требования сегодня заказчики предъявляют к отечественным системам, каким образом зарубежные вендоры пытаются остаться в РФ и почему экспорт российских PLM и BIM будет расти.

— мнение —

— В каком состоянии сейчас, чуть более чем через год после начала санкций, российский рынок технологий информационного моделирования в строительстве?

— Сегодня рынок технологий информационного моделирования находится в состоянии передела. Российские компании идут по пути замены зарубежных решений, которые десятилетиями укоренились на российском рынке, на отечественное программное обеспечение. Этот процесс далеко не всегда простой. Если для малых компаний переход с решений условного Autodesk на российское ПО не большая проблема. Нужно найти средства, чтобы приобрести софт, настроить его и установить. Для больших компаний это более трудоемкий процесс. Необходимо потратить средства и время не только на закупку и настройку софта, но также и на перенос уже существующих данных в новую среду, синхронизацию решений с внутренними системами и системами заказчиков. Компаниям необходимо работать со своими партнерами в едином формате данных.

В целом текущее состояние российского рынка можно оценивать положительно: отечественные решения закрывают потребности компаний практически во всех сегментах, в том числе моделировании в гражданском строительстве, различных секторах промышленности и так далее. В ряде узких сегментов, например в химической промышленности, еще есть над чем поработать.

— Можете оценить объем рынка BIM и PLM в России?

— Я бы оценил текущий объем рынка таких решений в России в 100 млрд руб. по итогам прошлого года. Зарубежные решения традиционно занимали существенную долю. Отечественные решения в сегментах информационного моделирования в гражданском строительстве и промышленности всегда были сильными. Но крупные зарубежные компании в силу агрессивного маркетинга мешали отечественным вендорам занять интересные для них ниши. В прошлом году ситуация изменилась кардинально: иностранные поставщики ушли или по крайней мере громко заявили о своем уходе, и мы увидели большой интерес к нашему программному обеспечению. Прошлый год перевернул все и позволил глобально перезапустить

процессы развития решений в области информационного моделирования. Я уверен, что по окончании процесса замещения иностранного ПО российские решения могут занять до 98% рынка.

— Какие решения в сегменте информационного моделирования могут предложить российские разработчики?

— Давайте по порядку. В части PLM российские разработчики полностью закрывают потребности заказчиков, решения в этом сегменте в России исторически хорошо развиты. Аналогичная ситуация в BIM и ряде САПР. Существующее российское программное обеспечение для гидравлических расчетов покрывает 90% от необходимого функционала. Есть потребность в разработке решения для геотехнического моделирования — в этой области российских решений практически нет, а имеющиеся — с недостаточным функционалом. Одна из самых больших проблем — отсутствие российских решений в области моделирования химических процессов.

Российские разработчики решений за последний год сделали огромный рывок: мы в части развития за 2022 год проделали путь, на который у западных вендоров уходили годы или даже десятилетия. Мне кажется, что мы в части развития идем быстрым темпом, порой даже слишком быстрым.

— Какие отрасли наиболее активно переходят на российские решения, а какие до сих пор предпочитают так или иначе использовать западное ПО?

— Активнее всего на российский софт переходят добывающие и промышленные компании. Дело в том, что такие предприятия восприняли необходимость заместить зарубежный софт не как трагедию, а как возможность развития. Мы заключаем с партнерами соглашения, которые подразумевают не просто продажу лицензий и замену одного программного обеспечения на другое. Наше партнерство подразумевает реализацию таких функций, которые невозможно было реализовать на иностранном софте. К тому же внедрение на крупных предприятиях отечественных продуктов позволяет решить и другую проблему, которая была характерна для западного стека технологий — лоскутную цифровизацию процессов моделирования. Компании внедряли решения от разных вендоров, не добиваясь единой и сквозной авто-



предоставлено АО «СИСОФТ ДЕВЕЛОПМЕНТ»

матизации процессов. Мы в «СиСофт Девелопмент» идем по пути построения единой экосистемы на стороне заказчика, внедряя целую линейку продуктов и адаптируя их под потребности нашего партнера.

Гражданский сегмент, в первую очередь девелоперы, воспринимает возможность замещения иностранных продуктов с меньшим энтузиазмом. Здесь дело не столько в нежелании переходить с привычных зарубежных систем на российские решения, сколько в том, что миграция на отечественный софт требуется и от самого девелопера, и от его партнеров, с которыми он взаимодействует в части передачи данных. Но этот тренд скоро сменится. Дело в том, что мы в импортозамещении за последний год зашли настолько далеко, что повернуть ситуацию вспять не выйдет, даже если зарубежные поставщики решат вернуться на российский рынок.

— Какие решения необходимы заказчикам, какие требования у них к этим решениям?

— Требования разнятся. Одни компании, как правило, небольшие, ориентированы на то, чтобы отечественные решения по функционалу и интерфейсу полностью копировали западный софт, к которому они привыкли. Но эта позиция без будущего: если слепо копировать чужое, ты всегда будешь отставать. Большие компании подходят к вопросу иначе. Для них важно не просто замещение с повторением функционала, а развитие. Это куда более зрелый подход, который позволяет совершить технологический скачок. Поэтому мы в «СиСофт Девелопмент» совместно с крупными заказчиками не только поставляем решения, но и проводим НИОКР (научно-исследовательские и опытно-конструкторские работы) в интересах компаний, чтобы доработать ПО под нужды заказчика, которому нужен конкретный результат.

— Если мы говорим о внедрении на инфраструктуре большой компании российских систем моделирования, какая доля в стоимости приходится на покупку лицензий, а какая — на само внедрение?

— Большая часть цены, безусловно, приходится именно на внедрение. В любом таком контракте на покупку лицензий затрачивается, как правило, треть или даже четверть от цены контракта, иногда меньше. Все остальное — услуги по внедрению и адаптации. Я приведу пример: мы реализовывали контракт на 2 млрд руб., из него только 300–500 млн руб. пришлось на покупку лицензий.

— Как компания—поставщик решения может обеспечить клиенту бесповную и быструю миграцию при внедрении отечественных разработок?

— Для этого мы предлагаем заказчикам большой пул услуг. Речь идет о внедрении наших решений, анализе уже имеющихся данных и их переносе, синхронизации решения с уже существующим ПО внутри компании заказчика, переносе макросов и утилит, которые ранее были написаны для заказчика зарубежными вендорами. Такой подход — наше конкурентное преимущество. Дело в том, что сейчас доля компаний на рынке, которые предлагают потребителям лишь лицензии без сервисного сопровождения, снижается. Заказчикам не интересно приобретать программное обеспечение, им нужно, чтобы решение заработало на их инфраструктуре.

— Я слышал, что зарубежные вендоры подобных решений ищут способы остаться в России, наладив продажи через альтернативные каналы. На ваш взгляд, так ли это и чем грозит эта ситуация российским разработчикам?

— Это правда, сегодня зарубежные вендоры решений в области инженерного ПО охотно используют различные пути обхода санкций, чтобы не потерять российский рынок. Одна из самых популярных схем работает следующим образом: российская компания, которая хочет продолжать использовать зарубежный софт, учреждает предприятие в нейтральной стране, например в Индии, ОАЭ, Узбекистане, покупает лицензии на софт на это предприятие, а затем передает российский компании права на его ис-

пользование. По сути, это нарушение лицензионного соглашения, но поставщики ПО готовы закрывать глаза на эти нарушения, лишь бы не потерять российский рынок. Мне известны примеры, когда подобные схемы использовали достаточно крупные российские промышленные компании, хотя, признаю, это единичные случаи в этом сегменте. Хотя были и более экзотические и вызывающе случаи.

— Например?

— Мне известен случай, когда топ-менеджеры российского представительства одного из крупных зарубежных поставщиков систем информационного моделирования официально покинули компанию, учредили новое российское юридическое лицо, с согласия материнской компании получили предварительно откомпилированный исходный код программы, причем достаточно дорогостоящей с точки зрения подписки, а затем попытались попасть в реестр российского программного обеспечения Минцифры. В министерстве достаточно быстро распознали схему и отказали компании во включении в реестр.

— Как российские поставщики смотрят на эту ситуацию и какова реакция регуляторов?

— Мы стараемся купировать эти лазейки, обсуждаем риски с регуляторами, но пока не видим с их стороны активного противодействия подобным ситуациям. Зато мы видим, как крупные предприятия с помощью отраслевых лоббистов пытаются облегчить для себя условия использования зарубежных решений, поставщики которых заявили об уходе из РФ. Одна из таких попыток, безусловно, попытка легализовать пиратство.

— Какие сегодня существуют перспективы для экспорта отечественных PLM, BIM, САПР?

— Потенциал экспорта таких решений сегодня огромен. Мы получаем запросы от индийских и корейских компаний в части поставок и внедрения наших решений на их предприятиях. Высокий интерес наблюдается и у предприятий в Африке и Латинской Америке. Но в последнем макрорегионе ситуация несколько осложнена. Дело в том, что из-за того, что американские компании в связке с правительственными лоббистами внедрились в странах региона технологические стандарты и нормы, удобные западным вендорам, выход на эти рынки несколько осложнен. Иная ситуация в странах СНГ и Востока. Сегодня один из наиболее перспективных рынков для экспорта PLM и BIM — это Узбекистан. Крупные промышленные предприятия заинтересованы в российских решениях. Мы поняли это еще три года назад, когда совместно с локальным партнером начали заходить на этот рынок, продвигая собственные решения. В итоге сегодня ряд крупных промышленных проектов в Узбекистане реализуется при помощи наших решений. Я говорю об ИТ-проектах в области добычи полезных ископаемых и строительстве крупных инфраструктурных объектов. То есть нам удается вытеснить с этого рынка американских вендоров.

Интервью взял
Никита Королев

Оборудование ждет помощи

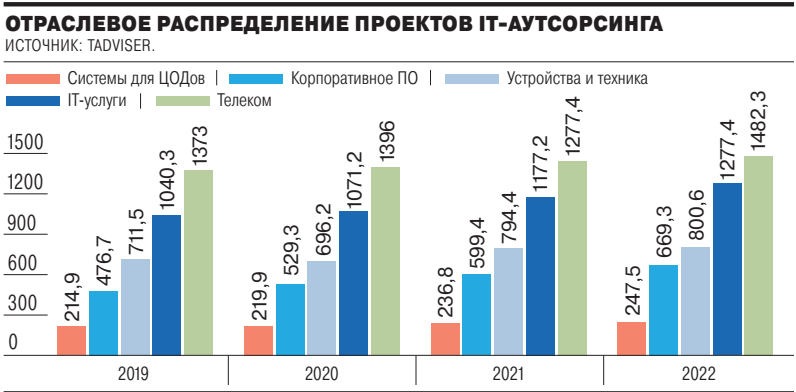
— инфраструктура —

Цена вопроса

В аутсорсинг парков оборудования, как правило, входит сопровождение и контроль его работы, предоставление инженеров под конкретные задачи клиентов, ремонт и замена «железа», интеграция с программным обеспечением, а также оптимизация затрат на поддержание работы инфраструктуры.

По данным участников рынка, за год в России стоимость услуг внешней поддержки ИТ-оборудования выросла до 40% в зависимости от класса оборудования и сложности его обслуживания. Нижний порог динамики цен аналитики оценивают в 15%, а драйвером роста стали удорожание логистики и стоимости поддержания складов запчастей, необходимых для оперативного ремонта (см. „Б“ от 22 апреля).

В целом цена техподдержки оборудования складывается из работы с дефектами «железа» и замены компонентов, причем именно замена составляет три четверти от цены услуги, рассказывает Владислав Бахаудинов. Стоимость техподдержки можно разделить на две части: поддержка вендора и интегратора. «Цена первой будет расти, так как для нее используются только оригинальные компоненты, а также требуются высококвалифицированные кадры, которые в дефиците», — говорит эксперт. Стоимость техподдержки от интегратора может даже падать, так как некоторые компании используют неоригинальные, но совместимые компоненты — китайские и уже бывшие в использовании, уточняет он. «Но при оказании таких услуг ин-



тегратор, например, привезет необходимые компоненты не завтра, а через месяц», — объясняет эксперт.

Наиболее дорогой услугой в текущих условиях стала замена комплектующих: она составляет три четверти от цены услуги, рассказывает Владислав Бахаудинов. Дороже стоят услуги компаний, позиционирующих себя вендорами «железа», то есть работающих только с оригинальными компонентами производителя. Поддержка интегратора, по словам господина Бахаудинова, обходится компаниям дешевле, так как чаще всего интеграторы работают с альтернативными компонентами из Китая или с «железом», которое уже было использовано.

Стоимость услуг сервиса и аутсорсинга растет без резких скачков, коррелируя с ростом инфляции и фонда оплаты труда, считает руководитель направления сервиса и аутсорсинга «Крока» Юрий Яновский. При этом в зависимости от размера инфраструктуры ИТ-партнеры могут предложить даже более выгодную стоимость по сравнению с тем, что предлагали производители, говорит он.

Собеседники „Б“ на ИТ-рынке объясняют, что за последний год дистрибуция комплектующих для импортного оборудования сильно изменилась: если раньше этот сегмент был поделен между крупнейшими интеграторами, работающими напрямую с зарубежными партнерами и гарантирующими как качество обслуживания, так и сроки доставки необходимых компонентов, то сейчас в этот сегмент вышло много небольших, малоизвестных компаний.

«Рынок внешнего обслуживания оборудования в РФ сейчас стремительно занимают небольшие фирмы, зарегистрированные в СНГ или других странах, которые и поднимают цены, но в то же время у небольших фирм больше возможности привезти необходимые комплектующие, и пока у заказчиков нет альтернативы, что также становится драйвером роста цен», — рассказал основатель сети дата-центров Охуген Павел Кулаков.

Переход неизбежен

Наименее зависимым от аутсорсинговой поддержки оборудования

еще с прошлого года остается госсектор, в том числе ведомственные и подведомственные структуры. Программа импортозамещения, которая была запущена правительством еще до 2022 года, стимулировала госсектор к переходу на парк российских оборудования, поддержка которого остается за отечественными вендорами.

Также более интенсивное замещение импортных парков оборудования происходит на объектах критической информационной инфраструктуры (КИИ, банки, ТЭК, операторы связи и др.). Согласно указу президента от 30 марта 2022 года №66, на объектах КИИ с 1 января 2025 года запрещается использовать и зарубежный софт, также к этому сроку компании должны реализовать миграцию на отечественное оборудование.

В других отраслях экономики переход происходит не так интенсивно, и рост спроса на аутсорсинговую поддержку уже имеющегося оборудования говорит о том, что бизнес будет по возможности продлевать срок его работы.

Многие компании предпринимают комплекс организационно-технических мер для снижения зависимости от зарубежных технологий, включающий переход на российское ПО и оборудование, соглашается Дмитрий Ретюнский. Цикл перехода, в свою очередь, обусловлен сроками, установленными государством (в первую очередь для объектов КИИ), а также средним сроком жизни технических решений (три-пять лет), объясняет он. Господин Ретюнский также отмечает, что в целом рост стоимости услуг поддержки

оборудования продолжится, «однако его размер будет сильно дифференцирован в зависимости от степени критичности задач и типов ПО и оборудования для бизнес-процессов».

Востребованность сервиса и аутсорсинга будет расти, так как это гибкие услуги, которые можно построить под требования, изменения и цели клиентов, уверен Юрий Яновский. Увеличение числа мультисекторных инфраструктур также создаст повышенный спрос на услуги у крупных ИТ-партнеров.

Если максимальный срок службы закупленного до 2022 года оборудования может составить семь лет, то российские организации будут вынуждены перейти на российские аналоги систем хранения данных, серверов, коммутаторов, промышленного и другого оборудования до 2029 года, рассуждает эксперт. Участники рынка уверены, что переход компании будут осуществлять в гибридном формате: они будут искать альтернативу импортному «железу» постепенно. На российском рынке уже есть компании, предоставляющие аналоги, альтернативой могут также стать китайские производители оборудования, которые могут в том числе предоставить комплектующие для уже работающих систем.

Но рынок аутсорсинга не перестанет расти даже на фоне усиливающегося процесса импортозамещения: компаниям будет необходимо продолжать процесс интеграции оборудования с российским софтом, отладку и тестирование новых парков, а также осуществлять контроль за работой ИТ-инфраструктуры, объясняют собеседники „Б“.

Учитывая сокращение каналов поставок через параллельный импорт, отмечает Владислав Бахаудинов, компаниям стоит рассматривать разные варианты развития ИТ-инфраструктуры: «Идти по пути импортозамещения, плановой замены оборудования на российских и китайских производителей». Это, поясняет эксперт, существенно снизит долгосрочные риски выхода систем из строя.

Переход на продукты отечественных производителей поможет решить проблему с поддержкой зарубежного оборудования, говорит директор по маркетингу и коммуникациям цифровой платформы для организации командировок и управления расходами «Ракета» Дарья Зубрицкая: «Здесь важно отметить, что ключевым вопросом может стать качество обслуживания оборудования со стороны отечественных вендоров. Западные поставщики традиционно оказывали качественную поддержку по своему оборудованию, а для сегмента enterprise это является одним из ключевых факторов при выборе поставщиков и типа оборудования».

Импортозамещение, добавляет эксперт, сможет снизить спрос на аутсорсинг поддержки оборудования в глобальном смысле только в случае, если предложения вендоров будут экономически целесообразны для бизнесов: «В противном случае может сохраниться большой процент компаний, пользующихся ресурсами аутсорсинга, поскольку в таком случае им не нужно нести затраты на смену инфраструктуры».

Татьяна Исакова

информационные технологии

«Все идет к умной дороге, автономному транспорту и нулевой смертности»

Первый квартал 2023 года продемонстрировал, что российский IT-сектор не только выстоял, но и нашел точки роста и собственные пути развития. Одной из наиболее динамично развивающихся технологий остается искусственный интеллект (ИИ). Востребованность применения таких решений растет в транспортном секторе, в том числе растет запрос на повышение безопасности на дорогах. Генеральный директор концерна «Телематика», объединяющего в своем составе десятки компаний в области интеллектуальных транспортных систем, **Алексей Нащекин** рассказал, **о** российских разработках, оснащенных искусственным интеллектом, об их внедрении на автодорогах и в ж/д транспорте, а также о повышении комфорта и безопасности водителей с помощью современных технологий.

— мнение —

— Как повлияли текущие внешние условия на развитие отечественных IT-технологий, что изменилось для вашего концерна?

— Последний год был для нас, как и для многих в стране, полон изменений. Мы ощутили сложности с поставкой комплектующих, санкционное давление, появился риск оттока персонала. Некоторое время заняла адаптация всей нашей деятельности, но нам удалось изменить цепочки поставок, внести изменения в продукты и выдержать большую часть негативных моментов. Мы открыли офис в Киргизии, стартовали новые и получили развитие наши текущие проекты на автомобильных и железных дорогах. На последних открыли новое направление по промышленной автоматике для ж/д, также в наш состав вошла компания, которая занимается системами весогабаритного контроля железных дорог. При этом хочу отдать должное нашему коллективу, именно благодаря которому получилось приспособиться к новым реалиям и открыть эти новые направления. В текущих условиях мы смогли сохранить команду наших первоклассных специалистов: инженеров, разработчиков, которые горят сво-

Россия всегда славилась сильной инженерной школой и в короткие сроки смогла создать технологии и ПО мирового уровня, которые активно применяются на наших дорогах, а в некоторых случаях даже превосходят зарубежные аналоги

им делом. И поскольку само направление интеллектуальных транспортных систем (ИТС) относительно молодой сектор, мы тесно сотрудничаем с вузами и НИИ, прикладываем усилия по развитию кадрового резерва в сфере ИТС и всегда рады видеть талантливую молодежь в рядах сотрудников концерна. — Как это отразилось на динамике выручки компании за 2022-й и какие ваши ожидания на 2023 год? — Несмотря ни на что, за счет новых направлений и новых проектов наша выручка в прошлом году практически удвоилась. Концерн показал хорошие результаты и по прибыли. На международном направлении есть трудности, в Латинской Америке у нас остановились проекты, но мы сохранили присутствие в Индии, в Индонезии, в странах СНГ — Киргизии и Узбекистане. Видим заинтересованность в наших решениях в других дружественных странах. Мы работаем с долгосрочными актуальными проектами, которые направлены на комфорт и безопасность на дорогах, улучшая экологическую обстановку, оптимизируют бизнес-процессы и снижают расходы для государства. Надеемся, что такие проекты будут дальше развиваться и в этом году мы тоже покажем положительную динамику. — Как изменились технологии, применяемые на дорогах России за последние годы? Как меняются сами дороги? — Дороги становятся быстрее, комфортнее, и это касается не только платных магистралей. Государство вкладывает большие инвестиции в развитие дорог, сильно изменились все федеральные трассы, региональные дороги, улицы в большинстве городов. Сделать их не только комфортными и быстрыми, но и умными, и более безопасными помогают технологии.

Именно на трех китах — комфорт, безопасность и экономичность — мы и опираемся при реализации наших проектов. Для этого мы поставили себе задачу и последние пять лет шли к цели разработать полностью российские платформы по всем направлениям интеллектуально-транспортных систем. К настоящему моменту мы обладаем всей линейкой продуктов с глубокой степенью локализации с точки зрения микроэлектроники и полностью отечественным программным обеспечением, которое позволяет комфортно путешествовать по стране, а грузам — быстрее перемещаться. Наш независимый отечественных стек включает десятки технологий ключевых ИТС-направлений: автоматизированную систему управления дорожным движением, современную систему платности, решение для умных дорог и подключенного транспорта V2X (vehicle-to-everything — автомобиль, подключенный ко всему. — „Ъ“) для взаимодействия автомобилей и дорожной инфраструктуры. Все эти технологии уже прошли апробацию и успешно применяются в крупнейших инфраструктурных дорожных проектах.

При этом современные технологии стали настолько совершенными, что для нас они почти не ощутимы. Например, технология «Свободный поток» (или free-flow. — „Ъ“) позволяет водителям ехать без остановок в пунктах оплаты. Сокращается время в пути, не надо останавливаться, ждать в очереди, снижается аварийность за счет отсутствия перестроений. Это уже работает на ЦКАД, на трассе М-12 и на Московском скоростном диаметре. Многие новые платные магистрали в России, как федеральные, так и региональные, проектируются как fгew-flow — это удобнее для водителей и дешевле в строительстве. В целом переход платных дорог на «Свободный поток» — это общемировая тенденция: более 40% платных дорог в мире уже без шлагбаумов. — Что касается умной части, в каком «интеллекте» нуждаются дороги и как технологии призваны помогать водителям? — Задачи интеллектуальных транспортных систем в городах отличаются от магистралей. В городах первоочередная цель — сокращение заторов. В тех агломерациях, где мы уже внедряем системы управления городским движением, пропускная способность выросла до 20% и продолжает прогрессировать. На скоростных магистралях наша задача — повышение безопасности, контроль скорости,



АЛЕКСЕЙ НАЩЕКИН

оператора из диспетчерского пункта, система сама отправляет инцидент на основе распознанного события.

Это повысит скорость информирования аварийных комиссаров, призванных помогать водителям на платных скоростных магистралях. Все это нацелено на сокращение времени реакции при происшествиях: в сложных случаях «золотые» минуты спасут жизнь, при бытовых случаях — закончился бензин, спустило колесо — это быстрая помощь и забота на дороге.

— Когда это заработает на всех дорогах? Что для этого нужно?

— По моему мнению, в горизонте десяти лет все дороги будут так или иначе оборудованы такими системами. Во всем мире движутся в этом направлении — Европа, США, Китай. Направление V2X мы считаем одним из самых перспективных с точки зрения развития комплексной ИТС-системы и предлагаем технические решения, которые при совместных усилиях с Минтрансом и автопроизводителями будут информировать в режиме реального времени о скоростных режимах, об изменении дорожной ситуации, метеорологической обстановки, предлагать маршруты объезда и тем самым сохранять человеческие жизни и экономить время. Это все является элементом работы автономного транспорта, для запуска которого в России ведется ряд важнейших государственных инициатив. В целом все усилия и развитие транспортных технологий ведут к одному: все идет к умной дороге, автономному транспорту и нулевой смертности.

— Что сейчас происходит с дорогами в городах?

— В городах также идет много проектов по модернизации дорожной инфраструктуры. В рамках федерального проекта «Безопасные качественные дороги» выделяют федеральные субсидии регионам на развитие ИТС-агломераций. Планируется, что к 2030 году интеллектуальные транспортные системы будут работать в 82 городских агломерациях. Сейчас уже 42 агломерации ведут проекты, в половине из них участвуют наши специалисты. Мы считаем это направление достаточно перспективным, поскольку это способствует увеличению пропускной способности улиц и улучшению городской среды. Первый этап — это создание базовой системы управления городским движением: интерактивные светофоры, системы фотофиксации, зеленые волны: приоритизация городского транспорта и аварийных экстренных служб. Эти проекты, думаю, в течение трех-пяти лет уже дадут существенные эффекты в городах.

В целом все усилия и развитие транспортных технологий ведут к одному: все идет к умной дороге, автономному транспорту и нулевой смертности

Применяемые здесь компьютерное зрение и искусственный интеллект обучались на десятках тысяч фотографий и видео дорожных событий, происходящих в разное время суток и при различных метеоусловиях.

Дорога также подключена к инновационной технологии V2X, которая позволяет автомобилю коммуницировать с окружающей инфраструктурой и другими транспортными средствами, в том числе с автономным транспортом. И это уже все работает: весной мы начали первый массовый пилот подключенного транспорта в Московском регионе — машины аварийных комиссаров, работающих на умной части ЦКАД, подключили к дороге. Комиссары получают в режиме реального времени сообщения о происшествиях сразу в машину на экран, не от звонка

— Распознавание происшествий на автодороге ведет нейросеть, а как они применяются на железных дорогах?

— У нас есть достаточно большой спектр решений для интеллектуальной диагностики на железных дорогах. Например, диагностические комплексы с нейронными сетями, которые полностью создают трехмерную модель подвижного ж/д состава, в автоматическом режиме анализируют на ходу все дефекты, смещение груза, нагрев, колесные пары. Тепловизоры, техновизоры, лазерные сканеры, камеры машинного зрения полностью диагностируют на ходу состояние подвижных составов и еще до прибытия на станцию выявляют потенциальные проблемы. В случае наличия каких-либо отклонений система тут же информирует сотрудников о необходи-

мости принять меры. В рамках комплексного проекта «Цифровая железнодорожная станция» обеспечивается роботизация и цифровизация всех процессов управления сортировочными станциями. Если смотреть с точки зрения эффективности, то это позволяет снизить влияние человеческого фактора за счет сокращения ручных операций и повысить производительность, и без нейронных сетей в наше время это сделать практически невозможно. Поэтому нейронная сеть, искусственный интеллект — это основа всех наших продуктов, в том числе и на ж/д.

На железной дороге реализуется достаточно большой объем задач по цифровизации, мы совместно с головным научно-технологическим институтом РЖД участвуем в создании возможно самого большого робота в мире, ведь в России самая большая протяженность железных дорог, и мы работаем над тем, чтобы все базовые операции на них были в автоматическом режиме. Это большой пласт работы, который за счет системы искусственного интеллекта и за счет роботизации и автоматизации даст эффект и увеличит пропускную способность сортировочных станций и путей. — Сколько в среднем времени и средств занимает разработка искусственного интеллекта на дорогах?

Искусственный интеллект поможет предотвратить потенциально опасные ситуации и выбрать наиболее эффективные способы управления дорожным движением, что позволит обеспечить высокий уровень безопасности и комфорта при перемещении

— Искусственный интеллект — это общее название технологии, и она применяется практически во всех наших решениях: от базового функционала при распознавании номерных знаков, определения габаритов, класса транспортного средства до сложных процессов выявления различных инцидентов и роботизированных диагностических комплексов. Например, если это камера, то разработки занимают от года. Если более сложные комплексно-диагностические системы — до пяти лет. Мы существуем на рынке уже более восьми лет, наши решения успешно эксплуатируются по всей России, но все это время мы не стоим на месте, развиваемся и дорабатываем наши системы и оборудование. Мы стараемся идти в ногу со временем, поэтому процесс развития может быть бесконечным. Также это обусловлено и сильным кадровым ресурсом, над этим всем работают наши высококвалифицированные инженеры, которые привносят свои идеи и ведут технологию к совершенству. — Это все работает с применением различных устройств и оборудования. Что смогли заместить и какие планы по локализации производства?

— На дорогах используются различные устройства: бортовое оборудование, камеры, лазерные сканеры, системы контроля, антенны, транспондеры и множество других.

Еще десять лет назад на рынке интеллектуальных транспортных систем были преимущественно иностранные решения. Сегодня ситуация кардинально изменилась. Россия всегда славилась сильной инженерной школой и в короткие сроки смогла создать технологии и ПО мирового уровня, которые активно применяются на наших дорогах, а в некоторых случаях даже превосходят зарубежные аналоги.

Большую часть устройств и компонентов, применяемых для умных магистралейных и городских трасс, нам удалось импортозаместить отечественными решениями, причем

собственной разработки: от камер фотовидеосъемки до бортовых устройств V2X. Оставшуюся часть зарубежных компонентов, а их небольшой процент, мы переориентировали на дружественные страны. Ранее компоненты и «железо» были со всего мира, теперь наши основные партнеры — это российские и азиатские компании. Помимо этого Минпромторг благодаря своей программе постоянно расширяет базу отечественной микроэлектроники, поэтому у нас увеличился значительно состав российских партнеров — поставщиков микроэлектроники, и мы стремимся к тому, чтобы локализация была максимальной. Также мы самостоятельно развиваем это направление и запускаем новую собственную производственную площадку в Подмосковье по изготовлению микроэлектроники и оборудования — расширяем производственные линии, инвестируем и локализуем практически все оборудование в России.

— Какими вы видите дороги будущего в России в перспективе десяти лет?

— Основу дорог ближайшего будущего составят умная инфраструктура и автономный транспорт. Интеллект будет у трасс федерального, регионального и местного значения. Каждая дорога будет иметь своего цифрового двойника, что позволит модели-

ровать и прогнозировать различные сценарии, происходящие на конкретном участке. Искусственный интеллект поможет предотвратить потенциально опасные ситуации и выбрать наиболее эффективные способы управления дорожным движением, что позволит обеспечить высокий уровень безопасности и комфорта при перемещении.

Проникновение подключенного и автономного транспорта станет все более заметным. В горизонте десяти лет — это скорее всего будет гибридный формат — будут и автономные машины, и автомобили, как говорится, с «белковыми» водителями. Но автономность — это не самоцель, а экономическая целесообразность и безопасность.

В целом дороги будут собой представлять единую бесшовную экосистему, непрерывно обменивающуюся информацией между водителями, пешеходами, различными видами транспорта и окружающими элементами. За счет широкого применения водителей смогут принимать важные упреждающие решения, а автономный транспорт — фактически получать команды от инфраструктуры. Глобальная цель мировой концепции снижения смертности на дорогах будет более достигаемой — жизнь как самое ценное будет в большей сохранности.

Для решения таких масштабных задач, создания прорывных технологий в науке, реализации долгосрочных проектов будущего нужны прежде всего квалифицированные кадры. Мы уверены, что привлечение в том числе молодежи привнесет новое видение в отрасль, и приглашаем к сотрудничеству вузы. Сегодня в нашей команде более 1,5 тыс. сотрудников, и у нас всегда открыты двери как для профессионалов, так и молодых перспективных специалистов, которых мы готовы развивать, инвестировать в их обучение и включать в интересные инновационные проекты динамично развивающейся отрасли.

Интервью взял Тимофей Корнев

информационные технологии

Смартфоны меняют ориентацию

Уход иностранных производителей еще в 2022 году запустил процесс трансформации российского рынка смартфонов: потребители переключились на известные и новые китайские бренды (Xiaomi, Realme, Tecno, Vivo и др.). Вместе с тем российские производители решили воспользоваться ситуацией и анонсируют выход своих устройств, произведенных в стране, среди них такие бренды, как F+, «Рутек», Yadro и др. В этот раз компании не повторяют судьбу Yota Devices и «Яндекс.Телефон», но даже при благоприятных условиях им будет трудно конкурировать с китайскими вендорами в потребительском сегменте, считают эксперты.

— оборудование —

После начала военной операции на Украине многие иностранные вендоры электроники начали ограничивать поставку своих смартфонов в РФ, среди них и лидеры российского рынка потребительских телефонов — американская Apple и южнокорейская Samsung. Кроме того, иностранные компании начали ограничивать работу своих сервисов на территории РФ и удалять приложения банков из Google Play и App Store.

На этом фоне доля бывших лидеров в сегменте смартфонов на российском рынке начала стремительно сокращаться. Так, к концу 2022 года лидером в этом сегменте стала китайская Xiaomi и ее суббренд POCO, занявшие 33% рынка в штуках. При этом доля Samsung в штуках снизилась на 51%, китайской Honor — на 47%, Huawei — на 33%, а Apple — на 45%. В то же время Tecno, Realme и Vivo, наоборот, показали наибольший темп роста продаж: спрос на Vivo увеличился на 20%, Realme — на 122%, а Tecno — на 563%. В деньгах лидером по-прежнему осталась Apple, однако и тут ее доля сокращается.. Продажи смартфонов от Apple и Samsung начали расти только у неофициальных продавцов на классифайдах «Авито» и «Юла».

В госсекторе стали предъявляться повышенные требования к безопасности систем. Так, в марте текущего года сотрудникам внутриполитического блока администрации президента (АП) было рекомендовано от-

казаться от использования смартфонов американской Apple. Тогда в АП рекомендовали перейти на смартфоны на системе Android или на системе «Ростелекома» ОС «Аврора». Незадолго до этого «Ростелеком» предлагал правительству направить около 480 млрд руб. на разработку и производство российских смартфонов на системе «Аврора»: по плану оператора к 2030 году в РФ должно было реализоваться около 70 млн отечественных устройств. Однако позже правительство начало обсуждать проект по созданию российского Android на основе открытого кода Android Open Source Project (AOSP). Среди разработчиков назывались VK, «Сбер», «Яндекс» и др. Также VK после удаления российских приложений из Google Play и App Store запустил свой маркетплейс приложений RuStore.

Помимо софта российские компании начали активно вкладываться в локализацию производства смартфонов и планшетов внутри страны. Так, в феврале основатель Национальной компьютерной корпорации Александр Калинин объявил о запуске проекта по производству розничной линейки отечественных смартфонов. В производство запланированы инвестиции в размере 10 млрд руб., а к 2026 году компания рассчитывает занять 10% рынка смартфонов. Компания Yadro (входит в ИКС холдинг) на своем сайте анонсировала выпуск планшетов на системе Android. Позже F+ tech анонсировал российский смартфон и планшет на ОС «Аврора», ко-



торый будет собираться в Калининградской области. А зеленоградский контрактный производитель электроники «Рутек» заявил о планах налаживания выпуска собственных смартфонов и планшетов на отечественной ОС «Роса» в 2023 году.

«Прежде всего изменилась геополитическая ситуация в мире и, как следствие, обострились задачи импортозамещения. В условиях ухода зарубежных вендоров необходимы гарантированные решения, обеспечивающие связь как для государственных целей, так и для повседневных нужд независимо от санкций», — заявил представитель концерна «Автоматика» (входит в госкорпорацию «Ростех»). По его мнению, в текущей ситуации российские вендоры сосредоточены на продаже устройств в корпоративном сегменте, однако при этом массовый потребитель также начинает интересоваться отечественным смартфоном. Представитель «Автоматики» считает, что российские смартфоны в скором будущем смогут занять значимую долю на отечественном рынке, однако для этого необходимо снизить цену устройств с помощью господдержки.

Одной из основных причин локализации производства российских вендоров в РФ может являться отказ Google от прямой выдачи лицензий на свои сервисы (YouTube, Google Play и др.) для китайских контрактных производств. В свою очередь, китайские компании уже начали предупреждать отечественных вендоров о возможном прекращении сотрудничества из-за американского правообладателя ПО. Из-за этого некоторые российские компании начали открывать производства в РФ, а также провозглашать себя международными организациями, чтобы обойти юридические проблемы с Google. В связи с этим по итогам первого квартала 2023 года поставки отечественных брендов смартфонов в РФ сократились с 2% общего объема импорта гаджетов до 0,1%.

«Ранее все российские смартфоны производились в Китае полностью на иностранных компонентах. Если рассматривать устройства Yota и „Яндекса“, то их смартфоны были более дорогими и при этом технологически более отсталыми по сравнению с китайскими конкурентами, поэтому эти проекты не были успешны-

ми», — рассуждает генеральный директор TelecomDaily Денис Кусков.

В конце 2010 года глава госкорпорации «Ростех» Сергей Чemezov представил тогдашнему президенту РФ Дмитрию Медведеву российский смартфон от Yota Devices. При старте производства гаджета в Китае продажи устройства не превосходили ожиданий, и в 2019 году компания обанкротилась и перешла во владение китайской China Baoli Technologies. В 2018-м «Яндекс» представил собственный смартфон — тогда эксперты считали, что компании удастся продать около 100 тыс. устройств. Однако уже через год «Яндекс» заморозил проект. Компании удалось продать всего около 18 тыс. смартфонов.

По словам господина Кускова, сейчас основная цель российских разработчиков — организация производства устройств внутри страны с локализацией компонентов в 20–25%, так как некоторые иностранные фабрики опасаются санкционного давления и отказывают в сотрудничестве: «Однако даже при таком плане существуют проблемы с импортными производственными линиями и производством компонентов».

Аналитик ФГ «Финам» Леонид Делицин считает, что российские смартфоны могут быть востребованы среди потребителей из госсектора и корпораций, где критическим является вопрос безопасности данных. Компании, производящие компьютеры, осваивают производство смартфонов с прицелом в первую очередь на госсектор, отмечает он: «Что касается потребительского рынка, то в связи с высоким уровнем конкуренции в обычных условиях требуются большой масштаб операций и высокие затраты на маркетинг». Он считает, что конкурировать с уже сформировавшимися экосистемами американских компаний на потребительском рынке сложно, поэтому отечественным компаниям необходимо сконцентрироваться на нуждах госсектора и удовлетворить их наиболее полно: «Это та рыночная ниша, которую занять можно».

Попытки производить смартфоны в России не новый тренд, они предпринимаются давно, говорит исполнительный директор F+ tech Михаил Волков. По его словам, из-за санкционного ограничения вендоры стараются локализовать производство смартфонов в РФ, но по-прежнему зависимы от иностранных компонентов. По словам господина Волкова, в России осуществляется пайка плат, поверхностный монтаж, сборка смартфонов, калибровка, прошивка, а также началось портирование российских мобильных ОС. «Сейчас российские компании разрабатывают смартфоны в основном для корпоративного сектора, так как пока не наступило время для экспериментов и нужно работать на сегмент, в котором есть деньги, а это бизнес и госсектор», — признает он, добавляя, что на данный момент конкурировать с китайскими брендами при их объемах создания пользовательских смартфонов, производственной базе и технологиях отечественные производители пока не могут. Однако исполнительный директор F+ tech считает, что через пару лет устройства на отечественных ОС будут восприниматься как стандарт, полностью замещающий и удовлетворяющий спрос — сначала на корпоративном рынке, а со временем и на потребительском.

Тимофей Корнев

ДЕРЖИТЕ НОВОСТИ ПРИ СЕБЕ

Подпишитесь на @kommersant

реклама 16+