Как трансформируется рынок систем защиты в агрессивной среде 2022 года | 15

ИТ

Тематические страницы газеты Коммерсантъ

Информационные технологии

Вторник 18 октября 2022 №193 (7394 с момента возобновления издания) kommersant.ru



17 | Можно ли внедрить 6G, минуя пятое поколение связи

20 | Как изменилось использование VPN-сервисов в РФ с начала года

21 | Что думает IT-бизнес о параллельном импорте

Доигрались

После начала военных действий на Украине и последовавших за ними финансовых и технологических санкций одним из наиболее уязвимых сегментов российского IT-рынка оказалась игровая индустрия. Российские игровые студии, традиционно сильные в разработке мобильных игр, оказались отрезанными от выплат средств из маркетплейсов, могли лишиться доступа к специализированному ПО, а также понести колоссальные репутационные риски. Эта ситуация разворачивается на фоне недавно появившегося интереса российских властей к поддержке отрасли. Игровая индустрия представляет для них интерес не только с экономической, но и с идеологической точки зрения. Как российский геймдев учится жить в новой реальности под пристальным вниманием государства?



ЮРИЙ МАРТЬЯНОВ

— гейминг —

Темные души

Для российской игровой индустрии, привыкшей работать на международном рынке и, следовательно, продавать игры через зарубежные сторы (App Store, Google Play, Steam, Epic Games Store), 24 февраля стало началом исхода из России. Крупнейшие игровые студии, которые держали в стране собственные офисы разработки, одна за одной начали сворачивать бизнес в стране. В начале апреля о прекращении работы в России и Белоруссии объявила Wargaming (разработчик игр World of Tanks, World of Warships). Местный бизнес компания передала под управление Lesta Studio. «Мы ожидаем, что понесем существенные убытки в результате этого решения»,— говорится в официальном заявлении Wargaming. Впрочем, проблемы Wargaming касались не только бизнес-процессов, но и безопасности сотен сотрудников, работавших в киевской студии компании.

«В начале этих событий бизнес-вопросы практически не обсуждались — главной задачей было эвакуировать наших сотрудников из Киева. Когда мы решили этот вопрос, уже начали думать о том, что вообще делать дальше»,— говорит один из сотрудников компании на условиях анонимности. По его словам, основные проблемы в работе российских студий Wargaming были связаны с трансакциями средств. «Технически деньги и в Россию, и из России можно провести, но для европейских банков это всегда очень плохой знак. Я знаю случаи, когда их представители приходили в компании и говорили: „Почему вам поступают средства из России? Вы понимаете, что мы имеем полное право заблокировать ваши счета?“ Работа в таких условиях — это большой риск для бизнес-процессов всей компании, поэтому закрыть проекты в России — это неизбежный шаг»,— продолжает он, добавляя, что все российские разработчики уже к началу марта понимали, что продолжать бизнес в стране будет невозможно. «В индустрии не поднимался вопрос, ударят ли по всем нам санкциями — все мы взрослые люди и прекрасно понимали, что однозначно ударят. Вопрос был лишь в том, когда и как»,— заключает он.

Wargaming — один из немногих разработчиков, свернувших российский бизнес публично. Уход же большей части студий из России зачастую был неожиданным даже для их сотрудников. В один день, 14 июня, в базе данных «СПАРК-Интерфакс» появилось два идентичных сообщения: заявления о собственной ликвидации направили два отечественных разработчика мобильных игр. Это краснодарский Plarium (Raid: Shadow Legends, Vikings: War of Clans) и Game Insight (Paradise Island 2, «Аэропорт-Сити»). Совокупно в компаниях работало около 1 тыс. сотрудников.

По словам одного из разработчиков Game Insight, 10 июня ряд сотрудников получил на корпоративную почту письмо с предложением подписать заявление об уходе из Game Insight и начале работы в новой неизвестной компании. «Многие отказались, и уже 13 июня мы узнали, что компания будет ликвидирована. С нами связался некий Павел Седов, который представился ликвидатором юрлица, и сказал, что компания просуществует до 15 сентября, а потом мы все будем автоматически уволены»,— рассказывает собеседник „Ъ“. Он добавляет, что господин Седов уговаривал ряд сотрудников подписать заявление об увольнении по соглашению сторон, в рамках которого компания не гарантировала выплату зарплаты. Однако ликвидатор заявил „Ъ“, что сам в процессе ревизии активов обнаружил, что на счетах предприятия недостаточно средств для погашения зарплат. Головная структура студии, находящаяся в Литве, отказывается перечислять средства на выплату зарплат сотрудникам, ссылаясь на санкционное законодательство страны.

Впрочем, военная операция на Украине и последовавшие за ней санкции не только привели к уходу с рынка уже работающих студий, но и поставили крест на так и не начавшихся проектах. В начале июня «Сбер» сообщил „Ъ“ о ликвидации своего игрового подразделения SberGames (ООО «Сбергеймз»). Компания была основана в 2021 году и планировала сфокусироваться на разработке мобильных игр.

На конец 2021 года убыток «Сбергеймз», по данным «СПАРК-Интерфакс», составил 345,4 млн руб., при этом компания не выпустила ни одной игры. Одной из причин закрытия проекта, говорят источники „Ъ“, стало то, что SberGames, как аффилированная с попавшим под санкции «Сбером» структура, не сможет продавать свои игры через крупнейшие маркетплейсы App Store и Google Play — к тому моменту они уже удалили мобильные приложения банка. В связи с внешними ограничениями для российских разработчиков на мировом рынке «Сбер» принял решение закрыть игровое направление, добавил представитель банка.

«Насколько я знаю, из игрового подразделения „Сбера“ на рынок вышло около 200 человек, всего же за июнь—август после закрытия студий на рынке оказалось где-то 2–3 тыс. специалистов,— говорит собеседник на рынке игровой разработки.— Часть из них влилась в российские студии, которые испытывали кадровый голод, другая — уехала за рубеж или ушла в новую сферу. Например, есть несколько игровых стартапов, которые ведут активный наем людей с обязательной релокацией в Грузию, Узбекистан и Казахстан. С другой стороны, часть разработчиков, особенно из числа художников, оказалась довольно востребованной и в геймдеве недружественных стран». Возглавлявшая игровое направление «Сбера» Алиса Чумаченко отказалась отвечать на вопросы „Ъ“.

Чиновники вцепились в джойстик

Российский рынок игровой разработки начало лихорадить как раз тогда, когда государство всерьез заинтересовалось поддержкой сегмента. По словам источника „Ъ“ в крупной русскоязычной игровой студии, впервые госструктуры стали проявлять интерес к сфере гейминга в 2019–2020 годах, причем было сразу два вектора поддержки: Минцифры, которое было сконцентрировано на помощи отрасли с точки зрения бизнеса и технологий, и администрация президента (АП), которой было интересно использовать видеоигры как способ продвигать определенную повестку. Сама же игровая индустрия отнеслась к такому интересу к себе настороженно.

«До этого мы видели только разовые инициативы депутатов, которые после каждого скулшуттинга кричали, что игры нужно запретить,— рассказывает собеседник „Ъ“, близкий к Минцифры и участвовавший в обсуждении ряда отраслевых инициатив.— В 2020 году ситуация стала меняться. Например, правительство Москвы пообещало поддержать разработчиков выплатами и налоговыми льготами, если они интегрируют в игры московские локации. Сами разработчики отвечали на такие предложения, как правило, вежливыми отказами и просьбами не лезть в то, что и так хорошо работает».

Собеседник добавляет, что особенный интерес к поддержке игр власти проявили в 2021 году: тогда обсуждались идеи создать фонд поддержки разработчиков, а аналитический центр Роскомнадзора выпустил доклад о развитии индустрии. «Тогда я понял, что государство заинтересовалось играми всерьез и перешло от популизма к действиям»,— говорит он.

Минцифры обсуждало концепцию фонда поддержки российских разработчиков видеоигр с конца прошлого года. Федеральный чиновник в беседе с „Ъ“ при этом уверял, что «никто не говорит ни о какой идеологии», а целью работы фонда должна была стать помощь независимым отечественным разработчикам. Однако после 24 февраля, как говорит собеседник „Ъ“, близкий к правительству, идея создания такого фонда была заморожена и, скорее всего, не получит дальнейшего развития.

Один из лоббистов индустрии добавляет, что интерес к разработке механизмов поддержки отрасли выразили АП, а именно управление по развитию информационно-телекоммуникационных технологий, которое возглавляет Татьяна Матвеева, и Институт развития интернета (ИРИ). «Для них игры — это новые медиа, которые пусть и не сегодня, но потенциально в будущем станут способом транслировать нужную повестку»,— говорит он.

Источники „Ъ“, близкие к одному из профильных управлений АП, поддерживают этот тезис: по их словам, впервые власти задумались об играх как о способе продвигать новые смыслы в 2019 году, когда происходил перезапуск ИРИ. «Тогда все пришли к пониманию, что игры — это наиболее важный канал коммуникации с молодежью и речь здесь идет не о топорной пропаганде и ура-патриотизме, а скорее о популяризации российской культуры и истории»,— говорит один из источников „Ъ“ и добавляет, что эту инициативу активно продвигал нынешний глава ИРИ Алексей Гореславский, убеждая ряд высокопоставленных сотрудников АП в необходимости системно поддерживать сегмент.

Впрочем, сам господин Гореславский намного аккуратнее рассуждает о своей роли в формировании госполитики по отношению к игровой индустрии. «Неверно говорить, что я кого-то убедил. Еще в 2019 году и у нас, и у правительства было понимание того, что заниматься этим направлением однозначно нужно»,— говорит он, впрочем добавляя, что интерес разработчиков к господдержке в 2022 году кратно вырос: если в прошлом году грант ИРИ запросили 50 проектов, а средства получили 4, то уже сейчас грант хотят получить на реализацию около 300 проектов в сегменте видеоигр, средства же выделят на 10–15 игр.

«У отрасли есть другая проблема: в России исторически нет ведомства, которое бы отвечало за ее поддержку. Минцифры — это больше про инфраструктуру и технологии, Минкульт — про контент. Рынок жил сам по себе, сейчас же задача — помочь ему системно развиваться. Это необходимо потому, что предложение части игр ушло, а спрос никуда не делся, и сейчас этот спрос нужно удовлетворять»,— резюмирует он.

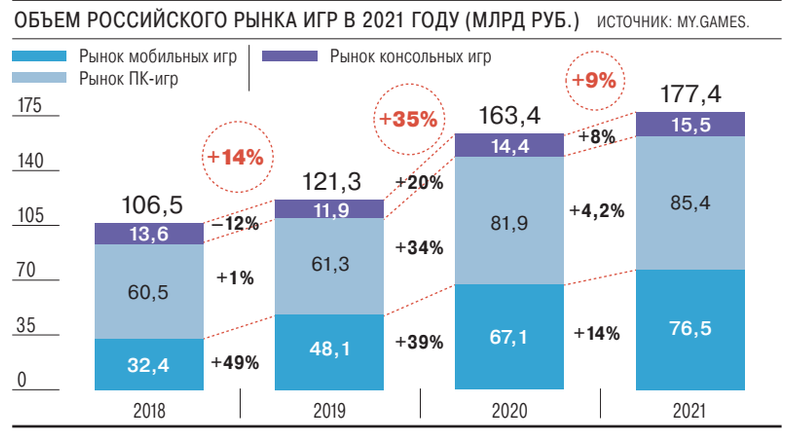
Игры в новой реальности

Несмотря на то что спрос россиян на покупку видеоигр действительно не упал, приобрести их становится все сложнее. С марта геймеры стали испытывать трудности с оплатой покупок в крупнейших сторах, например Steam. К тому же ряд крупных игровых студий, среди которых Creative Assemble (линейка Total War) и CD Projekt Red (линейка Witcher и Cyberpunk 2077), прекратили продажу продуктов в российском регионе. Трудности испытывают и владельцы консолей, например PlayStation: японская Sony ограничила продажу игр в своих цифровых магазинах.

Однако россияне нашли способ обходить запреты с помощью посредников, которые создают Steam-аккаунты из другой страны, например Турции, и под заказ российских геймеров закупают на эти аккаунты недоступные в России игры. Владельцы консолей, в свою очередь, также научились регистрировать аккаунты из других стран и оплачивать покупки через международные платежные сервисы — эти предложения уже несколько месяцев пользуются спросом у россиян. В частности, по данным TelecomDaily, число опубликованных на Avito объявлений с предложением оформить подписку и покупку контента на игровых сервисах за второй квартал выросло на 11% по сравнению с первым. Спрос на такие услуги увеличился на 24%.

с15

ОБЪЕМ РОССИЙСКОГО РЫНКА ИГР В 2021 ГОДУ (МЛРД РУБ.) ИСТОЧНИК: MY.GAMES.



Директивы из дата-центра

— экспертное мнение —

Директор по продажам Linxdatacenter РОМАН ШУЛИМОВ — о ключевых трендах на рынке услуг дата-центров на осень 2022 года

Дефицит предложения

Ситуация на рынке сейчас определяется дефицитом качественного предложения ресурсов ЦОДов в главных национальных хабах — Москве и Петербурге. Сложности с поиском локации и резервированием мощностей электроэнергии дополняются потерей доступа к инженерному и IT-оборудованию, что замедляет процесс запуска новых дата-центров еще сильнее. В регионах ситуация похожа, причем несмотря на меньшие объемы спроса. Сказываются удаленность локаций от основных маршрутов магистральных каналов связи, меньшие размеры пула потенциальных клиентов и ограниченные ресурсы инженерных сетей для обеспечения жизнедеятельности ЦОДов. Также общая для страны проблема с оборудованием усиливается в регионах скромными кадровыми возможностями для обеспечения дата-центров.



Рост цен неизбежен

Спрос на ресурсы ЦОДов растет стабильно на протяжении последних лет, и события 2022 года его практически не затормозили. Темпы прироста предложения снизились вдвое — с 10% до 5% — под влиянием кредитов, дефицита оборудования, а также традиционных факторов, сдерживающих рынок (тренд номер один). Создается ощутимый дисбаланс между главными рыночными константами, что позволяет предрекать рост цен на colocation и IaaS выше, чем привычные 10–15% в год. Затраты будут заложены в цену стоек, которые появятся на рынке в 2024 году.

Прогноз: мы увидим рост цен на эти услуги на 20–25%.

Скупают все, спешите занять очередь

В результате отставания предложения от спроса почти все новые ЦОДы оказываются распроданными еще на этапе ввода в эксплуатацию. Если вводится 100 стоек на новой площадке, то они будут распроданы полностью примерно за полгода. Если клиенту необходим целый машзал, то лучше планировать такие потребности примерно за два года и резервировать мощности у провайдера на этапе проектирования дата-центра. Иначе практически на 100% вероятно, что компания останется без IT-ресурсов. Никакой переплатой провайдеру и перекрытием рыночной цены «за срочность» вопрос объективного дефицита вычислительных мощностей решить сегодня не получится.

Открытость планов провайдеров

Раньше провайдеры услуг ЦОДов неохотно делились планами по развитию бизнеса: анонсы запуска новых площадок откладывались до последнего момента из-за коммерческой тайны, желания опередить конкурентов и т. д.

Но ситуация в корне поменялась: делиться планами по развитию ЦОДов, будь то создание крупных дата-центров, строительство небольших площадок в разных точках страны для развития облачной платформы или аренда мощностей у других провайдеров, стало новой приметой времени на рынке. Это делается для привлечения клиентов на ранней стадии реализации проекта, что особенно актуально в ситуации, когда спрос опережает предложение и мощности активно резервируют заранее, «на этапе котлована», в том числе в регионах.

Параллельный импорт: временный симптом

Дефицит носит системный характер: не только провайдеры, но и клиенты жалуются на сложности с поиском оборудования и подбором ПО. Пока в качестве решения используется параллельный (серый) импорт. Но все понимают, что это временное решение. Неизбежна смена вендоров на долгосрочную перспективу.

Из положительных последствий — вероятный всплеск развития российских производителей ПО и «железа» в средне- и долгосрочной перспективах. Многое будет зависеть от господдержки: целевое льготное финансирование на прозрачных условиях, забота о кадрах, поощрение спроса на российские разработки. Прорыв возможен только через коллективные усилия.

Спрос на российские разработки есть, и он растет: крупный и средний бизнес не сокращает IT-потребности. По оптимистичным прогнозам, за три-четыре года рынок адаптируется к новым условиям, а через восемь-десять лет — полностью восстановится и начнет функционировать в привычном режиме.

информационные технологии

positive technologies

Баг на длинную дистанцию

Нанять независимых «белых хакеров» для защиты бизнеса — в целом новый опыт для большинства российских компаний. Впрочем, в мировой практике и во многих российских публичных многопользовательских сервисах — банках, интернет-магазинах, IT-компаниях — это уже стало нормой. Объективно и достоверно оценить защиту бизнеса и сформировать доверие к новым продуктам и сервисам помогают программы Bug Bounty («охота за багами»). В ходе них компании выплачивают вознаграждение «белым хакерам» за найденные уязвимости в их информационных системах, сервисах или приложениях. Во сколько они могут обойтись заказчикам, какие есть способы для оценки Bug Bounty и какой сервис предлагают платформы-агрегаторы по поиску дыр в IT-контуре?


GETTYIMAGES

— ликбез —

Зарубежные агрегаторы Bug Bounty объединяют тысячи компаний — к примеру, только на платформе HackerOne опубликовано около 4 тыс. программ. Взаимодействуют с исследователями безопасности (багхантерами) и отечественные компании с сильными IT-подразделениями: на начало текущего года около 30 компаний из России имели свои программы по «отлову» уязвимостей, среди них: «Яндекс», Ozon, «Тинькофф», Wildberries и другие.

В среднем за найденную уязвимость такие программы платят от $50, стоимость же критической уязвимости на HackerOne в 2021 году составила $3 тыс. В отдельных случаях сумма может быть значительно выше: совсем недавно за найденную уязвимость в Instagram компания Meta (Meta и соцсети компании Facebook и Instagram признаны экстремистскими и запрещены в РФ) заплатила исследователю $49,5 тыс., или почти 3 млн руб., а российская VK готова платить за найденную уязвимость критического уровня опасности до 1,8 млн руб.

Весной зарубежные агрегаторы Bug Bounty отказались работать с российскими компаниями и исследователями, но в России уже появились собственные платформы: The Standoff 365 Bug Bounty (standoff365.com) от Positive Technologies, bugbounty.ru, BI.Zone Bug Bounty. На них переходят как работавшие ранее на иностранных платформах компании, так и новые заказчики, чья зрелость в области кибербезопасности возросла. Одни платформы сосредоточены на копировании западного функционала, другие привносят новые возможности, которых нет ни в одном международном агрегаторе. Например, на The Standoff 365 исследователям предлагается не только находить уязвимости в продуктах и сервисах, но и демонстрировать пути к реализации недопустимых событий целиком — иными словами, показывать, что могло бы произойти, если бы уязвимость не была обнаружена. Это позволяет обращать внимание заинтересованных пользователей на бреши в безопасности, которые могут привести к остановке бизнеса.

Компания, которая только начинает осваивать практику Bug Bounty, сразу сталкивается с рядом вопросов. Как грамотно оценить проект? Как не «слить» напрасно весь бюджет и получить максимальный эффект от взаимодействия с багхантерами? Об этом сотрудники Positive Technologies поговорили с руководителями служб информационной безопасности компаний, имеющих большой опыт в запуске подобных программ.

Сюрприз из пентеста

Пожалуй, самым быстрым способом оценить стоимость программы Bug Bounty станет экспертная оценка стоимости пентеста. Пентест, или тестирование на проникновение,— комплекс мер, которые имитируют реальную атаку на сеть или приложение, его цель — понять, может ли гипотетический злоумышленник взломать систему. Для этого «белые хакеры» сами пытаются ее взломать или получить контроль над данными. Такой тест проводится непублично, а его цели могут совпадать с ожиданиями от Bug Bounty: найти уязвимые места и пробить систему защиты сервиса.

Именно так поступила на запуске Bug Bounty «Азбука вкуса» в 2020 году. «Перед публичным запуском программы мы обратились в ряд российских компаний для оценки защищенности в режиме „черного ящика“ (заключаются в проведении работ по анализу и оценке защищенности без каких-либо исходных данных, кроме его адреса.— **„Ъ“**),— рассказывает технический директор „Азбуки вкуса“ Дмитрий Кузеванов.— В оценку вошли домены av.ru, azbukavkusa.ru, сервисы в беспроводных сетях „Азбуки вкуса“. Получив несколько разных оценок, на программу Bug Bounty в итоге заложили сумму, аналогичную оценке одного из сильнейших игроков на рынке пентеста».

Как любой другой подход, этот обладает своими преимуществами и недостатками. К числу первых относится то, что он подходит для новых на рынке продуктов и сервисов, а также его скорость и простота. К недостаткам же подхода стоит отнести его невысокую точность: компании оценивают сложность работ и объем задачи, но не ущерб от реализуемых бизнес-рисков.

Критический уровень

Критические уязвимости в Bug Bounty оцениваются наиболее высоко, именно за них компании платят сотни тысяч и даже миллионы рублей. Такие уязвимости больше всего влияют на бизнес и могут наделать много шума, если будут проданы на черном рынке. Например, атака шифровальщика на американскую трубопроводную компанию Colonial Pipeline в 2021 году привела к введению чрезвычайного положения в 17 штатах. За восстановление доступа к компьютерной сети компания заплатила хакерам выкуп $5 млн, сообщало Bloomberg со ссылкой на источники. Это произошло 7 мая 2021 года — в день кибератаки, которая привела к приостановке работы трубопровода. Но происходит такое нечасто: на одну критическую уязвимость приходятся десятки или даже сотни уязвимостей низкого и среднего уровня.

Компании, которые назначают стоимость критической уязвимости исходя из оценки потенциального ущерба, могут оценить стоимость выплат «белым хакерам» по программе Bug Bounty за первый год как 20–30 стоимостей критических уязвимостей. «При оценке бюджета мы стараемся заложить максимальную сумму — обычно это 15–20 критичных уязвимостей,— рассуждает директор по кибербезопасности Rambler & Co Евгений Руденко.— Однако это наша собственная формула расчета, которая учитывает предварительный динамический аудит и регулярное автоматическое сканирование, например, DAST-решением (от англ. „dynamic application security testing“ — „динамическое тестирование безопасности приложений“; автоматическое сканирование, которое имитирует вредоносные внешние атаки с попытками эксплуатации распространенных уязвимостей, задача — обнаружить незапланированные результаты раньше, чем это сделают злоумышленники.— **„Ъ“**). Таким образом можно отсеять большинство простых уязвимостей и не платить за них деньги».

Это значит, что такой способ подойдет, только если вы регулярно анализируете защищенность альтернативными инструментами и уверены, что багхантеры не принесут огромное количество уязвимостей низкой критичности, которые съедят весь бюджет. Плюсы подхода в том, что он подходит для давно существующих сервисов и продуктов, также это просто и быстро, а минусы: он подходит только для компаний с выстроенными процессами автоматического и ручного анализа защищенности.

Поэтапная разбивка

Управление уязвимостями в любой компании состоит из нескольких частей: выявления брешей, приоритизация и контроль их устранения. В зависимости от зрелости этого процесса искать уязвимости можно автоматизированно, с помощью коммерческих и open source решений, а также используя пентесты или открытое сообщество исследователей безопасности (Bug Bounty). На российском рынке встречаются разные варианты.

По словам вице-президента и директора по информационной безопасности VK Алексея Волкова, компания уже более девяти лет практикует взаимодействие с независимыми исследователями безопасности посредством Bug Bounty: «Мы применяем различные инструменты, чтобы укрепить киберзащиту, и давно используем Bug Bounty для проверки качества наших сервисов, видим в этом реальную, практическую пользу». С 2013 года, продолжает он, VK получила более 15 тыс. отчетов, что позволило «усилить защиту данных пользователей и исправить уязвимые места». Всего за время действия программы на выплаты было направлено более 185 млн руб.

Размер выплат по программе Bug Bounty напрямую зависит от того, насколько успешно компания работает с другими инструментами поиска уязвимостей. Процедура строится по принципу слоеного пирога. В его основе — автоматический анализ сканером уязвимостей. В результате анализа вы получите большое количество уязвимостей, без знания которых запускать Bug Bounty нет смысла: самые хитрые хакеры в первую очередь «натравят» сканер на вашу инфраструктуру, а регулярно платить за каждый неустановленный патч исследователям будет куда дороже, чем купить сканер.

Затем следует пентест. Если продолжать аналогию с пирогом, это «начинка», самая «вкусная» часть, которая помогает найти как точки проникновения в инфраструктуру, так и более глубокие проблемы в архитектуре, настройках и работе с IT-инфраструктурой вплоть до оценки возможности реализации недопустимых для компании событий. Пентест проводят исследователи безопасности, и обычно он связан с жизненным циклом продукта или сервиса. Наибольший эффект компания получает на этапе запуска нового продукта или обновления, получая усредненную оценку его защищенности. Клиент при этом платит за факт проведения такого рода тестирования, а не за полученный результат.

Наконец, Bug Bounty — непрерывный процесс исследования защищенности на всех этапах жизненного цикла продукта. В этом формате исследователи разного уровня будут присылать уязвимости различной критичности и ожидать оперативного подтверждения и выплат. Важно, что в случае Bug Bounty клиент платит только за результат, сколько бы времени багхантер ни потратил на поиски уязвимости. Это позволяет значительно экономить. Однако если в компании не выстроен процесс работы с уязвимостями с помощью автоматических сканеров, а новые релизы не проверяются пентестерами, высоки шансы просто «слить» бюджет на поиск дырок: багхантеры будут приносить отчеты об уязвимостях пачками, а закрыть их вы не успеете.

В ряде случаев бизнес использует Bug Bounty как экономичную альтернативу пентесту: «Bug Bounty при той же эффективности может быть выгоднее пентеста и по бюджету, и по формату,— считает Евгений Руденко.— В программе может одновременно участвовать огромное количество специалистов: ни один подрядчик не предложит такого разнообразия хакеров с разными профильными знаниями. Платит компания при этом только за фактически найденные уязвимости, а не за факт поиска».

Таким образом, если резюмировать: в компаниях с выстроенным процессом управления уязвимостями (vulnerability management) уже есть понимание влияния уязвимостей разной критичности на бизнес, поэтому бюджет на Bug Bounty можно рассчитать как 30–50% от суммарных затрат на автоматическое выявление уязвимостей и проведение пентестов.

К преимуществам этого метода можно отнести то, что процессы нетрудно наладить, а работа с уязвимостями Bug Bounty сразу интегрируется в общее управление уязвимостями. К тому же он лучше всего подойдет для оценки вывода дополнительных сервисов и продуктов в Bug Bounty. Изъянами же можно считать то, что такой подход чреват все еще низкой точностью, к тому же он не подойдет для компаний с только строящимися процессами управления уязвимостями.

Оценка step by step

Менее быстрый, но последовательный способ оценить стоимость Bug Bounty для компании заключается в постепенном открытии программы все большему числу исследователей с параллельным управлением стоимостью уязвимостей.

Например, на первом этапе можно реализовать закрытую программу Bug Bounty, отобрав для участия в ней наиболее сильных багхантеров. Выплаты для них обычно ставятся выше рынка, чтобы привлечь максимальный интерес специалистов за короткий период. По результатам этапа компании нужно оценить, во-первых, сколько отчетов и какого уровня критичности уязвимости были найдены, а во-вторых, сколько времени уходит на обработку отчетов и исправление уязвимостей.

Опытные исследователи обычно приносят небольшое количество уязвимостей, но их критичность довольно высока. Это нормально: на следующем этапе этот показатель значительно снизится. Однако если багхантеры на закрытом исследовании приносят множество уязвимостей низкой и средней критичности, компании стоит повременить с запуском открытой программы и усилить внутренние процессы поиска и устранения уязвимостей. Если этого не сделать, можно потратить бюджет очень быстро. На этот этап можно выделить бюджет в размере пяти-десяти критических уязвимостей, закрыв его по истечении срока (один-три месяца) или по окончании бюджета.

После проведения закрытого этапа компания может приступить к открытой публикации программы. Стоимость уязвимостей вначале может быть в три-пять раз ниже рынка: после первой волны интереса привлечь багхантера к программе можно, постепенно повышая выплаты и к концу года делая их выше рынка. Общая же сумма выплат за месяц в открытой и закрытой программе может быть близка.

Чтобы оценить годовую стоимость проекта, необходимо посчитать стоимость закрытой программы как среднюю за период и продлить ее на год. Например, если бюджет на нее закончился через 3 месяца, то за год (12 месяцев) общий бюджет на Bug Bounty можно рассчитать, как четыре стоимости закрытой программы.

Такой подход позволяет оценить сразу не только бюджет (причем точнее, чем у других способов), но и процессы управления уязвимостями как для новых, так и для давно существующих сервисов. Впрочем, и длится он дольше других.

«Бюджетные» маневры

Запуск Bug Bounty не обходится без принятия решения о справедливой стоимости уязвимости. Важно соблюсти баланс: при слишком высоких вознаграждениях опять же есть риск исчерпать бюджет на самом старте, а при низких — не привлечь исследователей и не достичь целей программы.

При этом стоимость одного и того же типа уязвимости может отличаться в тысячи раз для разных сервисов: уязвимость произвольного исполнения кода в сайте-визитке может привести к дефейсу сайта (то есть к его взлому, при котором главная, как правило, страница заменяется на другую — обычно вызывающего вида) и репутационным издержкам, а в платежном сервисе — к краже денег клиентов и потере доверия клиентов к компании.

Оценивать нужно двумя способами: с помощью анализа конкурентов и стоимости недопустимых событий. Например, в Positive Technologies проанализировали, сколько российские компании готовы платить за найденные уязвимости: уязвимости низкой критичности стоят до 34 тыс. руб., средней критичности — до 116 тыс. руб., критические — в среднем 393 тыс. руб. Это средние по рынку показатели. Клиенты платформы The Standoff 365 Bug Bounty, в свою очередь, ориентируются на стоимость уязвимостей у прямых конкурентов, ведь здесь и влияние на бизнес будет максимально схожим, и в программу придут исследователи со схожей специализацией.

По словам директора экспертного центра безопасности Positive Technologies (PT Expert Security Center) Алексея Новикова, оперировать только средними ценами на рынке недостаточно: важно учесть потенциальный ущерб от уязвимости, то есть стоимость реализации недопустимого события. «Если это событие может привести к остановке бизнеса, отчет багхантера конкретно для этой компании о последовательном наборе действий, включая уязвимость, ее эксплуатацию, повышение привилегий, может оцениваться значительно выше конкурентов,— продолжает он.— Сегодня немногие платформы работают с отчетами о полной цепочке атаки, однако именно подход на основе реализации наиболее критичных для компании рисков значительно повышает бизнес-ценность программ Bug Bounty».

Из чего состоит бюджет

Стоимость программы Bug Bounty складывается из следующих компонентов: выплаты багхантерам, стоимость закрытия найденных уязвимостей и привлечение исследователей на программу (маркетинг). О выплатах багхантерам говорили выше, а стоимость закрытия уязвимостей полностью зависит от сервиса и его бизнес-процессов.

Неочевидной денежной нагрузкой для компании, которая только планирует запуск Bug Bounty, может стать построение взаимоотношений с багхантерами и привлечение их интереса к программе. Общение с багхантерами, анализ отчетов (иногда багхантер присылает «пачку» уязвимостей, которые увидел сканером), проведение выплат — задача для целого отдела. В то же время компании необходимо найти каналы коммуникаций с хакерами, рассказать им о своей программе, заинтересовать и постоянно напоминать о себе — по сути, выстроить полноценную PR-кампанию проекта. Чтобы не заниматься этим самостоятельно, существуют платформы-агрегаторы Bug Bounty. За определенную часть от стоимости выплат они возьмут на себя весь пул задач по взаимодействию с хакерским сообществом и привлечению исследователей.

Например, The Standoff 365 Bug Bounty предлагает заказчикам полный комплекс работ по взаимодействию с багхантерами: от публикации программы на платформе до предпроверки отчетов, проведения выплат и привлечения сотен исследователей с профильным опытом.

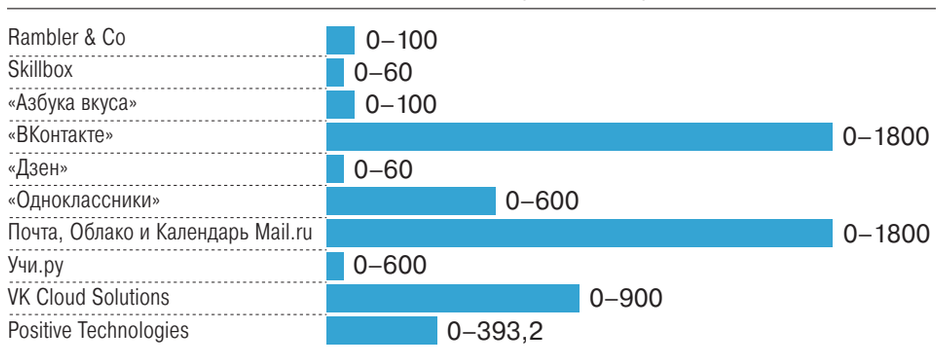
«Positive Technologies имеет большой опыт работы в индустрии кибербезопасности, авторитет в сообществе и одну из сильнейших на рынке экспертиз, что является дополнительной гарантией в привлечении специалистов и решении возможных спорных ситуаций,— объясняет Евгений Руденко из Rambler & Co.— На отечественном рынке платформа The Standoff 365 Bug Bounty выглядит наиболее зрелым решением, поэтому от участия в программе мы ожидаем вовлечения большого числа „белых хакеров“, сильной экспертизы и, как следствие, дополнительного повышения уровня защищенности наших проектов и сервисов».

Резюме

Найти единый и подходящий для всех способ оценки бюджета на программу Bug Bounty непросто: в зависимости от зрелости процессов управления безопасностью и критичности сервисов для бизнеса, новизны и частоты обновления продукта стоимость двух разных сервисов для одной и той же компании может отличаться в разы. Каждый из вышеперечисленных вариантов не раз опробован различными компаниями и доказал свою эффективность для них. Оценка бюджета — необходимый и важный этап запуска Bug Bounty, если решение взаимодействовать с багхантерами и открыто и доверительно работать над повышением безопасности своих клиентов принято. А это значит, что первый, но самый важный шаг уже сделан.

Александр Якушев

РАЗМЕРЫ ВОЗНАГРАЖДЕНИЙ ПО ПРОГРАММАМ BUG BOUNTY НА ОНЛАЙН-ПЛАТФОРМЕ THE STANDOFF 365 (ТЫС. РУБ.) ИСТОЧНИК: THE STANDOFF 365.



информационные технологии

ЦИФРОВОЙ ЭКОНОМИКИ

«Все больше российских компаний усиливают меры защиты»

К 2026 году российский рынок информационной безопасности (ИБ) может вырасти сразу в 2,5 раза — со 186 млрд до 469 млрд руб.— с учетом влияния геополитических факторов, прогнозировал фонд «Центр стратегических разработок» (ЦСР). В блицинтервью директор практики ИБ Лиги Цифровой Экономики **Денис Ковалев** рассуждает о предпосылках такого роста и влиянии геополитики на рынок кибербезопасности.



— блиц —

— Справедливы ли оценки ЦСР, по вашему мнению?

— Солидарен с мнением, что рынок в России будет расти. Для этого сложились все предпосылки. Значительно растет число кибератак на органы власти, бизнес и промышленные предприятия нашей страны. Ужесточается законодательство в сфере защиты информации. Введен запрет на закупку зарубежного ПО для значимых объектов критической информационной инфраструктуры. Наконец, уходят иностранные вендоры. Вместе с поддержкой государства все это открывает новые возможности для отечественных производителей софта программного обеспечения и продуктов ИБ.

В решениях для кибербеза особенно нуждаются оборонный, энергетический, сырьевой и финансовый секторы. Именно на них направлены основные атаки злоумышленников. Мы и сами ощущаем высокий спрос на услуги ИБ в связи с атаками и утечками: участились запросы на такие продукты от наших клиентов из разных секторов экономики.

— Кто будет главными бенефициарами этого роста?

— Текущая ситуация для российских вендоров выглядит позитивно. Западные игроки уходят с нашего рынка и освобождают направления, где ранее была высокая конкуренция. Например, сетевая защита, защита рабочих станций и приложений. Мы видим, что в РФ появляются новые продукты от наших вендоров: «Кода безопасности», «ИнфоТеКСа», «Лаборатории Касперского», Positive Technologies, «КриптоПро», InfoWatch и «Аладдин Р.Д.». У них сейчас есть возможность увеличить свою долю на рынке. Все больше российских компаний начинают беспокоиться об ИБ и усиливают меры защиты.

— Специалисты наблюдают рост объема потерь данных, составляющих коммерческую тайну и ноу-хау. Компании до сих пор не уделяют этому должного внимания? Или это связано с наращиванием усилий киберпреступников?

— Действует несколько факторов. Активность киберпреступников сильно выросла. К тому же многие компании не уделяли должного внимания защите информации, пока на собственном опыте не столкнулись с проблемами. По разным отчетам, в первом квартале 2022 года количество атак выросло на 14–20% по сравнению с четвертым кварталом 2021 года. Чаще всего атакам подвергались государственные и медицинские учреждения, а также промышленные предприятия. Причем более половины атак были целенаправленными. Их последствия разнообразны, и масштаб варьируется от воздействия на одного человека до влияния на целую отрасль экономики или регион. Как правило, атаки злоумышленников направлены на получение конфиденциальной информации, в первую очередь — персональных данных.

— Что сейчас влияет на развитие рынка в большей степени — уход западных компаний или госрегулирование, согласно которому госорганам запрещается использовать средства защиты из «недружественных стран» с 2025 года?

— Госрегулирование всегда влияло на рынок, но в современных внешнеполитических реалиях его роль усилилась. ФСТЭК вводит ограничения на использование иностранных средств защиты информации (СЗИ). Так, в марте было приостановлено действие 56 сертификатов СЗИ от Cisco, CyberArk, Fortinet, Microsoft, Oracle, Red Hat, SAP, SUSE Linux, VMware и др. Уход западных компаний стал дополнительным катализатором развития рынка ИБ.

Кроме того, появляется все больше примеров, когда с помощью свободного ПО причиняется ущерб IT-инфраструктуре российских компаний и обычным пользователям. Для этого злоумышленники вносят в разрабатываемое ПО недокументированные возможности, которые впоследствии могут навредить. Использовать в России иностранные решения для ИБ становится рискованно. Программы продолжают работать, но обновить их или базы сигнатур невозможно, поэтому рекомендуется отказаться от таких решений. Неактуальные версии ПО могут содержать уязвимости, а невозможность обновления негативно влияет на его эффективность.

— На каких рынках могли бы быть востребованы наши решения в текущих геополитических условиях?

— Можно пробовать продвигать российские решения на рынках СНГ, Ближнего Востока и Азии. Но все чаще иностранные партнеры боятся вторичных санкций. Тяжело спрогнозировать, в какую сторону изменится ситуация. В основном за рубежом популярны компании, которые специализируются на расследовании и предотвращении киберпреступлений.

Интервью взял Владимир Шадрин

Офицеры кибербезопаса

— информбезопасность —

После начала конфликта на Украине и перехода его в цифровое поле — усиления кибератак на российскую IT-инфраструктуру — за развитием информбезопасности (ИБ) стали пристально наблюдать все: от государства на самом высоком уровне до представителей малого и среднего бизнеса (МСБ). Аналитики предсказывают рост этого рынка более чем вдвое до 2026 года и на 20% уже к концу 2022-го. Несмотря на общее ухудшение состояния экономики на фоне специальной военной операции и частичной мобилизации, кибербезопасность может стать отраслью, для которой происходящее — основной драйвер. Но так ли безоблачно будущее рынка ИБ и что в большей мере будет на него влиять?

УТЕЧКИ-2022 ИСТОЧНИК: ПУБЛИЧНЫЕ ДАННЫЕ.

	КОМПАНИЯ	ПРИЧИНА	ОБЪЕМ
28 VIII	Онлайн-кинотеатр Start	Ошибка в системе	44 млн строк
29 VII	«Почта России»	Хакерская атака	10 млн строк
6 VI	«Ростелеком»	Недобросовестные действия сотрудника	109,3 тыс. строк
20 V, 10 VI	Delivery Club	Хакерская атака	2,2 млн строк
3 V	Лаборатория «Гемотест»	Хакерская атака	30 млн пользователей
1 III	Сервис доставки «Яндекс.Еда»	Недобросовестные действия сотрудника	109,3 тыс. строк
28 II	Сервис доставки СДЭК	Хакерская атака	1,2 млрд строк

Атаки как ключевой драйвер

В начале августа Центр стратегических разработок (ЦСР) выпустил исследование современного рынка ИБ в России и просчитал его динамику на горизонте пяти лет. По его оценке, если в 2021 году объем рынка составлял 186 млрд руб., то к 2026 году он может вырасти в 2,5 раза, до 469 млрд руб. Одним из драйверов станет уход зарубежных вендоров (IBM, Cisco, Fortinet, ESET), их доля на отечественном рынке сократится с 73 млрд руб. в 2021 году до 23 млрд руб. в 2026 году, а российских — вырастет со 113 млрд до 446 млрд руб. соответственно. Вторым фактором исследователи считают рост кибератак на российские компании, охватывающих уже не только крупных игроков и госсектор, но и МСБ.

Как рассказал „Ъ“ гендиректор Group-IB в России и СНГ Валерий Баулин, в 2022 году в стране «рекордно растет число кибератак, в некоторых сегментах — на порядок с начала года». Например, за лето в открытый доступ хакеры выложили 140 украденных баз данных против 73 весной, говорит он. Также сохраняется тренд атак вирусов-шифровальщиков и DDoS-атак, которые могут «полностью остановить бизнес компании» (см. „Ъ“ от 21 сентября). В текущем году атакам хакеров подверглась даже игровая индустрия: за первые полгода такие ресурсы подвергались DDoS-атакам в три раза чаще, чем за весь 2021 год (см. „Ъ“ от 1 августа). Такая динамика подталкивает компании закупать доступные им решения для защиты, и, хотя МСБ еще пользуется приобретенными ранее продуктами ушедших компаний, многие уже задумываются о переходе на российские.

Прогноз аналитиков в области импортозамещения схож с «горизонтом планирования» ЦСР: по их подсчетам, на полное замещение иностранных продуктов потребуется два-три года. Локомотивом этого процесса станут субъекты критической информационной инфраструктуры (КИИ; к ним относят банки, энергетические компании, ведомства, телеком-компании и др.). И в случае с этим сегментом дело не только в осознании угроз самими игроками, но и в твердой руке правительства.

Указ на защиту

1 мая президент подписал указ №250 «О дополнительных мерах по обеспечению ИБ РФ», который распространяется на предприятия с госучастием (от ведомств до госфондов), стратегические предприятия, системообразующие организации и субъекты КИИ. В частности, указ запрещает им использовать средства защиты из «недружественных стран» с 2025 года, а также обязывает назначить заместителей руководителя по ИБ и создавать спецотдел, отвечающий за это направление. Указ президента запустил целый ряд изменений как в правительстве, так и в отрасли.

Так, важную роль для рынка стал играть новый регулятор — Минцифры. Ранее ИБ занимались в первую очередь ФСБ и Федеральная служба по техническому и экспортному контролю. «Цифровому ведомству» удалось оперативно решить ряд значимых для отрасли задач, например запустить реестр недопустимых событий в области кибербезопасности, открытый для всех организаций. Это, с одной стороны, систематизирует знания самих компаний о том, что может произойти с их инфраструктурой в случае атаки: утечка конфиденциальных данных, остановка производства и т. д. С другой — дает возможность заказчику грамотно распределять ресурсы и не тратить их на все средства безопасности подряд, пытаясь защититься от всего. Напомним, уже к маю российские решения для кибербезопасности подорожали более чем на 20% по сравнению с мартом (см. „Ъ“ от 31 мая).

Минцифры же подняло вопрос об усилении ответственности компаний за утечки данных и о материальной компенсации гражданам, чьи данные оказались в руках хакеров по вине бизнеса. Если ведомство реализует этот механизм и согласует его с ЦБ, то средства на погашение ущерба могут начать отчисляться из оборотных штрафов за утечки (см. „Ъ“ от 19 августа).

Эти и другие изменения активизировали диалог государства и отрасли, который в текущих условиях может помочь оперативно решать насущные проблемы и, как говорят в компаниях, «перейти от бумажной безопасности к реальным действиям».

Сейчас на развитие рынка в первую очередь влияет уход западных компаний, а во вторую — реальные киберинциденты, вызванные геополитической ситуацией, считают в Positive Technologies. Только потом идет госрегулирование, но первые два фактора ситуативны, а госрегулирование — это «игра вдолгую», поэтому этот фактор будет сильнее других влиять на рынок.

Бенефициары роста

Российский рынок ИБ даже до ухода иностранных компаний был достаточно насыщенным. По оценкам ЦСР, по объему выручки в 2021 году отечественные вендоры его делили наравне с западными: 13% занимала «Лаборатория Касперского», 9% — Positive Technologies, 9% — «ИнфоТеКС», 7% — израильская Check Point Software Technologies, 7% рынка было у «Кода безопасности», по 6% — у американских Cisco Systems и Fortinet, 3% — у IBM. Так, зарубежные игроки в 2021 году занимали 39% от общего объема российского рынка.

Аналитики TAdviser приводят более полную картину российского рынка: на первом месте по выручке по-прежнему «Лаборатория Касперского», на втором — ГК Softline, затем «РТК Солар», «Газинформ Сервис», BiZone и др. В перечень TAdviser входят не только производители необходимых решений, но еще дистрибуторы и интеграторы.

К 2026 году доля отечественных вендоров вырастет на 33%, а зарубежных — упадет на 19%. На долю российских компаний придется почти 95% объема рынка — 343,6 млрд руб., прогнозируют в ЦСР.

Камни преткновения

Несмотря на благоприятный прогноз и условия для роста рынка, у него есть и сдерживающие факторы. Первым и самым очевидным на данный момент является объявленная 21 сентября частичная мобилизация населения. Пока речь идет о 300 тыс. резервистов в возрасте от 20 до 60 лет. Минцифры прорабатывает вопрос освобождения сотрудников IT-отрасли от мобилизации, компании и сотрудники уже могут подать заявку на отсрочку через портал «Госуслуг», но отрасль обеспокоена, и многие специалисты стремятся оперативно покинуть страну, а компании — вывести бизнес за границу.

Собеседники „Ъ“ в отрасли предупреждают: профильные специалисты на стороне заказчика в подавляющем большинстве — мужчины среднего возраста, служившие, с военно-учетной специальностью. Бронь распространится на единицы. «Выпадение специалистов как со стороны заказчика, так и разработчика из рабочего процесса на неопределенный срок станет серьезной проблемой для отрасли»,— делятся с „Ъ“ представители IT-компаний.

Вторым сдерживающим фактором может стать нарастающий дефицит вычислительной базы, с которой ситуация обстоит значительно хуже, чем с софтом. Если и до кризиса российские производители «железа» не могли удовлетворить клиентский спрос, то сейчас практически вся промышленность попала под западные санкции, что не дает компаниям возможность закупать современное производственное оборудование или разворачивать производство своих чипов на иностранных фабриках по лицензии.

Так, 15 сентября Минфин США включил в SDN-лист российские дизайн-центры и крупнейших производителей вычислительной техники, в том числе «Байкал Электроникс», МЦСТ, НПЦ «Элвис», «Аквариус» и структуру ГК Yadro. Американские компании должны до 15 октября свернуть все операции с российскими партнерами.

С другой стороны, радиоэлектронная промышленность тоже может пострадать от частичной мобилизации: на профильных предприятиях работает около 350 тыс. человек, примерно половина из которых — мужчины. Пока порядок предоставления брони специалистам обсуждается в правительстве.

Еще одним не самым очевидным, но значительным камнем преткновения может быть сложный экспортный путь продуктов ИБ. Из-за санкций многие рынки для российских компаний оказались закрыты, а те, что пока доступны, или насыщены своими игроками, или имеют другие ограничения.

По подсчетам аналитиков ЦСР, сейчас заинтересованы в покупке российских продуктов и услуг 18 стран, среди которых Китай, Бразилия, Индия, Турция, Саудовская Аравия и Израиль. Но, например, в Бразилии высока конкуренция с мировыми вендорами. В Китае и Вьетнаме российские IT-решения могут быть вытеснены собственными игроками, а в Турции «высокие политические риски». Таким образом, в перечне наиболее благоприятных стран для экспорта остаются Узбекистан, Казахстан, Пакистан, Белоруссия, Бангладеш и Египет.

Это притом, что сейчас для иностранных компаний возрастают риски вторичных санкций за какое-либо сотрудничество с Россией, и далеко не все страны окажутся готовы к такому опасному партнерству. Поэтому в первую очередь отечественным разработчикам предстоит развиваться на своем рынке, отстаивая свои ниши и стараясь завоевать новые в условиях агрессивной конкуренции и токсичной внешней среды.

Татьяна Исакова

Доигрались

— гейминг —

с13

Впрочем, геймеры из РФ используют и другие пути обхода ограничений — в частности, они покупают игры не напрямую в сторах, а через подарочные ключи, которые можно приобрести на ряде российских сайтов. Купив ключ, геймер вводит его в специальном поле Steam и получает игру «в подарок», обходя необходимость проводить оплату за продукт. «Трафик в магазинах ключей, оставшихся на российском рынке, вырос примерно в три раза, и связано это с дефицитом AAA-контента (высококачественные игры с крупным бюджетом.— **„Ъ“**)»,— подтверждает топ-менеджер крупной IT-компании.

Он добавляет, что сейчас в России фактически существует только одна альтернатива таким крупным сторам, как Steam и Epic Game Store,— магазин VK Play (принадлежит VK). С этим согласен другой источник „Ъ“ на рынке игровой разработки, однако он добавляет, что сегодня на VK Play крайне мало качественных и высокобюджетных игр, хотя компания и работает над тем, чтобы получить права на AAA-проекты. Например, в сентябре компания анонсировала права на эксклюзивную продажу игры Atomic Heart от студии MundFish.

«На рынке сейчас происходит большое количество изменений. Мы хотим, чтобы условия для разработчиков и игроков оставались комфортными. На VK Play мы предлагаем самые выгодные условия для создателей игр и постоянно работаем над тем, чтобы площадка была удобной в использовании»,— утверждают в VK Play. По словам его представителя, магазин уже сделал возможной публикацию игр физлицами, а также добавил кабинет разработчика и функции локализации игр.

Участники рынка уверены, что для развития российской игровой индустрии в текущих условиях крайне важно развивать собственные площадки дистрибуции контента, причем не только VK, но и силами других компаний. «России нужно несколько сторов, в том числе не привязанных к определенному издателю игр,— считает директор по развитию игровых технологий Wargaming Виктор Масалов.— Тогда родится конкуренция (как между Google Play Market и App Store, Sony и XBox, Steam и Epic Game Store), что всегда на пользу игрокам».

Впрочем, опрошенные „Ъ“ источники в правительстве, собеседники на рынке игровой разработки и эксперты сейчас смотрят на ситуацию намного позитивнее, чем в начале весны. «Первый шок после 24 февраля прошел: те, кто хотел уехать,— уехали, остальные думают, как работать в России дальше»,— говорит собеседник на рынке игровой разработки. По его словам, часть студий готовы оставить разработку в России, продавая и продвигая контент через зарубежные юрлица, чтобы избегать санкций. О том, что ряд российских студий решил лишь частично вывезти бизнес из страны, говорит господин Масалов. «А из тех, кто перевел юрлица за рубеж, на мой взгляд, довольно многие не ушли в прямом смысле, а разделили бизнес с юридической точки зрения с целью минимизации рисков»,— уточняет он.

В поисках Perpetuum Mobile

Необходимость вывести юрлица за рубеж, наладить механизм перевода средств со счетов одних компаний на другие, а также оперативно масштабировать российские сервисы дистрибуции игрового контента — это текущие проблемы, с которыми необходимо справиться в ближайшей перспективе. Однако отрасль опасается в скором времени столкнуться с еще одной трудностью: из-за санкций российские студии могут лишить средств разработки игрового контента, а именно движков. Наиболее популярные из них — Unity и Unreal Engine — принадлежат зарубежным компаниям, которые в перспективе могут отказать к доступу к ним.

«Российскому рынку нужна своя экосистема. Весь мир игровой разработки живет на использовании одних и тех же решений, что сильно удешевляет разработку и решает кадровые проблемы в условиях постоянно высокого спроса на профессиональных разработчиков. В условиях, когда доступ к тому или иному сервису может быть прекращен по воле компании-производителя, нужно подстраховываться и создавать свое»,— уверен Виктор Масалов.

Интерес к разработке движка проявили сразу две крупные организации. Первым был «Ростех»: глава госкорпорации Сергей Чемезов написал письмо главе Минцифры Максуту Шадаеву с просьбой выделить средства на создание игрового движка, общие затраты на реализацию проекта оценивались в 10 млрд руб. Министерство порекомендовало господину Чемезову обратиться за субсидией в Российский фонд развития информационных технологий. При этом, как говорят в «Ростехе», движок может понадобиться не только для разработки игр. «Продукт может быть использован в разных отраслях, в том числе в проектах в сфере образования, культуры, здравоохранения. Конечно, он сможет использоваться и для моделирования в машиностроении, например в авиастроении»,— заявил „Ъ“ представитель госкорпорации.

Вторым кандидатом на разработку этой системы стал VK: компания обратилась в Минцифры с предложением разработать движок. Поддержка игровой индустрии активно обсуждается участниками рынка и профильным министерством в разных направлениях, в том числе обсуждается и вопрос создания отечественного игрового движка, подтвердил представитель VK.

Топ-менеджер одной из крупнейших компаний-разработчиков игр в СНГ считает, что создание конкурентного движка — это долгая история: «Разработчикам придется пройти через множество „детских болезней“, поэтому что-то качественное, с моей точки зрения, может появиться не ранее чем через четыре-пять лет после старта разработки». При этом, по его мнению, уже на этапе разработки нужно целиться в качество картинки, которое выдает, например, Unreal Engine. «В противном случае и браться не стоит»,— резюмирует он.

Никита Королев

GIS ГАЗИНФОРМ СЕРВИС

Айти в программу

Экономические и политические изменения 2022 года затронули все сферы бизнеса в России. Словами года в области IT уже сейчас можно смело выбрать «импортозамещение» и «кибербезопасность»: уход западных игроков поставил российские компании перед фактом и заставил экстренно переходить на отечественные решения, при этом российская инфраструктура подверглась беспрецедентному числу кибератак. В сложных условиях IT-отрасль быстро сплотилась, а профильные мероприятия оказались как никогда востребованы для обмена опытом и экспертизой. Одним из таких событий стал форум Global Information Security Days (GIS DAYS 2022) компании «Газинформсервис», который прошел 5–7 октября сразу на трех площадках в двух городах: Москве и Санкт-Петербурге.



ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ GIS DAYS 2022

— форум —

День I: кибербез и импортозамещение

Импортозамещение и кибербезопасность стали главными темами GIS DAYS 2022, первого IT-дня, который прошел в Москве. Здесь встретились представители бизнеса, профильных регуляторов, разработчики отечественного программного обеспечения (ПО), электронной компонентной базы и интеграторы. Так, на пленарной сессии «Актуальные вопросы импортозамещения в IT» выступили сенатор РФ Артем Шейкин, заместитель главы Минцифры Александр Шойтов, директор департамента цифровых технологий Минпромторга Владимир Дождев и другие. А участниками сессии «Российское программное обеспечение и оборудование — оценка перспектив и задачи» стали топ-менеджеры компаний YADRO, «РЕД СОФТ», «Аладдин Р.Д» «Аквариус» и «Скала^р». Общая аудитория только IT-дня, включая онлайн-трансляцию, составила более 20 тыс. зрителей.

Участникам форума было что обсудить. Уход зарубежных вендоров, с которыми привык работать российский бизнес, заставил компании очень быстро принимать решение по переходу на отечественные продукты, рискуя допустить остановку всех производственных процессов в случае отключения западных решений, и даже если лицензии на них были куплены более чем на полгода, все понимали: это не является гарантией бесперебойной работы инфраструктуры. Тем более что поддержки закупленных продуктов тоже больше нет.

Также с конца февраля российские компании подвергаются масштабным кибератакам: от DDoS (атака на сервер) до атак вирусов-шифровальщиков. По геополитическим причинам с отечественного рынка ушли почти все зарубежные компании как в области кибербезопасности (ESET, Fortinet, Cisco Systems и др.), так и многие IT-игроки в целом. Вопрос о переходе на российские решения стал самым насущным, притом что сделать это необходимо в очень сжатые сроки и максимально безопасно.

Основными темами дискуссий в первый день форума стали: проверка на прочность IT-инфраструктуры в период импортозамещения, тестирование инфраструктуры на проникновение, переход на новые российские решения, развитие отечественных систем управления базами данных (СУБД) и операционных систем (ОС) и даже цифровое искусство — нейросети и искусственный интеллект. Не обошлось, конечно, без обсуждения темы IT-кадров, которых отрасли сейчас очень не хватает — проблему с их подготовкой признают на самом высоком уровне: от главы Минцифры Максута Шадаева до вице-премьера РФ Дмитрия Чернышенко.

Также в первый день форума прошла презентация продуктов «Газинформсервиса»: СУБД Jatoba, средства доверенной загрузки SafeNode и решения для комплексной защиты информационных ресурсов Efros ACS. Каждый продукт отвечает вызовам времени и предлагает современное решение насущных задач. По словам представителей разработчика, они подходят как для небольших компаний, так и для крупнейших корпораций.

Особый интерес вызвала СУБД Jatoba, которая построена на основе одной из самых известных и распространенных в мире СУБД с открытым кодом PostgreSQL — именно это решение является на рынке основным после ухода из России SAP, Oracle и Microsoft.

«Компания имеет значительный опыт миграции СУБД корпоративного сегмента на отечественное ПО и готова предложить разработку и сопровождение таких проектов, а также отдельные консультации по вопросам переноса данных и бизнес-логики СУБД»,— рассказал менеджер по продукту Jatoba в «Газинформсервисе» Константин Семенчук. При этом скорость миграции зависит от объема информации, хранящейся в базе данных, важности отказоустойчивости при работе с СУБД, софта, с использованием которого работает заказчик, а также множества других условий, говорят в компании.

Важно напомнить, что компаниям в переходе на российские решения в том числе помогает государство: по данным Минпромторга, Фонд развития промышленности предоставляет льготные займы под 1% и 3% годовых на создание и внедрение цифровых продуктов на предприятиях. А партнерство между самими разработчиками позволяет быстро выводить на рынок необходимые качественные решения.

«После февральских событий произошла заметная консолидация отрасли,— рассказывает заместитель генерального директора, технический директор „Газинформсервиса“ Николай Нашивочников.— Все игроки были сосредоточены на том, чтобы защитить не только свои ресурсы, но и те, что так или иначе относятся к госсектору и представляют особенную ценность — речь, например, о критической информационной инфраструктуре. С марта по июнь страна подвергалась массовым кибератакам, и, считаю, с этой ситуацией мы справились. Благодаря отраслевым мероприятиям мы обмениваемся опытом, движемся к решению общих проблем, чтобы каждый шел не своим путем, а мог учиться на опыте коллег». Это позволит каждой компании избежать множества ошибок, уверен Николай Нашивочников.

День II: инвестиции в будущее

Второй день форума прошел в Петербурге на площадке Санкт-Петербургского государственного университета телекоммуникаций (СПбГУТ) им. М. А. Бонч-Бруевича и неслучайно был назван студенческим. Его эксперты и все участники форума посвятили время общению с молодежью — как в формате мастер-классов и дискуссий, так и батла («Студенческая киберарена»), интеллектуального состязания по IT и кибербезопасности между студентами.

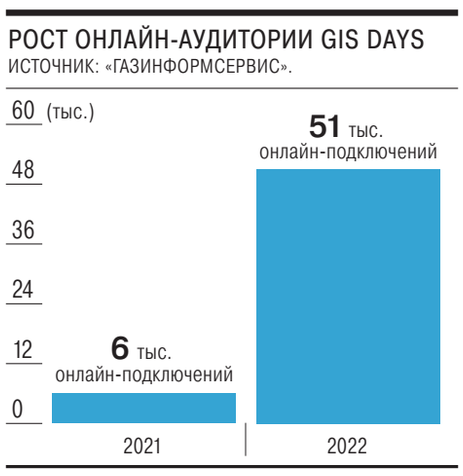
Общей темой мастер-классов стали искусственный интеллект (ИИ) и нейросети. Сессии получились весьма представительными и экспертными: в них приняли участие заместитель гендиректора «Газинформсервиса» Николай Нашивочников, директор по развитию технологий ИИ «Яндекса» Александр Крайнов, глава Суперкомпьютерного центра Санкт-Петербургского политехнического университета Алексей Лукашин, руководитель группы защиты инфраструктурных IT «Газинформсервиса» Сергей Полунин и главный специалист отдела комплексных систем защиты информации «Газинформсервиса» Дмитрий Овчинников.

После этого СПбГУТ и компания «Газинформсервис» подписали соглашение о сотрудничестве, значимое для обеих сторон. В рамках соглашения партнеры планируют развивать сотрудничество в сфере образовательной, научно-технической и инновационной деятельности. Работа будет направлена на создание и развитие совместных проектов и мероприятий разного формата, позволит проводить обмен профессиональным опытом между сотрудниками компании и студентами университета, развивать компетенции в сфере информационной безопасности.

«Договор о сотрудничестве позволит предоставлять нашим студентам еще больше возможностей для обучения и развития профессиональных навыков и компетенций»,— отметил проректор по цифровой трансформации СПбГУТ им. М. А. Бонч-Бруевича Антон Зарубин. По словам же Николая Нашивочникова, подписанное соглашение поможет партнерам «в формировании высокопрофессиональных кадров для отрасли».

В тот же день организаторы презентовали совместный с «Деловым Петербургом» проект «Биржа IT-стартапов». Свои проекты в таких сферах, как кибербезопасность, ИИ, робототехника, бизнес-аналитика и импортозамещение, для участия в конкурсе направили 92 IT-предпринимателя. В финал прошли пять лучших работ, конкурс к тому времени длился уже четыре месяца. На кону был 1 млн руб. на развитие и рост бизнеса. Победителем стали Pruffme.com, создатели онлайн-платформы для совместной работы и учебы.

Конкуренция в ходе конкурса была очень серьезной, рассказал „Ъ“ генеральный директор Pruffme.com Сергей Подузов, по словам которого в проект уже многое вложено — как технически, так и с точки зрения креативного подхода к решению задач. «Команда видит переход аудитории от формата простых онлайн-конференций к полноценным инструментам совместной работы, где пользователи могут систематизировать свои задачи, зафиксировать договоренности и решить сразу несколько вопросов в ходе коммуникации»,— указывает он. Поэтому Pruffme.com старается делать процессы работы или учебы наиболее интерактивными: «Мы очень плотно взаимодействуем с потребителями, разбираем каждый инсайд, чтобы сделать решение лучше».



Своим ключевым активом Сергей Подузов называет людей: в команде 38 человек, и Pruffme.com старается делать меньшими силами масштабный продукт. Полученный грант команда планирует инвестировать в сотрудников: направить их на развивающие курсы и семинары по повышению квалификации. В Pruffme.com уверены, что именно это сейчас позволит компании развиваться быстрее и укреплять свои позиции на рынке.

«Мы искренне верим в проект»,— говорит Николай Нашивочников. Конкурс «Биржа IT-стартапов» позволил поддержать начинающих IT-специалистов и их команды, помочь воплотить в жизнь бизнес-идеи, скорректировать план продвижения и позиционирования продуктов на рынке, рассказал он. «Венчур и гранты для стартапов — это то, что будет продолжать существовать и расти, несмотря на изменения на рынке. При этом экспертиза зрелых компаний не меньшая помощь, чем инвестиции в случае со стартапом»,— уверен он.

Эксперт также поделился мнением о стартапах в области кибербезопасности, указав, что это «сложные проекты». По его мнению, без поддержки крупного игрока на рынке такие проекты практически невозможны в силу специфики темы и ограничений, которые она накладывает. «Например, зарегулированность отрасли — невозможность в ряде случае применения продукта без его сертификации по требованиям безопасности информации»,— объясняет Николай Нашивочников.

Также в кибербезопасности до момента первых продаж, которые так важны для начинающей компании, проходит гораздо больше времени, чем в целом по IT-сектору. Поэтому в кибербезопасности для создания и развития нового проекта сотрудничество с уже зрелой компанией является хорошей поддержкой, уверен он. Даже при этом условии срок развития полноценного киберстартапа в самостоятельного игрока может составить до полутора лет. Поэтому «Газинформсервис» готов выступить тем зрелым игроком, который поддержит новый проект и даст ему шанс.

День III: диалог как ключ к решению задач

Заключительный день форума прошел в «Ленинград–центре» и был полностью посвящен актуальной теме информационной безопасности. На первых сессиях представители ведущих компаний на рынке делились опытом и рассказывали, с чем им пришлось столкнуться с начала года, какие решения они находили и какие стратегии уже выработали.

Так, бизнес-консультант по безопасности Positive Technologies Алексей Лукацкий выступил с докладом «Quick win в кибербезопасности. Как получить результат при минимуме затрат». Основной акцент он сделал на концепции недопустимых событий, которые могут быть реализованы в любой компании, у которой есть IT-инфраструктура. Например, в случае с банком это кража средств или утечка персональных данных клиентов. В случае с промышленным предприятием — внеплановая остановка производства. Эксперт уверен, что этот подход является более грамотным и экономичным, нежели следование исключительно требованиям регулятора или практике выявления сегментов, определенных когда-то профильным департаментом организации.

По словам господина Лукацкого, необходимо сначала заниматься мониторингом и исключением выбранных недопустимых событий хотя бы на 15% сетевых узлов. После улучшать выбранный механизм и проводить киберучения, тестируя сеть на проникновение, охватывая уже до 40% инфраструктуры, и затем переходить к третьей фазе — полному ее покрытию и 100-процентному исключению недопустимых сценариев. Так компании удастся оперативно решить свои ключевые задачи, а также структурировать расходы на кибербезопасность, не пытаясь внедрить сразу все доступные средства защиты.

Своим опытом и мнением на сессии поделились также ведущий менеджер продуктов «ИнфоТеКС» Алексей Власенко, директор по развитию компании «Арбайт» Александр Семеняченко, заместитель генерального директора Zecurion Александр Ковалев, руководитель направления по развитию бизнеса на территории Северо-Западного федерального округа InfoWatch Татьяна Ксюнина и директор по развитию «Стаффкоп» Дмитрий Кандыбович.

Все эксперты сошлись во мнении, что чем больше сейчас мы знаем об угрозах и методах атакующих, тем надежнее можем выстроить защиту. Поэтому доклады спикеров были насыщены не только ключевыми трендами, но и реальными индивидуальными кейсами.

Российская ИБ-отрасль всегда была в некоторой оппозиции по отношению к западной, и российский рынок оказался готов к текущим вызовам, рассказал „Ъ“ заместитель генерального директора «ИнфоТеКСа» Дмитрий Гусев. «Мы предупреждали, что риски отключения России от иностранных продуктов есть — так оно и случилось,— рассуждает он.— Когда в России присутствовали зарубежные вендоры, рынок работал по принципу „что нового создали и предложили иностранные компании, и чем могут ответить российские игроки“, а заказчик имел возможность выбирать. Сейчас ситуация изменилась: выбора больше нет. Диалог между российскими заказчиками и поставщиками стал плотнее».

Как утверждает господин Гусев, российские компании продолжают развиваться, совершенствуя свои продукты и создавая новые, осваивая открывшиеся ниши и ускоряясь, как того требуют условия времени. «С одной стороны, заказчику нужно оперативно принимать решения, потому что он находится под риском остановки своей деятельности из-за отказа ранее работавших иностранных систем,— делится наблюдениями он.— Разработчики же должны ускоряться, чтобы догнать по функциональному составу зарубежные решения, которые им предстоит заместить своими в ближайшее время». В этом контексте движение навстречу друг другу усилилось, и такие мероприятия, как GIS DAYS,— «хорошие площадки для обмена мнениями и опытом», заключает Дмитрий Гусев.

Наиболее динамичной частью третьего дня форума стала панельная дискуссия «Кибербезопасность в новых условиях. Первые итоги». В ней приняли участие спикеры дня Алексей Лукацкий, Николай Нашивочников и Дмитрий Гусев. Эксперты обсудили ключевые вызовы нового времени, актуальные проблемы и решения. Как отметили Николай Нашивочников и Дмитрий Гусев, не для всех компаний и корпораций процессы 2022 года стали шоком — так, госсектор с 2015 года начал переход на отечественные продукты, отчасти по требованию регуляторов, отчасти понимая риски лучше, чем бизнес. Причем этот сектор является крупным и интересным заказчиком, указывали они, тогда как в госкорпорациях и бизнес-секторе ситуация иная: многие не спешили с импортозамещением и в итоге оказались в стрессовой ситуации.

Состояние заказчиков IT-решений вызвало отдельную дискуссию об их желаниях и возможностях. В сфере бизнеса, по словам экспертов, часто ситуация выглядит как немедленное желание перейти на российское решение, но с условием, чтобы «оно было не хуже зарубежного, при этом за меньшие деньги». Это практически невозможно, поэтому, как говорят спикеры, клиенты сейчас идут на компромисс, понимая, что выбора у них почти нет.

В то же время «заказчики разные, и нельзя воспринимать их как единую структуру с одинаковыми запросами», напоминает Дмитрий Гусев. По его словам, те компании, которые переходили на российские продукты до текущего года, знают, что, например, сервисное обслуживание у отечественных производителей лучше, а возможностей подстроить инфраструктуру под свои задачи куда больше в силу доступности диалога. А если какой-то блок функционала сейчас отстает от продуктов, которые больше приобрести нельзя, то вендоры в России будут нагонять и закрывать эти ниши сейчас «семимильными шагами».

Но иногда в развитии продуктов IT-компаний и потребностях рынка возникают расхождения. Николай Нашивочников заявил, что во избежание конфликта интересов заказчика и вендора необходимо «договариваться, формировать определенные „дорожные карты“, определить сроки и функционал, необходимый заказчику и в то же время рынку». Это станет эффективной и успешной стратегией развития отрасли, считает он.

Не обошлось и без обсуждения оттока IT-кадров за рубеж: спикеры признают, что происходящая сейчас миграция населения может усугубить кадровый голод, поэтому решать проблему нужно быстро. Другой проблемой является и общая экономическая ситуация, в которой многие компании не понимают, выживут ли вообще. По словам Алексея Лукацкого, возрастает риск сокращения числа компаний в области кибербезопасности и такой уход конкурентов с рынка может скорее усложнить жизнь оставшихся. «Не факт, что крупные вендоры в условиях дефицита „железа“ и нехватки кадров смогут закрыть потребности рынка»,— высказал свои опасения господин Лукацкий.

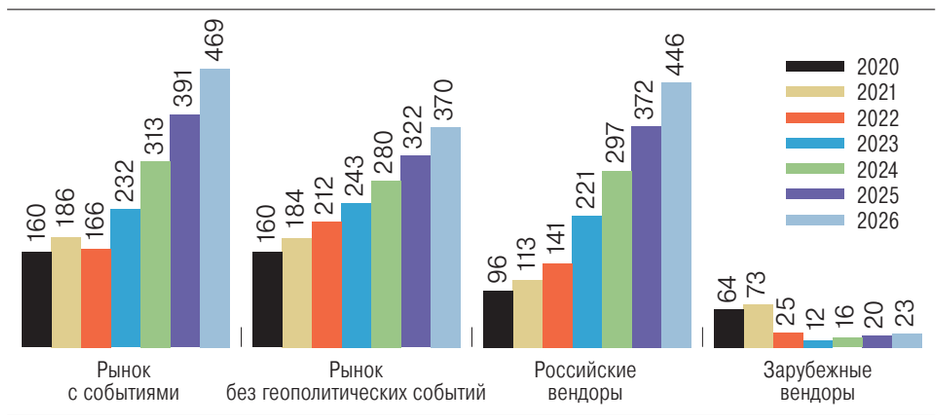
Финал

Несмотря на очевидные вызовы времени, эксперты настроены оптимистично. Рост рынка в каждом сегменте — от СУБД до обеспечения ИБ, а также рост внутренней конкуренции на рынке стимулирует и развивает игроков, ставя сложные задачи. При этом у отрасли как никогда есть мощный драйвер, который уже через год может вывести все российские IT-продукты на новый уровень, считают участники форума.

Игроки IT-рынка видят и участвуют в трансформации отрасли, отмечая тенденции и высоко оценивая возможность обменяться мнениями на одной площадке. В силу того что форум проходил в разных городах на нескольких площадках, GIS DAYS 2022 вобрал в себя все актуальные темы и дал возможность представителям IT пообщаться в подходящем им формате. О своевременности и актуальности GIS DAYS 2022 свидетельствует и суммарная аудитория онлайн-просмотров и радиотрансляции форума, которая составила более 170 тыс. человек, и это кратно превышает показатели прошлого года.

Эксперты уверены: формат живых мероприятий остается актуальным, так как диалоги, как на сцене, так и в кулуарах, сейчас остро необходимы всем. А расширенная география форума позволила обменяться экспертизой между многими городами России.

Татьяна Исакова



информационные технологии

На линии защиты

Количество массовых кибератак на российские компании осенью пошло на спад после всплеска в первой половине текущего года. При этом они сменились более сложными, таргетированными атаками. Бизнес и госсектор стали уделять особое внимание информбезопасности (ИБ), расширяя список решений и переходя на отечественных вендоров. Однако наличие средств информационной защиты не означает, что они гарантируют стопроцентную защищенность, предупреждают эксперты. Поэтому важно уделять внимание повышению цифровой грамотности сотрудников и тестированию инфраструктуры

— информбезопасность —



ЕВГЕНИЙ ДУДИН

Не количество, а качество

Нынешней осенью наблюдается спад количества массированных атак на IT-инфраструктуру компаний, отмечают в компаниях по кибербезопасности. По сравнению со всплеском атак в начале года, когда их количество год к году увеличилось в десять раз, к концу сентября число атак снизилось в три раза.

О росте атак с марта по июнь в 9,6 раза говорил руководитель направления по технологической поддержке облачных и инфраструктурных решений ПАО «МегаФон» Григорий Айкашев на форуме «Технопром-2022». В феврале и начале марта профильные компании отразили в 4,5 раза больше атак, чем за аналогичный период 2021 года. С началом специальной военной операции (СВО) 24 февраля число DDoS-атак на российские компании выросло как минимум в три раза, при этом к концу июня интенсивность атак снизилась вдвое по сравнению с маем. Многие атаки были успешными: по итогам проверки компаний из всех отраслей экономики — от финансового сектора до промышленности — выяснилось, что у 79% в системах были уязвимости и 86% из них удалось успешно взломать, сообщал „Ъ“ 10 июня.

Нынешний спад атак произошел в связи с тем, что компании стали более ответственно относиться к обеспечению ИБ и легких целей для взлома практически не осталось, полагает руководитель отдела исследования киберугроз экспертного центра безопасности Positive Technologies (PT ESC) Денис Кувшинов. По его словам, если в начале года компании взламывали через незакрытые уязвимости на периметре, то сейчас большинство таких легко эксплуатируемых уязвимостей закрыто.

Хотя общее число атак снизилось, их качество выросло: атаки стали более мощными, умными и таргетированными, отмечает директор по развитию облачных и инфраструктурных решений «МегаФона» Александр Осипов. Например, в мае страховая компания ВСК тестировала доступ к услуге «МегаФон WAF» (Web Application Firewall — защитный экран для веб-приложений). WAF представляет собой облачное решение, которое находит и предотвращает атаки на веб-ресурсы, выявляет уязвимости в системе и запрещает удаленное выполнение вредоносных команд. Во время пилотирования решения на один из сайтов страховой компании началась атака.

«Использование WAF позволило сразу же устранить основные негативные последствия и сохранить работоспособность сайта для клиентов. Затем на протяжении суток мы совместно с коллегами из „МегаФона“ корректировали политики блокировки, после чего, наглядно убедившись в эффективности решения, перешли от пилотного тестирования к внедрению в промышленную эксплуатацию»,— рассказал Александр Замулин, руководитель Центра управления рисками Страхового дома ВСК. По его словам, если бы кибератака оказалась успешной, это остановило бы на ее время продажи по дистанционному каналу.

Что предпринимают компании

В текущем году информационная защищенность стала одним из основных приоритетов для многих организаций. Активнее прочих этим занимается госсектор, отмечает замгендиректора Infosecurity a Softline Company Сергей Пыжик. Госорганизации наращивают защищенность «особенно активно, так как они у всех на виду», полагает Александр Осипов. После начала СВО на Украине IT-системы российского госсектора попали под прицел хактивистов со всего мира. Так, в марте хакерской атаке подверглась Росавиация, в апреле — Минкультуры и региональные администрации, в сентябре — платежная система «Мир» и серверы правительства Москвы. На фоне атак закупки госсектором средств для доработки информационных систем и усиления защищенности от кибератак выросли с 20 февраля по 20 апреля на 10% в штуках и 12% в деньгах.

Интерес бизнеса относительно закупок средств кибербезопасности склоняется в сторону импортозамещающих российских продуктов и решений, рассказывает господин Пыжик. По его словам, заказчики видят риски в сотрудничестве с зарубежными компаниями, так как они в любое время могут покинуть рынок. Так, после начала военных действий с российского рынка ушли словацкая ESET, чешская Avast, американские Fortinet, NortonLifeLock Inc., Forcepoint (Websense), Cisco Systems и другие компании из сферы кибербезопасности. Российские игроки, у которых остались контракты с иностранными вендорами, пытаются «выжать из сотрудничества максимум и не допустить дополнительных расходов на закупку альтернатив», параллельно с этим происходит активное пилотирование отечественных решений, рассказывает Сергей Пыжик.

Про повышение интереса бизнеса к средствам кибербезопасности говорят финансовые результаты работы отечественных вендоров — например, по итогам первого полугодия объем продаж Positive Technologies вырос на 72%, увеличившись с 1,8 млрд до 3,1 млрд руб. по сравнению с аналогичным периодом прошлого года, рассказали в компании. В «Лаборатории Касперского» после ухода западных игроков видят «существенное увеличение спроса» на все классы решений, поскольку компаниям нужно заменить продукты, которые перестали полноценно функционировать, на отечественные, рассказал руководитель отдела предпродажной поддержки компании Евгений Бударин.

Однако закупка средств защиты информации и импортозамещение не всегда решают проблему защищенности, так как бОльшая часть сливов данных является результатом не внешних атак, а внутренних нарушений, подчас непреднамеренных, указывает Александр Осипов. Так, от недобросовестных действий сотрудников в апреле—мае материальный ущерб понесли 87% из опрошенных «Ростелеком-Солар» компаний.

Впрочем, отмечает эксперт, в последнее время интерес компаний к повышению цифровой грамотности сотрудников растет — так, спрос на решение «МегаФон Security Awareness» увеличился в нынешнем году в четыре раза по сравнению с 2021 годом. Этот продукт представляет собой платформу для обучения сотрудников ИБ. Она содержит материалы с правилами корпоративной цифровой гигиены, а также позволяет проверить полученные сотрудниками знания на практике. Платформа может имитировать фишинговые атаки. С помощью этой функции IT-департамент оперативно выяснит, кто из сотрудников пока является уязвимым звеном, чтобы назначить дополнительное обучение. Его периодичность и частоту тренировочных атак каждая компания может настроить под себя в зависимости от внутренней политики безопасности.

Интерес бизнеса вырос не только к тестированию бдительности сотрудников, но и к тестированию инфраструктуры компании в целом. Так, рост востребованности пентестов с начала года составил более 200%, рассказали в «МегаФоне». Возросший интерес компаний к подобным тестированиям отмечал и министр Максут Шадаев в кулуарах Петербургского международного экономического форума. Пентест — тестирование защищенности инфраструктуры компании в «боевых условиях»: «белые хакеры» атакуют IT-системы, анализируют код и внешний сетевой периметр, после чего представляют заказчику отчет о найденных уязвимостях и способах их устранения. Подобная проверка позволяет определить наиболее вероятные и опасные векторы атак для конкретной IT-системы.

Взгляд в будущее

Количество взломов и утечек в крупных и среднекрупных компаниях может увеличиться за счет того, что хакеры уже заразили своих жертв, но еще не активировали вредоносы, полагает Александр Осипов. Так, при расследовании атаки на одного из клиентов «МегаФона» обнаружилось, что до активации вирус спал в его инфраструктуре в течение пяти месяцев. «Поэтому тот факт, что у компании есть средства информационной защиты, не значит, что они работают в формате „нашел, удалил и заблокировал“,— рассказывает эксперт.— Они могут работать по принципу „проблема найдена“, то есть факт „сработки“ произошел, но гарантий того, что IT-инфраструктура защищена, нет».

Поэтому, с одной стороны, действительно необходимы пентесты и «белый хакинг», с другой — состав инфраструктуры, кроссфункциональное взаимодействие и процессы реагирования должны быть максимально прозрачны для сотрудников ИБ и всех участников обеспечения киберзащиты в компании, подчеркивает господин Осипов. Особое внимание защите следует уделять организациям ВПК — таргетирование кибератак будет смещаться на них. В Positive Technologies прогнозируют рост кибератак, разработанных с применением техник и вредоносного ПО, ориентированного под ОС Linux. На эту операционную систему сейчас активно переходят отечественные компании.

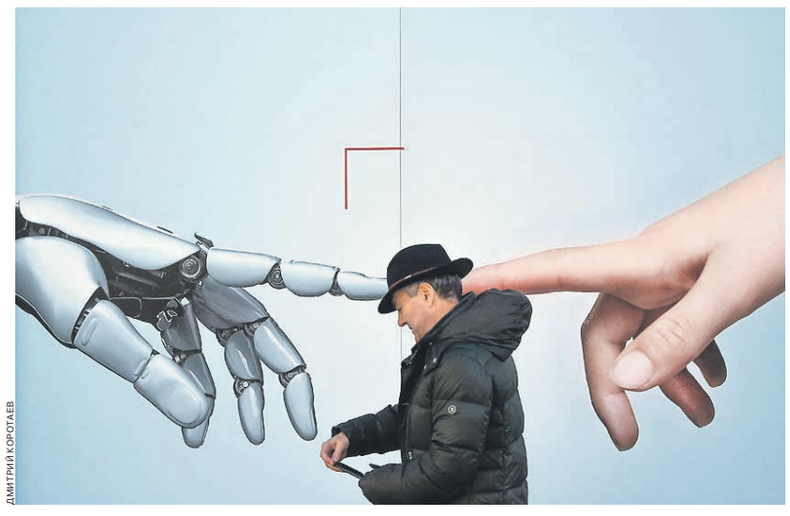
Кроме того, важно помнить о личной ИБ, напоминают эксперты. Растет число мошеннических звонков физическим лицам: количество жалоб на них среди пользователей приложения Kaspersky Who Calls в августе увеличилось в два раза по сравнению с июлем и июнем. «МегаФон» уже имеет решение, которое позволяет операторам блокировать звонки с подменой номера. Важной особенностью данного решения является то, что оно должно быть установлено как в сети оператора, принимающего звонки, так и в сети оператора—инициатора вызова. Сейчас такая система работает также в сетях нескольких других операторов. С ее помощью ежедневно блокируются более 1 млн звонков с подменой номера.

Юлия Степанова

Над пропастью 6G

— связь —

Эксперты сходятся во мнении: страна, которая сможет одной из первых освоить 6G и развернуть сети этого поколения, обеспечит себе внушительный задел в дальнейшем технологическом развитии. Китай и США уже оспаривают первенство в работе над частотными испытаниями 6G, инвестируя в них огромные суммы, но исследования электромагнитной совместимости и безопасности абонентов, которые начали в текущем году «Сколтех» и Научно-исследовательский институт радио, тоже весьма примечательны. Впрочем, какой в этом смысл, если у России до сих пор нет сетей пятого поколения в коммерческом применении? „Ъ“ опросил экспертов, что они думают о развитии сразу 6G, без предыдущей стадии?



ДМИТРИЙ КОРОТАЕВ

Пятым будешь?

Чтобы стать реальностью, 6G нужно еще по меньшей мере десять лет. Благодаря в 100 раз большей скорости передачи данных, чем пиковая у 5G, это поколение связи сделает возможными технологии, которые долгое время были предметом научной фантастики: от голограмм в реальном времени до летающих такси и подключенных к интернету человеческих тел и мозгов. Для правительств целых стран, не только для бизнеса, ставки сегодня очень высоки.

Российское правительство обещает представить первые прототипы отечественного оборудования связи 6G к 2025 году. В то же время другие страны еще даже не определились, что подразумевать под этой технологией. Международный союз электросвязи приступит к формированию технического стандарта только в 2027 году, следует из данных Next G Alliance.

Начало работы над 6G удивительно, учитывая, что в России еще не развернуты сети пятого поколения мобильной связи. Сетей 5G в коммерческой эксплуатации у российских операторов нет, поскольку они не могут получить частоты в наиболее подходящем «золотом диапазоне» 3,4–3,8 ГГц — он используется практически во всем мире, но в России занят спецслужбами и военными. Еще одно препятствие для 5G в РФ — обязанность операторов строить сети пятого поколения на отечественном оборудовании, которого пока нет.

Может, и не строить столь проблематичные сети пятого поколения, которые так и не заработали из-за занятых военными и спецслужбами частот, и сразу перейти к освоению шестого?

Руководитель фабрики инженерных проектов «Симметрия» Сергей Додонов считает, что четко выраженных стадий у поколений мобильной связи вообще связи нет — это рынок выбирает те или иные форматы: «Имеют значение только частота и объем переданных данных на единицу времени». Аналитик Mforum Алексей Бойко полагает, что это принципиально невозможно. 6G — это технология, дополняющая 5G, а не альтернатива ей. «Технологии мобильной связи устроены так, что каждое последующее поколение базируется на предыдущем»,— согласен гендиректор TelecomDaily Денис Кусков.

Тем не менее гендиректор подведомственного Минцифры НИИ радио Олег Иванов говорит, что задачи «проскочить» 5G не стоит — просто на услуги на базе сетей 5G в России сейчас нет достаточного спроса. Первые четыре поколения связи в основном были направлены на удовлетворение потребности людей в межличностной коммуникации. Новые же поколения будут использоваться преимущественно при взаимодействии машин с машинами, а не людьми, поясняет он.

«Смысл в развертывании 5G прежде всего в том, чтобы защитить уже сделанные инвестиции. Ведь если не внедрять 5G, то по мере роста трафика качество работы сетей LTE будет неизбежно снижаться»,— возражает Алексей Бойко.

На данный момент без 5G можно обходиться — объем трафика в мобильных сетях еще не превысил критических значений, поясняет гендиректор «ТМТ Консалтинг» Константин Анкилов, вопрос в том, насколько хватит ресурсов технологии связи четвертого поколения.

Массовый запуск сетей 4G в России начался в 2012 году, до 2018 года 3G оставалась ведущим стандартом связи на рынке. То же самое будет и с пятым поколением. Даже если запустить 5G прямо сейчас, до 2024–2026 годов 4G будет являться опорной технологией для операторов для оказания услуг абонентам, считает Денис Кусков. Так что поздний запуск сетей 5G может только сократить срок использования этой технологии в России, но отменить ее — нет, заключает он.

На чужих чипах

Что нужно сделать, чтобы развернуть коммерческие сети пятого поколения? Сети российских операторов находятся в высокой степени готовности к предоставлению услуг 5G, полагает Алексей Бойко. «Мы бы уже не один год имели возможность пользования 5G в России как минимум в крупных городах, если бы не позиция, занятая регуляторами»,— говорит он.

Запустить в производство оборудование 5G отечественной сборки можно, но оно будет со значительной долей зарубежных электронных комплектующих, продолжает аналитик, а это приведет к росту зависимости российских производителей от поставок из Китая. Кроме того, отечественное решение, скорее всего, будет заметно более дорогим, если сравнивать его с глобальными вендорами, что повлечет необходимость больших инвестиций от операторов или господдержки. Это, в свою очередь, скажется на тарифах операторов, подчеркнул он.

По мнению Дениса Кускова, строить сети 5G можно путем замены всего оборудования операторов «под ключ» или же меняя только базовые станции. «В первом случае необходимо наладить массовое производство оборудования, что сложно и затратно, да и на локализацию производства необходимых комплектующих надежды нет. А во втором — решать проблемы совместимости с уже имеющимися сетями, что тоже весьма непросто»,— пояснил он.

По мнению Алексея Бойко, более позднее внедрение новых технологий может дать выигрыш, поскольку позволяет не набивать шишки, что характерно для первопроходцев, а также экономить на инвестициях, так как к моменту зрелости технологии стоимость решений снижается в несколько раз. Но плата за задержку с очередным поколением связи — общее негативное влияние на экономику страны из-за опоздания с внедрением новых технологий и сервисов, добавляет он.

Проблемы поколений

6G — это технология следующего десятилетия: появления первых сетей стоить ожидать в 2030-х годах, рассуждает Константин Анкилов. Однако сложности с внедрением 5G только подтверждают необходимость как можно раньше начать заниматься следующим поколением, подчеркивает Олег Иванов.

По его мнению, 6G — необходимое условие для новой технологической революции, в которой основную роль будут играть автономные системы. Для взаимодействия между ними очень важна сеть с быстрой передачей громадных объемов данных. Он приводит в пример автономные автомобили, которые напичканы датчиками и радарами для анализа дороги и окружающего пространства: «Когда таких машин мало, то этот подход оправдан, но когда их станет много, точно появится необходимость взаимодействия между машинами, а также между машиной и дорожной инфраструктурой. Такие коммуникации возможны только в рамках 6G».

Операторы не считают, что государство торопится с исследованием технологии мобильной связи шестого поколения. Так, в «МегаФоне» «приветствуют любые российские научные изыскания в сфере 6G», а в Tele2 называют это направление «очень важным для развития телеком-отрасли», добавляя, что вопрос определения частотного ресурса для 6G при этом должен быть основополагающим.

Подводные камни 6G

С какими проблемами неизменно придется столкнуться при разработке 6G? Алексей Бойко напоминает, что 6G не подходит для обеспечения непрерывного покрытия в городе. Радиоволны с частотами в сотни гигагерц не могут пробиться даже через тетрадный лист. Помехи для них могут создавать даже молекулы газов воздуха, объясняет он. 6G будет использоваться прежде всего для передачи данных, очень объемных и очень быстро, однако на весьма небольшие расстояния: от сантиметров до нескольких метров.

Самая большая проблема состоит не только в передаче сигнала на определенных частотах, но и в принимающем оборудовании (модемах, антеннах и др.), которое работает в связке с трансляционными сетями, обращает внимание Сергей Додонов. Для перехода на новый стандарт оно должно быть совместимо и собрано в единый комплекс. Также для строительства сетей 6G придется решать проблему совместимости с текущим оборудованием и пересматривать стандарты монтажа подобного рода приборов. «Необходима глобальная кооперация многих инженерных школ, чтобы создать подобный стандарт передачи данных. Это займет годы исследований и разработок»,— уверен он.

На безымянной полосе

Впрочем, НИИ радио вместе со Сколтехом уже направили в Минцифры свои предложения по мероприятиям, которые надо делать прямо сейчас, напоминает Олег Иванов. Прежде всего нужно подобрать диапазон частот, который уже доступен или можно его освободить. Это даст возможность предлагать эти частоты на международных площадках, поясняет господин Иванов.

Кроме того, по его словам, необходимо решить сугубо технические вопросы (на каком расстоянии друг от друга должны будут находиться базовые станции 6G, с какой мощностью они должны работать и др.) и проблему электромагнитной безопасности. «Мы уходим вверх по спектру, эти диапазоны радиоизлучений пока не исследованы с точки зрения воздействия на живые организмы,— рассуждает он.— Если мы обнаружим, что воздействие сети 6G на человека недопустимо, то нам нужно будет вернуться на шаг назад и искать другие диапазоны или изменить режим работы сети таким образом, чтобы она не оказывала вреда».

Еще одним вопросом станет производство отечественного оборудования и электронной компонентной базы. Если сейчас срочно не заняться этими вопросами, никакой технологической независимости в сфере телекоммуникаций достичь не получится, резюмирует господин Иванов.

Анастасия Гаврилюк

информационные технологии

«На импортозамещение технологий в сельском хозяйстве России хватит одного года»

Построение экосистем вокруг банков — в числе ключевых трендов финансового рынка последних лет. Одна из самых удачных и востребованных получилась у Россельхозбанка. Он объединил в собственной цифровой экосистеме «Свое» десятки тысяч фермеров и поставщиков сельхозоборудования. Лидер этого проекта директор Центра развития финансовых технологий Россельхозбанка **Елена Батурова** в интервью рассказала о высокой степени готовности агропромышленного комплекса (АПК) к импортозамещению технологий и назвала главный фактор роста индустрии.



ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ РОССЕЛЬХОЗБАНКА

— первые лица —

— Как вы оцениваете уровень использования технологий в сельском хозяйстве сейчас и что, по-вашему, предстоит сделать в этом направлении в ближайший год, в том числе в части импортозамещения технологий?

— Отрасль на 9,5 балла из 10 готова к сложившейся ситуации. Есть ряд задач в производстве деталей для сельхозтехники, есть вопросы по генетике и селекции, но все это можно решить за год — глобального отставания в отрасли не существует.

Технологии, которые помогают аграриям в решении различного рода производственных задач, можно условно разделить на три категории: технологии «до фермы», «на ферме» и «после фермы». Долгое время инвесторам представлялась привлекательной именно последняя категория. Маркетплейсы, решения для сбыта продукции, сервисы доставки получали максимальный объем инвестиций. Инвесторов привлекали простота технологий, короткий срок выхода на окупаемость, небольшой объем инвестиций для запуска MVP-продукта. Но быстрое развитие технологий искусственного интеллекта и интернета вещей существенно изменило подход к организации производственного процесса в сельском хозяйстве. Системы дистанционного управления производством, позволяющие с помощью снимков с неба отслеживать состояние посевов и корректировать применение удобрений или средств защиты растений, автономные сельскохозяйственные роботы, IoT-технологии и многие другие решения уже сегодня успешно применяются как в крупных российских агрохолдингах, так и в фермерских хозяйствах. 90% этих технологий разработаны в России, они созданы российскими инженерами и предпринимателями.

Категория технологий «до фермы» тоже очень интересная. К этой категории относятся прежде всего технологии, связанные с созданием новых типов удобрений, средств защиты растений, семян и т. д. Раньше селекция и генетика была автономной наукой — чтобы ее применять, нужно было разбираться исключительно в биологии, средний срок вывода нового продукта на рынок составлял 10–15 лет.

Тренд последнего года — соединение знаний в биологии с технологиями искусственного интеллекта, что позволяет гораздо быстрее формировать гипотезы по необходимости внесения изменений в гены растений для улучшения их характеристик. Переход от спорной для многих технологии генной модификации к технологии генного редактирования и применение технологий искусственного интеллекта позволяют сократить срок вывода нового вида семян на рынок в три-пять раз. Использование современных научных достижений на фундаментальной российской научной базе поможет нам сэкономить в этом процессе десятки лет. Россия показывает хорошие результаты в генетике и селекции. Уверена, что в течение двух-трех лет достигнем больших успехов в этом направлении.

— Какие технологии могут обеспечить настоящий прорыв в АПК?

— Есть прекрасный проект AgroCode Hub. Он объединяет всех, кому интересны современные технологии в сельском хозяйстве, и раз в год награждает лучшие агротех-компании. Поддерживая этот проект, мы находимся на переднем краю прогресса в сельском хозяйстве и видим, что сейчас революцию могут совершить новые достижения в области биотехнологий.

Например, производство растительного белка. Немногие знают, что растительный белок — это не просто замена натурального мяса, это в том числе альтернативное питание для людей, испытывающих определенные проблемы со здоровьем. Новые виды биологических удобрений, использующие бактерии в качестве транспорта для доставки питательных веществ к корням растений, новые органические средства защиты растений — все это кардинальным образом меняет существующий подход, повышает его эффективность, позволяет создавать натуральные продукты питания в промышленных масштабах.

Многие технологии в биотехе имеют много общего с технологиями, используемыми в химической промышленности или при производстве известных нам уже сейчас продуктов питания. Поэтому у России очень хороший фундамент и большие перспективы.

Также мы с оптимизмом смотрим на развитие в России вертикальных ферм. Погодные условия, качество почвы, наличие ее в достаточном количестве для посадок культур — теперь это уже не так важно. Вертикальные фермы позволяют выращивать сельхозкультуры там, где раньше это было невозможно. Да, затраты на производство на таких фермах выше, чем при обычном земледелии, но при учете логистики их привлекательность значительно повышается.

— А сами фермеры готовы к насыщению технологиями и их использованию?

— Мы постоянно получаем обратную связь от наших клиентов, а это около 100 тыс. сельхозпроизводителей. Банк знает потребности своих клиентов до самых мельчайших деталей, так как проходит с ними весь путь от выбора места для ведения хозяйства до продажи товаров конечному потребителю. Например, есть потомственные фермеры с большой историей. Так вот даже они мечтают о технологиях. При этом у них высокий уровень технических знаний, который отличает исключительно российских фермеров — они, например, сами могут заказать в интернете разные детали и сами собрать из них работоспособное устройство.

— РСХБ — опорный банк АПК. В вопросах цифровизации сельского хозяйства вы тоже опора? Что конкретно вам уже удалось сделать и как вы будете двигаться дальше?

— Мы выбрали для себя ряд приоритетных направлений, объединив их под брендом «Свое», и активно развиваемся. Среди них — помощь малому и микробизнесу, для которого мы развиваем маркетплейс фермерской продукции «Свое Родное» (9,5 тыс. участников в сегменте B2C работает по всей стране), платформу продажи агротуров и гастрономических туров по всей России «Свое. За городом», B2B-экосистему «Свое Фермерство», которая помогает в поиске товаров и сырья, необходимых для производства сельхозпродукции, содержит самый большой в России онлайн-магазин цифровых сервисов для аграриев и платформу для поиска практических навыков и знаний «Агромнение». Мы развиваем площадки «Свое Жилье» для подбора недвижимости в городе и «Свое Село» для строительства дома в сельской местности. Это был базовый минимум, который мы создали в кратчайшие сроки.

Теперь мы перешли ко второму этапу. Мы недавно запустили платформу по образованию и поиску работы в сельском хозяйстве «Я в агро». Здесь можно узнать много нового и сориентироваться в отрасли, выбрать профессию, вуз, найти стажировку и получить предложение о работе. Престиж отрасли АПК как работодателя растет, а задачи становятся все более интересными и технологически емкими.

Любые достижения в отрасли невозможны без квалифицированных специалистов. Наша задача — привлечь в сельское хозяйство молодых, перспективных, творческих людей. Дать условия для развития. Сейчас мы уже практически завершаем эту работу. И совсем скоро мы увидим результат.

Студентам ведущих вузов страны мы предлагаем возможность получать именные стипендии, а в дальнейшем попробовать свои силы в создании новых сервисов для обучения и профессионального развития в агротехе. Кроме того, мы постоянно сотрудничаем с вузами и развиваем совместные кафедры.

А бесплатная для учеников «Школа фермера» выросла во всероссийскую образовательную инициативу обучения аграрным профессиям. Благодаря проекту подготовлено почти 2 тыс. квалифицированных аграриев в 53 регионах.

— Недавно банк запустил проект «АгроИнвестКлуб». Какова сверхидея этого проекта? Насколько стартапы в принципе способны усилить отрасль прямо сейчас?

— Стартапы — как маленькие дети. Чтобы дети стали успешными и умными, им необходима поддержка. У маленьких компаний есть креатив и желание, но без финансовой подпитки, без понимания, где найти покупателя и как довести продукт до финального состояния, очень проблематично развиваться. В России в агротехе много талантливых стартапов. Часть из них мы знаем лично и хорошо понимаем, чем они живут и какие технологии внедряют. Мы хотим им помочь найти партнеров или покупателей. Именно это является основной целью «АгроИнвестКлуба». Мы хотим дать возможность новым проектам в АПК обмениваться опытом, хотим заниматься трансфером технологий из России в дружественные нам страны и, наоборот, из дружественных стран в Россию, приглашать оттуда потенциальных инвесторов и последовательно объединить российские стартапы со стартапами из Белоруссии, Бразилии, Индии, Китая и ЮАР.

Американская модель инвестирования, при которой миллионы долларов могли вкладываться исключительно под обещания харизматичных лидеров и красивые презентации, себя изживает. Мы выступаем за прагматичный подход в инвестировании, стремимся соединить технологические команды не только с инвесторами, но и реальными потребителями их продукции. Как сказал один из классиков японской литературы Кодзиро Сэридзава, «для того, чтобы вырасти настоящим человеком и им оставаться всю жизнь, надо всегда быть чуточку голодным».

Беседовал Евгений Паладьев

В параллельной реальности

— параллельный импорт —

Параллельный импорт в IT дает возможность избежать дефицита оборудования и выиграть время на поиск альтернативных вариантов и разработку собственных решений. Однако пока минусов больше, чем плюсов: такие поставки нестабильны, дороги и могут негативно отразиться на информационной безопасности (ИБ) организации.



АНАТОЛИЙ ЖДАНОВ

После 24 февраля об уходе с российского рынка или о приостановке работы объявили десятки компаний. В ответ Россия разрешила параллельный импорт: ввозить в страну партии товаров определенных брендов (в том числе технику, электронику, смартфоны) без разрешения правообладателя. До этого компании были обязаны выплачивать штраф за параллельный импорт — до 5 млн руб.— в качестве компенсации и в ряде случаев уничтожать сами товары.

Для IT-отрасли это способ решить проблему доступности оборудования в условиях ухода множества зарубежных производителей. Однако многие считают, что эта мера не способна полностью закрыть слабые места и обеспечить регулярные поставки по приемлемым ценам.

Что можно ввозить

В перечень товаров, разрешенных к параллельному ввозу, включены продукты: APC, Schneider Electric, Delta Electronics, HP, Tripp Lite, MSI, Intel, Microsoft, Cisco, Dell, Oracle, Hitachi, Huawei Enterprise, IBM и др., перечисляет управляющий партнер ГК IT Expert Михаил Грибов. «Фактически закон разрешает параллельный импорт всей электроники, к которой мы привыкли. В частности, Samsung, Asus, PlayStation, Xbox и пр.»,— продолжает технический директор Swordfish Security Антон Башарин.

По мнению гендиректора ООО «НИИ СОКБ Центр разработки“» Игоря Калайды, такой импорт помогает решить проблему доступности новых смартфонов или ноутбуков с предустановленными новыми версиями операционных систем, но не в состоянии полностью решить проблему доступности IT-оборудования для инфраструктурных решений. «Применительно к такой категории, как базовая IT-инфраструктура, параллельные схемы решают проблему по принципу „латания дыр“, то есть бессистемно,— сетует гендиректор компании „Аэродиск“ Вячеслав Володкович.— Обеспечить стабильный, гарантированный канал поставок качественного „железа“ под большой проект или задачу масштабирования со всем необходимым сопровождением невозможно».

Как меняются цены и маршрут

Проблемы, сопутствующие параллельному импорту, взаимосвязаны — это прежде всего цены и логистика. «Цена на IT-оборудование уже выросла по некоторым позициям на 80–100%,— обращает внимание IT-директор hh.ru Геннадий Береговский.— Но в марте—апреле цены были еще выше из-за ажиотажного спроса. Так что сейчас они незначительно снизились, но еще существенно выше начала февраля». Классическая схема поставки обычно выглядит так: производитель—дистрибутор—склад—продажи через партнеров. «Сейчас же история носит более бутиковый вариант: производитель против, дистрибутора может и не быть, на складах ничего нет, заказчики самостоятельно ищут тех, кто готов ввезти „под ключ“»,— объясняет руководитель отдела ИБ СДЭК Павел Куликов.

Увеличение логистических цепочек отражается на сроках поставок и цене для конечного потребителя. «Например, мы возим электронику как составляющую оборудования для машино- и судостроения. Даже если речь идет о европейских производителях, мы везем через Азию, что удорожает и стоимость поставки, и саму закупку»,— рассказывает гендиректор транспортно-логистической компании «Мультитранспорт» Людмила Корсуновская. В итоге, по ее словам, такая электроника для конечного потребителя подорожала примерно вдвое. Скорость и сроки поставок тоже изменились: возможности работать напрямую с европейскими поставщиками нет, нужен транзит через Азию, продолжает она: «В азиатской части страны не такая развитая инфраструктура, как в европейской. В результате большие очереди и в порту, и на сухопутных границах».

После изменения каналов поставок стоимость техники в сегменте пользовательского оборудования выросла на 20–40%, оценивает руководитель направления «Системная интеграция» в «КОРУС Консалтинг» Владислав Бахаудинов. «Больше всего, до 120%, в цене выросло высокотехнологичное оборудование: это серверное, сетевое „железо“ и сопутствующее ПО. Ведущие производители IT-оборудования отказываются предоставлять те же условия закупки, что и раньше, приходится брать оборудование по „рекомендованным ценам“, которые в два раза выше, чем специальные»,— поясняет он. Ситуацию осложняет тот факт, что, по словам замдиректора департамента консалтинга ГК Innostage Марата Залотдинова, сегодня на рынке отсутствует возможность оплаты оборудования постфактум или с отсрочкой — можно оплатить только сразу. Предоплата, в свою очередь, не дает гарантии оперативной доставки оборудования.

Цепочка поставок увеличена за счет добавления дополнительных участников, в долларах цена выросла на 5–25%, говорит представитель BuyCisco, дистрибутора оборудования Cisco, HPE и Dell, Юрий Бондаренко: «К примеру, Китай после начала СВО поднял цены на 10%, Турция — на 15%. Расходы с оплатой и логистикой увеличивают цену еще примерно на 5%».

Компания поставляет в Россию оборудование по каналам параллельного импорта. «Мы закупаем по всему миру, чаще это Китай, ЕС, США, Канада, а везем через страны Евразийского экономического союза,— говорит господин Бондаренко.— Но сроки поставки зависят от многих факторов, и один из них — наличие оборудования на складах. Если его нет, нужно заказывать производство, время на которое у каждого вендора разное. Для HPE и Dell это 3–4-месяца, у Cisco — от 7 до 12 месяцев».

Чем и кто рискует

К этим срокам прибавляются не только время на обходной путь доставки, но и на поиски этих альтернативных каналов, которые тоже могут вырасти — из-за частичной мобилизации сотрудников во всех отраслях.

Людмила Корсуновская называет параллельный импорт «ручной вышивкой», требующей навыков и большого опыта работы в отрасли. «Это не классические поставки, где все отлажено и специалистов внутри одной команды легко заменить,— рассуждает она.— Призыв сотрудников логистической компании — большая потеря для ее руководителей и существенный удар по логистике в целом. Это профессионалы, которые умеют работать со всеми видами транспорта, обладают знаниями в области таможенного оформления грузов. Потеря ключевых сотрудников будет очень критична для бизнеса».

Для конечных заказчиков рисков тоже много. Самое ценное в современном IT-оборудовании — это слой ПО, которое управляет «железом» и обеспечивает уникальные возможности, из-за которых его и покупают. «Без официальной поддержки вендора сопровождение ПО невозможно, соответственно, придется все это как-то обходить. Но это приведет к потере качества работы, снижению отказоустойчивости, а также повышает риски „окирпичивания“, то есть отключения вендором базовых функций решения»,— предупреждает Вячеслав Володкович. В итоге ввезенные решения станут менее функциональными и более уязвимыми. «ПО будет необходимо взламывать и обновлять, проводить диагностику»,— предостерегает Михаил Грибов.

Поддержка будет замедляться, а цены на нее будут расти крайне высокими темпами из-за дефицита специалистов с компетенциями в оборудовании различных вендоров, говорят эксперты. Причем эти кадры останутся без доступа к официальным консультациям вендора и документации.

Павел Куликов называет основные риски в ИБ: отсутствие обновлений и поддержки, остановка функционирования и гипотетическое наличие «закладок» в поставляемое в Россию оборудовании. Главная сложность связана именно с обновлениями, считает Антон Башарин. «Когда появляются опасные уязвимости, злоумышленники оперативно о них узнают. И если не происходит своевременного обновления, они могут атаковать системы. Быстрее всех выпустить „патч“ может только производитель. Например, недавняя уязвимость в Log4j, которая позволяет выполнить код на удаленном хосте (RCE) и имеет наивысшую оценку критичности. Данная библиотека активно использовалась в продуктах Microsoft, Oracle, VMWare. Исправление и обновление выпустили оперативно, но без доступа к порталу поддержки получить их нельзя»,— рассказывает он.

Кто выиграет

Большим интеграторам и дистрибуторам параллельный импорт вряд ли выгоден: в течение 20 лет они официально работали по хорошо отлаженным каналам поставки и сейчас вынуждены перестраиваться. «Да и после возможного снятия санкций производители оборудования могут отказаться работать с крупными дистрибуторами из-за того, что они занимались параллельным импортом»,— рассуждает технический директор Skillaz Дамир Шияфетдинов.

Впрочем, и в сценарии, при котором западные вендоры не вернутся в Россию никогда, излишняя ставка на параллельный импорт — это «путешествие с конечной остановкой», считает господин Володкович. «Если пренебрегать развитием альтернативных IT-решений, таким как российские разработки и open source, можно в какой-то момент обнаружить себя в числе безнадежных аутсайдеров рынка»,— предупреждает он.

Конечный потребитель от параллельного импорта в IT если и выигрывает, то только «здесь и сейчас». Пока у него все же есть возможность купить, пусть втридорога и с дополнительными рисками нужное оборудование, чтобы продолжить работать. Больше всего страдает проектный бизнес: раньше, когда заказчики не могли оплатить дорогостоящее оборудование одним чеком, их кредитовали дистрибуторы. Сейчас же нужна 100-процентная предоплата.

Анастасия Жигач

ЛАНИТ

Времена кода

Одна из самых обсуждаемых тем и главных тенденций последних лет в IT-отрасли — рост востребованности Low-Code, то есть разработки с минимальным использованием кода. В результате появляются решения, не требующие при настройке и модификации написания программного кода. По прогнозам Research and Markets, за 2020–2030 годы рынок Low/No-Code увеличится с $10,3 млрд до $187 млрд со среднегодовым темпом роста 31,1%. Почему Low-Code становится таким популярным, в чем его преимущества в сравнении с классической разработкой и какие сферы наиболее перспективны для развития Low-Code платформ?



GETTY IMAGES

— программирование —

Предпосылочный ящик

Согласно общему мнению экспертов, уже через несколько лет рынок разработки будет выглядеть совсем не так, как сегодня. К 2026 году более 40% организаций будут полагаться на платформы и инструменты Low-Code для создания интеллектуальных пользовательских приложений, затратив на развертывание на 33% меньше усилий, прогнозирует IDC. Другую оценку для этого сегмента приводит Gartner: к 2024 году более 65% разрабатываемых приложений будет построено с помощью инструментов Low-Code. Такие «оценки» позволили авторитетному журналу о технологиях SD Times назвать 2021 год годом Low-Code платформ.

Как бизнес пришел к тому, что Low-Code может выручить его во многих ситуациях?

Во многом взрывной рост интереса к такой разработке вызван пандемией и, как следствие, самоизоляцией, на которую пришлось пойти сотрудникам огромного числа компаний. Люди начали работать из дома — компаниям понадобились новые приложения, чтобы управлять проектами, выполнять заказы и работать с клиентами. При этом решение нужно было срочно, а обычная разработка не успевала за спросом. Помогли Low-Code платформы, которые позволяют собирать приложения без кода, пишет SD Times.

Кроме того, на руку популярности Low-Code сыграло и большое количество инициатив, связанных с цифровизацией и автоматизацией «буквально всего и вся», объясняет директор по продвижению продуктовых решений Goodt (входит в группу ЛАНИТ) Иван Лихачев. Раньше, по его словам, был некий базис: бухгалтерия, ERP, склады, банковские системы. «Сейчас автоматизировано все вплоть до заказа пропусков. Любое действие переведено или переводится в „цифру“,— говорит он.— Важным требованием и условием становится нормальная автоматизация с минимумом усилий и действий со стороны человека. Это задало темп большому количеству проектов и, как следствие, обусловило рост потребности в приложениях и разработке».

Предпосылки для появления Low-Code — современные технологические вызовы, связанные с усложнением разработки корпоративных систем, продолжает Александр Наймарк, директор департамента продуктовой разработки НОРБИТ (входит в группу ЛАНИТ). Low-Code стал именно тем инструментом, с помощью которого команды архитекторов и аналитиков могли эффективнее понимать и решать задачи заказчика, делится наблюдениями он.

Еще одна причина востребованности Low-Code — прекращение в 2022 году работы в России крупных иностранных IT-компаний, «забравших» с собой решения, которые фактически были платформами для разработки вспомогательных приложений. Многие, по словам Ивана Лихачева, использовали их в работе годами, успели привыкнуть к функциям, действиям и готовым правилам. Однако уход таких решений с рынка не парализовал работу во многом благодаря использованию Low-Code.

Темпы цифровизации также повлияли на потребности бизнеса в сотрудниках, создающих информационные системы, и теперь они нужны как никогда раньше. Вместе с тем налицо проблема быстрого обучения новых программистов, рассуждает директор по платформе ТУРБО X «Консист Бизнес Групп» (входит в группу ЛАНИТ) Сергей Бобрецов. «Потребовалось искать другие способы восполнения дефицита сотрудников. Простой вход в разработку через Low-Code дает определенный импульс в найме, но при этом требует принципиально другого методологического подхода в развитии персонала»,— рассказывает он о том, как Low-Code стал одним из вариантов для компаний, нуждающихся в IT-специалистах.

Преимущества подхода

На самом деле Low-Code платформы существуют уже много лет, но раньше на эти решения смотрели свысока, будто они не подходят для ответственных приложений, говорят эксперты. Однако польза таких инструментов видна все отчетливее.

Что же представляет собой Low-Code? Это модель создания и модификации систем и приложений, требующая минимального написания программного кода. «Технология, с одной стороны, позволяет собирать какое-либо решение или процесс из готовых блоков, с другой — дает возможность что-то дополнить, дописать скрипт, добавить ячейку для более глубокой кастомизации решения. Мы используем это на нашей платформе Insight, которая позволяет разрабатывать аналитические приложения и все, что связано с данными»,— рассуждает Иван Лихачев. «Чистую» разработку он сравнивает с пустым листом, на котором можно написать все, что угодно, а Low-Code — с листом, на который нанесены точки, и их нужно соединить линиями, чтобы получился рисунок.

Ключевым плюсом метода эксперты называют «гибкость и сокращение параметра time-to-market» (время от начала разработки идеи до ее конечной реализации и вывода на рынок). Сначала заказчик формулирует набор гипотез, которые хотел бы развивать, но к моменту завершения проектирования и разработки требования могут устареть, карта процессов и ключевые метрики — измениться, а пользователи — уволиться. «Целевое решение может кардинально отличаться от первоначальной идеи,— отмечает Александр Наймарк.— Программные решения, реализуемые по принципу Low-Code, конфигурируются быстрее. Например, заказчик на нашей платформе NBT, получая результат, может корректировать гипотезы, способы решения или даже оптимизировать бизнес-процессы в компании».

О time-to-market говорит и Иван Лихачев, приводя в пример ситуацию, когда есть много инициатив, которые нужно реализовать быстро, но специалистов для этого нет. Решением выступает «полуготовый конструктор», с которым можно оперативно создавать приложения под требования бизнеса. «Гибкость — ключевой момент: то, что разрабатывается сегодня, не высекается в камне. Постоянно требуются уточнения, модернизация, у бизнеса появляются новые идеи,— рассказывает он.— В таких условиях у Low-Code очевидные преимущества: он позволяет переконструировать и заново собрать любой процесс».

Как объясняют специалисты, помимо этого подход обладает целым рядом других плюсов. Среди них — быстрая окупаемость затрат за счет более гибкого изменения алгоритмов через Low-Code по сравнению с кодированием, а также высокая скорость обучения и ограниченный набор необходимых знаний для решения задач. К тому же он сокращает зависимость от высококомпетентного IT-персонала (разработчики, архитекторы), и во многом поэтому последние относятся к такому методу с опасением и предубеждением, боясь потерять работу. Однако практика показывает, что так не происходит и «потребность в людях, которые не только знают, как программировать, но и понимают контекст, разбираются в предметной области, сохранится», говорит господин Лихачев.

Кому это нужно

Современные корпоративные программные продукты, которые не предоставляют возможности конфигурирования без привлечения разработчика, становятся неконкурентоспособными, констатирует Александр Наймарк. Low-Code может быть использован в торговле, производстве, строительстве, государственном и муниципальном управлении, перечисляет Сергей Бобрецов: «Примеры — настройка торговых операций, когда из-за ремонта склада, при изменении логистики или добавлении маркетинговых акций требуется модифицировать цепочки прохождения процесса продажи, добавив специфический процесс или временно изменив маршрут прохождения. Подобные задачи легко решаются на платформе ТУРБО X». Гибкая настройка с применением Low-Code, по его словам, может требоваться и для организации производства инновационных изделий, которое не укладывается в общую цепочку процессов.

Здесь те же правила, что и для «обычных» информационных систем, рассуждает Иван Лихачев. По его мнению, Low-Code будет наиболее востребован там, где автоматизация и цифровизация является жизненно важным элементом для развития бизнеса: банки и страховые компании, розничный бизнес, включая онлайн и маркетплейсы, телеком и связь, транспорт, органы государственной власти, крупные производственные холдинги.

Low-Code платформы могут решить не только задачи CRM- и BPM-систем, но и большинство функциональных задач корпоративного уровня, в том числе создание систем класса ERP, утверждают эксперты. При этом такой подход проникает в самые нагруженные бизнес-процессы, говорит господин Бобрецов: торговые операции, логистику и производство с его большим разнообразием функций и огромными потоками информации.

Взгляд в будущее

Участники рынка полагают, что у Low-Code отличные перспективы, проводя аналогию с облачными решениями: вначале всех это пугало, менеджеры по IT были осторожны, и никто представить себе не мог, как можно отдать кому-то управление инфраструктурой и даже приложением, но постепенно все оценили преимущества и перестроились. Сейчас рынок облачных технологий в РФ оценивается в сотни миллиардов рублей: в мае Statista прогнозировала, что в 2024 году его объем достигнет почти 213 млрд руб.

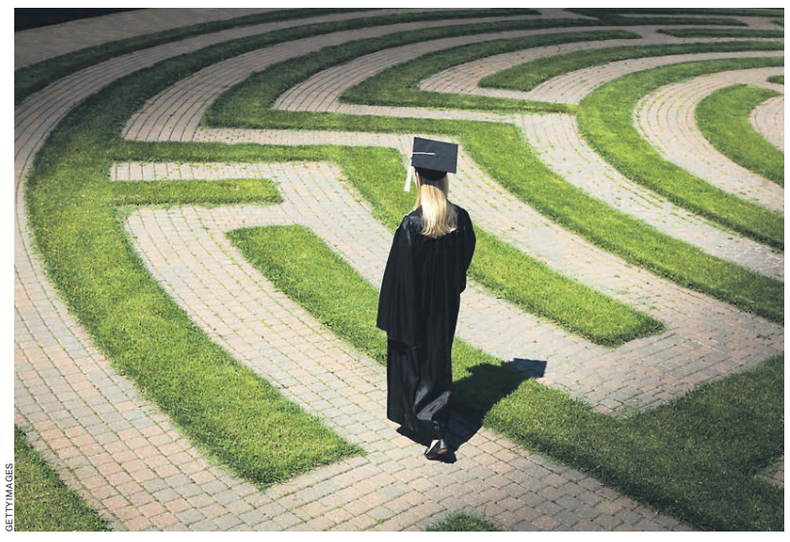
«Потребуется определенное время для смены привычек и адаптации. Рынок будет развиваться, появится больше провайдеров подобных решений, а также специалистов. Low-Code вполне способен изменить правила игры для многих организаций»,— резюмирует Иван Лихачев.

Виктор Шалимов

Ученья идут

— EdTech —

Стремительно выросший на фоне пандемии коронавируса российский рынок онлайн-образования в 2022 году столкнулся с резким спадом: инвестиции в сегмент с начала года снизились в четыре раза, а динамика доходов замедлилась на фоне падения спроса. Причинами тому стали снижение реальных доходов населения на фоне очередного кризиса, а также отток в корпоративном сегменте, которому пришлось сократить расходы. Но участники рынка рассчитывают на восстановление динамики уже в следующем году за счет сотрудничества с вузами, а также господдержки в части реализации программы «Цифровые профессии».



GETTY IMAGES

В текущем году на фоне специальной военной операции и последовавших за ней санкций инвестиции в российские компании, работающие в секторе онлайн-образования, резко снизились. По оценке «Нетологии», только в сегмент дополнительного профессионального образования (ДПО) вложения в 2022 году могут составить 20% от объема 2021 года — около $30 млн. В прошлом году, по данным исследования «Нетологии» и Аналитического центра Агентства инноваций Москвы, общий объем вложений в этот рынок составил $149,2 млн.

С начала года общие инвестиции в онлайн-образование рухнули в четыре раза, оценивал Smart Ranking. Во втором квартале они составили лишь 650 млн руб., и большая часть за этот период пришлась всего на одну сделку: венчурный фонд ВЭБ.РФ вложил 520 млн руб. в платформу «Профилум». При этом последние годы рынок EdTech в России стремительно развивался: в 2019 году он вырос более чем на 30% и еще на 80% в 2021 году.

Не только сокращение инвестиций говорит о непростом положении, в котором оказался рынок. По информации «Ъ», EdTech-компании, специализирующиеся на обучении взрослых, в начале октября фиксировали падение трафика на 10–30% с начала частичной мобилизации в России. Падает интерес даже к самым востребованным ранее курсам Data Science и иностранных языков. В целом, по прогнозу экспертов, рынок в 2022 году впервые может показать падение на 10–15%.

Как участники рынка справляются с работой в новых условиях?

Эффект удаленки удален

По данным Kepios, на январь 2022 года в России насчитывалось 129,8 млн интернет-пользователей (89% от общей численности населения), это восьмое место в мире. Рунет проник в повседневную жизнь, помогая совершать финансовые операции, заказывать еду, такси или общаться в соцсетях. В том числе учиться.

В последние годы дистанционное обучение, подталкиваемое спросом как со стороны государства, так и частных компаний, быстро развивалось по всей России, а пандемия COVID-19 стала основным катализатором изменений. Потенциал российского рынка EdTech подтверждал массовый рост числа локальных игроков.

Рынок онлайн-образования в России достиг $1 млрд в 2021 году (рост на 30–35% в 2020 году и почти удвоение в 2021 году), отмечали аналитики Frost & Sullivan в отчете по итогам 2021 года: «Этому способствовал усиливающийся спрос на повышение квалификации и переквалификацию, в том числе на фоне пандемии, появление крупных игроков („Нетология“, Skillbox, „Яндекс.Практикум“). Российские университеты также не отстают, интегрируя онлайн-составляющую в учебный процесс».

«В периоды стресса и неопределенности людям сложно думать о каком-то обучении, заставить себя учиться во время тревоги, но, с другой стороны, большая часть населения сначала в период пандемии, а потом после февральских событий поняла, что изменения в карьере и жизни необходимы»,— полагает гендиректор «Нетологии» Марианна Снигирева.

Текущий «кризис» затронул не все сегменты EdTech, указывает гендиректор Maximum Education Михаил Мягков: «Например, в сегменте школьного и дополнительного школьного образования детей сильного замедления роста, если смотреть год к году, мы не заметили». Топ-10 игроков сегмента, по его словам, продолжают расти, но перестраивать работу и фокус пришлось: «В нашем сегменте мы также фиксируем интерес семей к IT-профессиям, программированию и информатике».

Новые перспективы

Учитывая размер традиционного рынка высшего образования, в EdTech все чаще обращают внимание на него, допуская, что именно это направление способствует восстановлению после кризиса. Например, Skillbox сотрудничает с МГУ, НИТУ МИСиС, РАНХиГС и МПГУ. «Нетология» также является партнером РАНХиГС и НИТУ МИСиС плюс МФТИ. Skyeng со своим проектом Skypro (онлайн-образование для взрослых) стала пионером на российском рынке модели ISA (соглашение о разделе доходов), предлагая студентам бесплатное обучение в обмен на долю их будущей зарплаты. «Если в прошлом году мы сами пробивались к вузам и пытались их заинтересовать, то сейчас они сами приходят к нам»,— отмечала ранее в интервью „Ъ“ Марианна Снигирева. Кроме того, по ее словам, растет как количество госпроектов, так и суммы финансирования, потому что государство еще в прошлом году говорило, что России не хватает 1 млн IT-специалистов: «А сейчас из-за того, что те, кто был в России, вообще уехали, сохраняется серьезный дефицит».

Фактором роста, полагают эксперты Frost & Sullivan, окажется и господдержка, в частности реализация нацпроекта «Цифровые профессии», запущенного в 2019 году по инициативе Минцифры и Университета 2035. Главная цель — восполнить дефицит IT-кадров. В 2021 году, по данным Минцифры, в IT-отрасли не хватало от 500 тыс. до 1 млн сотрудников. «Рынок начал меняться вследствие масштабирования госпрограмм — онлайн-обучение стало доступнее. Например, мы присоединились к проекту „Цифровые профессии“, в этом году расширившему число льготных категорий граждан, которые смогут получить дополнительное профессиональное образование в сфере IT»,— говорит сооснователь и программный директор Skillbox Сергей Попков.

Перенастройка каналов

Весной EdTech сильно пострадал из-за невозможности размещать рекламу в Google, YouTube, Facebook и Instagram — именно они приносили самый большой процент трафика компаниям. В этой связи в «Нетологии», говорит госпожа Снигирева, перевели фокус на работу с органическим трафиком для балансирования основных метрик на разных уровнях воронки.

«С марта мы протестировали почти все новые инструменты»,— говорит об источниках трафика директор по маркетингу Moscow Digital School Милла Ли, добавляя, что раньше компания могла себе позволить намного легче отказываться от размещения на площадке. «Были понятные качественные источники, дававшие больший результат при меньших вложениях. Теперь все варианты рассматриваются. Равноценной замены ушедшим рекламным площадкам так и не появилось»,— заключает она.

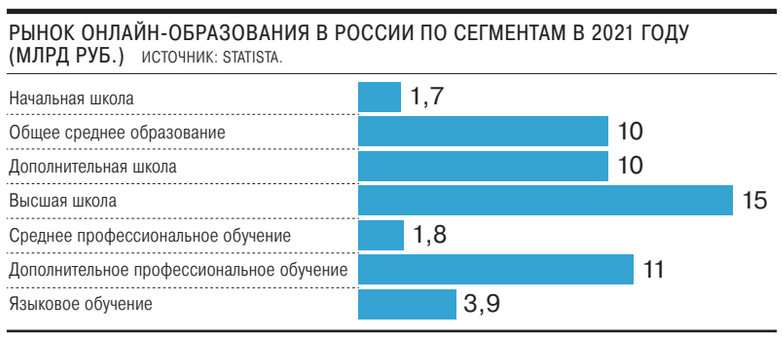
Единственный новый инструмент, который появился за этот период,— таргетированная реклама в Telegram, говорит Сергей Попков, отмечая также масштабирование рекламных кампаний во «ВКонтакте». Перспективным, по его мнению, выглядит направление геомаркетинга (с его помощью можно рассказать о своем продукте или услуге локальной аудитории тем, кто находится поблизости) и смешанных форматов (когда компания предлагает тестировать онлайн-продукт в офлайне).

«Мы перестроили работу глобально: вышли на новый рынок,— рассказал Head of RnD в „Профилум“ Виталий Алтухов.— До весны мы развивали B2C-продукт для подростков и их родителей: профдиагностика и обучение карьерной грамотности с сопровождением тьюторов. Это была достаточно новая для аудитории услуга, поэтому нужно было создавать в ней потребность». В начале года стало ясно, что продукт, спрос на который еще полностью не сформировался, продавать сложно — в ситуации ограниченных возможностей продвижения в соцсетях и одновременно возросшей потребности людей в экономии средств, объясняет он.

Основным вызовом для компаний действительно стала быстрая перестройка процессов, включая смену основных рекламных каналов и потребительской модели поведения, рассуждает управляющий директор образовательного холдинга Ultimate Education Никита Подлипский. В целом отечественный EdTech достаточно оперативно адаптировался к новым условиям и перестроил свои продуктовые и маркетинговые стратегии, отмечает он: «У всего рынка произошло ускоренное взросление. Снизилась доля спонтанных покупок — пользователи при выборе образовательных продуктов стараются принять взвешенное решение». Он считает это позитивным трендом, так как высокая осознанность покупки обеспечивает и высокую вовлеченность в процессе обучения: «Кроме того, это влечет за собой перераспределение спроса от инфобизнеса в сторону профессионального EdTech».

Юлия Тишина

РЫНОК ОНЛАЙН-ОБРАЗОВАНИЯ В РОССИИ ПО СЕГМЕНТАМ В 2021 ГОДУ (МЛРД РУБ.) ИСТОЧНИК: STATISTA.



информационные технологии

BSS

Родная технологическая речь

Искусственный интеллект (ИИ) остается одним из самых заметных и востребованных технологических трендов. По данным НИУ ВШЭ, в 2021 году почти каждое третье крупное предприятие в России использует ИИ. Все более существенную роль начинают играть речевые технологии: голосовые ассистенты, чат-боты, речевая аналитика и другие инструменты. Их внедрило около 70% организаций, использующих ИИ. Значительная часть внедрений приходится именно на госсектор. Так, в 2021 году рынок речевого ИИ в России с учетом госзаказчиков увеличился на 81%, до $120 млн, и он будет продолжать расти. Какие проекты реализуются в госсекторе и кто является одним из крупнейших поставщиков решений в этой сфере?



АНАТОЛИЙ ЖДАНОВ

— речевой AI —

Плюс цифровая трансформация всей страны

С лета 2020 года все ключевые отрасли экономики, социальной сферы, министерства и ведомства взяли курс на цифровую трансформацию как национальную цель развития России во исполнение поручения президента Владимира Путина. В прошлом году премьер Михаил Мишустин утвердил план мероприятий по цифровой трансформации в сфере госуправления на ближайшие десять лет. Согласно ему, доля массовых социально значимых услуг, доступных в электронном виде, должна составить 95%. Глава Минцифры Максут Шадаев подчеркивает, что госуслуги должны предоставляться так же быстро, как покупка билетов или бронирование гостиниц.

ИИ, большие данные и интернет вещей — основные технологии для внедрения в госсекторе. Заместитель председателя правительства РФ Дмитрий Чернышенко, ответственный за создание «дорожной карты» сотрудничества в сфере искусственного интеллекта, анонсировал запуск Национального центра развития ИИ при правительстве РФ. В последней версии федерального проекта «Цифрового государственного управления» затраты бюджета на его реализацию до 2024 года составят до 411 млрд руб. В апреле правительство утроило финансовую поддержку разработчиков ИИ-систем. Ожидается, что к 2024 году около 1,2 тыс. таких компаний получат в общей сложности более 17 млрд руб., включая внебюджетные средства индустриальных заказчиков.

Госсектор ищет альтернативный голос

Развитие ИИ в госсекторе уже активно идет. Взрывной рост эксперты связывают в том числе с пандемией. Многие перешли на удаленную работу, и офлайн-взаимодействие сократилось. Госсектору пришлось оперативно перестраиваться и быстро адаптироваться к растущему числу запросов в онлайне. Кроме того, внедрению способствует зрелость речевых технологий.

При реализации единого контактного центра (ИС ЕКЦ) в Пенсионном фонде России были успешно внедрены голосовой и текстовый бот, инструменты речевой аналитики. Все это обеспечивает доступность, оперативность и качество обслуживания запросов клиентов. ИС ЕКЦ является единой информационной системой ряда ведомств: Фонда социального страхования, медико-социальной экспертизы, Роструда, Минтруда, а в дальнейшем и органов соцзащиты субъектов страны. Систему более чем со 100 сценариями самообслуживания опробовали в десяти пилотных регионах. Бот одновременно обслуживает свыше 800 сессий: голосовых и текстовых запросов клиентов. На момент запуска автоматизировано 15% обращений граждан, и показатель растет.

Речевая аналитика контролирует обращения граждан по различным вопросам социального характера, анализирует качество работы операторов ЕКЦ. «Сервис речевой аналитики дает информацию, ценную как для работы контакт-центра, так и для всей организации в целом. Он позволяет проводить оперативный анализ работы ЕКЦ, контролировать качество обслуживания»,— отмечали ранее в Минтруде. Получаемые данные позволяют отслеживать тренды в обращениях граждан, оперативно реагировать на изменения их запросов, повышать качество обслуживания. В проекте ПФР использовались речевые технологии BSS. «Это очень ответственный и амбициозный проект для нас,— говорит гендиректор BSS Георгий Кравченко.— Его масштаб и успешность позволяет говорить о том, что речевые решения BSS готовы работать в очень разных условиях, способны реализовать сложные сценарии заказчиков, обладают высокой гибкостью, эффективны и надежны». В планах на ближайший год увеличить до 30% количество обращений, которое будет полностью обслуживаться роботом.

К слову, BSS выступает одним из крупнейших участников рынка речевых технологий в госсекторе на уровне федеральных и региональных госорганов. Решения компании представлены во всех федеральных округах более чем в 30 субъектах РФ (Тульская область, Санкт-Петербург, Камчатский край, Амурская, Воронежская, Курская области и др.), развернуты в региональных правительствах и обслуживают жителей, в том числе по основным социально значимым направлениям: медицина, услуги МФЦ, ЖКХ, соцзащита и занятность и т. д.

Одни из последних региональных проектов на базе решения BSS реализованы в партнерстве с «БФТ-Холдингом», российским разработчиком программного обеспечения и заказной разработки для госсектора.

Так, в МФЦ Санкт-Петербурга на базе решений BSS внедрен виртуальный ассистент. Робот обслуживает около 60% обращений граждан самостоятельно, оператор подключается только в случае, если требуется учесть индивидуальные особенности ситуации конкретного заявителя. Робот-консультант первым отвечает на звонки граждан в контакт-центр МФЦ независимо от времени суток, сокращая время ожидания на линии. Голосовой помощник информирует граждан о ходе предоставления услуги, дает необходимую справочную информацию. В целом консультирует по 60 тематикам.

Аналогичный проект на базе речевых технологий BSS реализован и в Тульской области. С момента запуска робота «Николая» в три раза увеличилось количество обрабатываемых обращений в месяц. На 79% поступающих вопросов «Николай» отвечает самостоятельно, без переадресации на специалистов. Робот позволяет экономить ежегодно до 4 млн руб. регионального бюджета.

Жителям Камчатки виртуальный ассистент «Полина», работающий на базе технологий BSS, помогает записаться на прием к врачу. Проект стартовал по поручению краевого правительства. Интеграция с краевой медицинской информационной системой позволяет «Полине» идентифицировать абонента по фамилии и дате рождения, определить прикрепление к поликлинике и предложить наиболее удобное время записи. В результате более 15% абонентов записываются в поликлинику с помощью виртуального консультанта.

В период пандемии BSS установила рекорд быстрого развертывания: от первого совещания до полномасштабной работы — 46 часов, внедрив голосового робота в государственном контакт-центре в регионе России более чем с 4 млн жителей. Во время эпидемии COVID-19 региональные службы захлестнул поток звонков: свыше 80% вызовов находилось в очереди в течение длительного времени или оставалось без обслуживания. Внедренный голосовой бот выдавал пропуска для местных передвижений — требование, введенное правительством. Он обрабатывал до 300 вызовов одновременно и автоматически выдавал около 10 тыс. пропусков в день.

Новые перспективы

В конце 2021 года BSS выиграла грант Российского фонда развития информационных технологий на развитие омниканальной диалоговой платформы Digital2Speech, которая включена в единый реестр российского ПО. Компания предлагает полный технологический стек собственной разработки. Все компоненты бесшовно интегрированы друг с другом и могут внедряться как все вместе, так и по отдельности. Установленные компоненты легко дополняются новыми, которые используют уже адаптированные в процессе работы первых модулей алгоритмы. По словам Георгия Кравченко, платформа BSS покрывает все потребности заказчика в области речевых технологий с использованием ИИ и машинного обучения.

Роботы-консультанты позволяют выйти на новый качественный уровень коммуникации и взаимодействия граждан и коммерческих организаций с органами госвласти в цифровом формате, объясняет господин Кравченко: «Системы, внедренные на региональном и федеральном уровне, уже демонстрируют значительный потенциал с точки зрения функциональных возможностей и широкого применения в МФЦ».

По его мнению, основная специфика внедрения речевых технологий в госсекторе — динамично развивающееся законодательство, потребности общества и вызовы времени, диктующие повышенные требования к автоматическим системам для обслуживания граждан: «К примеру, пандемия и другие внештатные ситуации порождают высокую потребность граждан в онлайн-общении и решении вопросов в максимально короткие сроки».

Задача государства — обеспечение развития социальной среды, повышения удовлетворенности граждан госсервисами, развитие и внедрение новых услуг, рассуждает Георгий Кравченко: «Интерес в применении речевых технологий на базе ИИ для дистанционного обслуживания граждан появляется на всех вертикалях госвласти и является важной составляющей цифровой зрелости региона».

Диалоговые системы с искусственным интеллектом постепенно вытесняют стандартные схемы организации работы в контакт-центрах, показывают высокую эффективность, становятся новым трендом цифровизации сферы госуслуг, отмечает первый заместитель генерального директора «БФТ-Холдинга» Наталья Зейтениди: «Когда есть задача заменить человека, но сохранить человечность, помогают диалоговые роботы. Они значительно снижают нагрузку ведомств и при этом сохраняют доверие граждан к ним. Роботы действительно могут слушать и слышать — благодаря машинному обучению понимают живую речь человека по телефону и поддерживают диалог на естественном языке. Технологии голосовых роботов сегодня востребованы и активно используются в регионах».

Евгений Зимин

Русская душа на чужбине

— шифрование —

Использование VPN-сервисов, обеспечивающих защищенное соединение между пользователем и сервером, с конца февраля увеличилось в стране в пять-десять раз. После этого Россия поднялась с 15-го на 2-е место в мире по загрузке таких приложений. Эксперты утверждают, что в основном россияне используют VPN для заблокированных на территории РФ социальных сетей. Однако вместе с этим вырос и спрос на VPN обратного применения — из-за рубежа в РФ, прежде всего из-за того, что многие соотечествен ники в 2022 году покинули страну. Как «виртуальные частные сети» стали одними из самых востребованных ресурсов в России?



ИГОРЬ ИВАНКО

После начала военной операции на Украине ряд иностранных онлайн-сервисов был заблокирован Роскомнадзором (РКН), кроме того, и сами компании решили ограничить доступ для россиян. Так, в начале марта РКН объявил о блокировке соцсетей корпорации Meta и признании ее экстремистской (речь о Facebook и Instagram), а также Twitter, сославшись на нарушения прав и свобод граждан России. Закрыли доступ к своим сервисам по собственным причинам и из-за блокировки оплаты через Visa и Mastercard Netflix, Spotify и множество других сервисов.

Это повлекло за собой массовое использование в РФ VPN-сервисов, чьи серверы могут находиться где угодно: в Индии, США, Швеции или Германии. Как только происходит подключение, сервер заменяет IP-адрес пользователя на свой. По данным AppMagic, в марте—июле Россия занимала второе место в мире по количеству загрузок VPN-сервисов, уступая только Индии, сообщал РБК. Только за первые три недели июля VPN-сервисы в России скачали более 12 млн раз. Для сравнения: в январе 2022 года их загрузили 2 млн раз, и страна занимала 16-е место в мире по этому показателю, в июле 2021-го — 2,7 млн и 15-е место соответственно.

Около 25% граждан РФ используют VPN, оценивают в TelecomDaily, из них более 90% используют бесплатные сервисы, платные в основном применяют юрлица. По словам гендиректора TelecomDaily Дениса Кускова, в платных VPN утечек и вирусов практически нет, а скорость работы на порядок выше бесплатных сервисов, не говоря уже о количестве рекламы. По его данным, средняя стоимость платного VPN-сервиса составляет от €5 до €20 (280–1000 руб.) в месяц.

«Параллельный» Instagram

Пользователи не стали отказываться от привычных площадок, тем более что для многих соцсети были не просто местом досуга, а частью бизнеса или работы. Скачивание доступных VPN-сервисов выросло в пять-десять раз, оценивает заместитель гендиректора по технологическому развитию группы «Иннотех» Антон Якимов.

Кроме приложений пользователи начали использовать специализированные веб-браузеры, в которые уже интегрированы VPN-сервисы, поэтому полностью перекрыть каналы доступа к заблокированным ресурсам и приложениям у РКН сейчас просто нет возможности. «VPN призваны скрыть трафик и/или исходный IP-адрес, и пользователи, применяющие эти сервисы, выпадают из поля, регулируемого государством. Но — именно нашим государством. Например, известная пиратская библиотека „Флибуста“ заблокирована в России, но легально доступна на территории Турции»,— приводит пример заместитель гендиректора по науке и развитию ИВК Валерий Андреев.

VPN — враг номер один

После массового перехода россиян на VPN РКН решил блокировать и их, официально подтвердив свои действия по ограничению работы таких сервисов в стране. «Средства обхода блокировок противоправного контента признаются угрозой. Центр мониторинга и управления сетью связи общего пользования принимает меры по ограничению работы на территории России VPN-сервисов, нарушающих российское законодательство»,— заявили в июне в РКН после сообщений о проблемах с подключением в России к популярному VPN-сервису Proton.

С юридической точки зрения правительство имеет право на блокировку VPN-сервисов по закону «Об информации», рассуждает руководитель Tech & Product консалтинговой компании Comply Сергей Сайганов. Чтобы эти сервисы не были заблокированными, продолжает он, разработчикам необходимо поддерживать бан-лист заблокированных сайтов РКН: «Для этого нужно подключиться к автоматизированной системе рассылки РКН и пройти соответствующую регистрацию. По понятным причинам иностранные сервисы эти шаги часто не выполняют».

Родная, течь!

Согласно августовскому опросу, проведенному экспертами «АльфаСтрахования», почти половина населения России (48%) в 2022 году столкнулась со взломом личных страниц в соцсетях. Это не единственная впечатляющая цифра: подавляющее большинство участников опроса (76,4%), которые стали объектами внимания злоумышленников, заявили, что используют VPN для входа в заблокированные в РФ сети.

По словам господина Якимова, с точки зрения общей безопасности использования VPN велика вероятность утечки данных из трафика, который проходит через сервис: почтовые адреса, телефоны, персональные данные и пароли. Впрочем, вице-президент «Лаборатории Касперского» Вячеслав Закоржевский указывает, что технология VPN, наоборот, призвана повышать кибербезопасность пользователей — именно поэтому ее часто применяют, например, при подключении к удаленному компьютеру в корпоративном сегменте. «Она позволяет установить зашифрованное соединение между устройством и VPN-сервером, который отправляет запросы конечному ресурсу в интернете. Таким образом, можно в зашифрованном виде передавать конфиденциальные данные, скрыть IP-адрес и местоположение»,— поясняет он.

Однако, по словам господина Закоржевского, частным пользователям необходимо ответственно подходить к выбору VPN-решения, так как полностью бесплатные сервисы зачастую собирают данные о пользователях для последующей монетизации. «Например, в конце 2021 года исследователи обнаружили данные 45 млн пользователей предположительно компании ActMobile Networks, владеющей рядом VPN-сервисов,— говорит топ-менеджер.— К сожалению, время от времени даже крупные международные сервисы подвергаются атакам с утечкой данных пользователей».

Любое VPN-подключение использует определенный протокол, и, например, далеко не самый безопасный протокол PPTP по-прежнему достаточно распространен, обращает внимание эксперт «Доктор Веб» Александр Горячев. «Наличие уязвимостей, которые могут быть использованы злоумышленниками, сводит на нет всю безопасность и приватность VPN-подключения»,— говорит он, добавляя, что узнать, какие именно протоколы использует тот или иной VPN-сервис, невозможно.

Главной опасностью любого VPN-сервиса, продолжает господин Горячев, остается возможная утечка персональных данных. Помимо этого пользователи при скачивании VPN-приложений могут столкнуться с программами-подделками, которые лишь имитируют работу VPN, а на самом деле либо не шифруют трафик, либо могут передавать его злоумышленникам, «работая как троянские приложения-шпионы».

«VPN наоборот»

Наблюдатели указывают и на противоположную тенденцию — запрос на «VPN-наоборот», то есть на сервисы с российскими точками выхода для доступа к госсервисам из-за рубежа. На начало сентября из России с начала года выехали 419 тыс. человек по сравнению с 202 тыс. за аналогичный период прошлого года, писал РБК, ссылаясь на данные Росстата. При этом за две недели после объявления о частичной мобилизации страну, согласно данным Forbes, покинуло еще примерно 700 тыс. человек. Власти, впрочем, называют сообщения о 700 тыс. покинувших страну с начала частичной мобилизации «уткой»: по словам пресс-секретаря президента РФ Дмитрия Пескова, реальные цифры далеки от этого.

«Главным образом востребованы госуслуги, налоговая служба, сайты судов и другие ресурсы органов власти. Многие из них недоступны из-за рубежа без VPN»,— отмечает технический директор iD EAST Денис Хоружий. «Обратным VPN» пользуются также для потребления развлекательного и мультимедийного контента отечественных интернет-кинотеатров, музыки и онлайн-ТВ. Доступ к ним по лицензионным соображениям также зачастую ограничен российскими IP-адресами, и VPN-сервис в этом случае также позволит использовать имеющиеся подписки, находясь за пределами РФ.

По словам Валерия Андреева, российские VPN-сервисы официально не существуют. «Это удивительно, ведь наша страна является одной из самых продвинутых в теории и практике сферы криптографии. Российские криптоалгоритмы одни из самых стойких в мире, эта сфера тщательно контролируется различными регуляторами»,— говорит эксперт. Он указывает, что существуют отечественные стандарты сетевого шифрования — «Кузнечик», «Магма», Streebog: «Страна, имеющая такой мощный интеллектуальный задел в сфере криптографии, вполне могла бы составить достойную конкуренцию на этом поле»,— считает эксперт.

Сегодня VPN становится массовым продуктом, так как раньше этим инструментом пользовались несколько десятков тысяч профессионалов, констатирует Валерий Андреев. Кроме того, законодательно VPN-подключение не является нарушением и дальнейшее ужесточение регулирования может привести к потере выручки у средних и малых бизнесов, которые активно продвигали свой продукт на заблокированных площадках: «Пока существуют возможности обойти запреты, люди будут изыскивать эти возможности. Единственный радикальный способ — отрезать кабель».

Тимофей Корнев

информационные технологии

Ренессанс КРЕДИТ
КБ «Ренессанс Кредит» (ООО)

«Ни один серьезный банк не остановил программ развития»

Банковская сфера современной России всегда развивалась в условиях высокой турбулентности, адаптируясь к новым вызовам, условиям, технологическим требованиям. Возможно, благодаря этому банки в достаточной степени готовы к любым изменениям. Финансовый сектор достаточно устойчив как с точки зрения обеспечения стабильного функционирования, так и дальнейшего развития, уверен старший вице-президент по IT и цифровой трансформации бизнеса банка «Ренессанс Кредит» **Денис Сотин**. В интервью он рассказал об актуальных задачах для банковского IT, цифровизации, сложностях импортозамещения, перспективах развития финансовых сервисов и кадровых ресурсах.



ПРЕДОСТАВЛЕНО ПРЕСС-СЛУЖБОЙ БАНКА «РЕНЕССАНС КРЕДИТ»

— первые лица —

— Банковскую отрасль в последние годы называли одним из флагманов цифровизации в России. Изменилось ли что-то в этой области с февраля?

— Сказать, что сейчас ситуация кардинально изменилась, нельзя. Безусловно, происходящее в стране повлияло на нас: образовались дополнительные векторы движения. Но ни один серьезный банк не остановил программ развития. В том числе «Ренессанс Кредит»: мы продолжаем инвестировать в развитие бизнеса. Идет адаптация и продолжается цифровизация бизнеса за счет реализации новых моделей взаимодействия с клиентами, анализа потребительского поведения, предложения более комплексных услуг.

— Появились ли какие-то новые приоритетные направления?

— Возникли дополнительные направления развития. Они становятся более важными, чем раньше. Например, тема импортозамещения стала более актуальной из-за событий этого года, санкций, ухода ряда компаний. Речь и об инфраструктуре, и об операционных системах, и о базах данных, и о прикладном ПО. Здесь по-прежнему стоит большое количество задач, хотя много шагов предпринималось еще в период с 2014 года. Сейчас мы, как и весь банковский сектор, вынуждены интенсифицировать меры по переходу на аналоги, в том числе российские.

— Насколько задача импортозамещения для банков сложна?

— С прикладными банковскими системами ситуация одновременно и сложнее, и проще, чем с другими элементами IT-периметра. Проще — потому что в значительной степени банковские системы были построены вокруг российского банковского учета. Поэтому иностранного ПО в сердце банковской системы не очень много — как правило, это системы российской разработки, и с ними проблем не возникает. Хотя стоит задача перевода ряда систем на другие базы данных. Однако есть достаточно много различных западных технологий, которые активно использовали банки для построения более гибких моделей взаимодействия с клиентами, анализа их поведения, быстрого выстраивания процессов. Эти решения сейчас пересматриваются. Степень критичности у всех систем разная, но абсолютно точно в какой-то обозримой перспективе встанет вопрос перехода на аналоги — опенсорс или российские решения.

Второй дополнительный вектор немаловажный — это, на мой взгляд, утроившееся внимание к вопросам ИБ и защиты периметра, наиболее критичных элементов банковской инфраструктуры.

— В каких областях с поиском аналогов могут возникнуть затруднения?

— В большинстве случаев прикладной софт в банках — от главной бухгалтерской книги и продуктовых движков до процессных движков и фронтальных решений — это, по сути, либо «коробочные/околокоробочные» решения российской разработки, либо самостоятельные разработки банков, в том числе с использованием иностранных платформ и технологий. Подавляющее большинство этого контура может быть переведено на аналоги. Правда, в ряде случаев нужно будет переписывать функционал при переходе с определенных решений западных вендоров на аналогичные опенсорс-решения или локальные платформы Low-Code/No-Code. Это, кстати, одна из причин роста популярности таких решений в последнее время.

Но больше всего неудобств, как ни странно, связано с решениями для внутреннего пользователя в банке. Например, в части коммуникационных сервисов пока, к сожалению, аналоги средств корпоративной связи и видеоконференций функционально не на том уровне, к которому мы привыкли. Будем откровенны: когда есть коммуникационный инструмент, используемый в 80% компаний как стандарт, это удобно. Заменить его непросто. Сейчас мы уже практически определились с альтернативой, но в любом случае российские аналоги еще находятся в стадии активного развития. Думаю, в ближайшие год-полтора они смогут достичь нового уровня.

— Какие приоритеты на ближайшее время стоят перед банком в части развития цифровых сервисов?

— Мы как раз определяемся со стратегией развития 2022–2026. Фундамент ее заложен в 2021 году, и ситуация начала года, конечно, привнесла элемент неожиданности. Но наши планы остаются в силе: мы диверсифицируем бизнес и намерены активно развиваться. Раньше «Ренессанс Кредит» был больше известен на рынке розничного кредитования, в первую очередь POS-кредитования в торговых сетях. Сейчас мы в том числе активные участники рынка бесцелевого кредитования, кредитных и дебетовых карт, брокерских услуг. В следующем году запускаем и будем активно развивать направление МСБ. Таким образом, банк становится все более универсальным и в дальнейшем продолжит наращивать количество и качество предоставляемых нашим клиентам продуктов и сервисов.

Сейчас мы определяем объем инвестиций в развитие на следующий год, он точно будет не меньше, чем в этом. Безусловно, эта история строится вокруг цифровых сервисов, новых моделей взаимодействия с клиентами, повышения качества и уровня представляемых продуктов и сервисов через дистанционные каналы. И в то же время мы уделяем повышенное внимание вопросам ИБ и стабильности нашего периметра и прагматично реализуем планы по импортозамещению.

— В последние годы банки были одними из самых активных игроков на рынке труда IT-специалистов. Что сейчас с этим рынком?

— Мы подходим к вопросу кадрового обеспечения не только с точки зрения наличия готовых кадров на рынке, но и подготовки новых на базе банка. Например, мы делали ряд школ по интересующим нас направлениям в нашем региональном центре в Пензе: готовили Java-разработчиков и тестировщиков. И планы развития этого направления у нас тоже есть. Это необходимо для того, чтобы люди, только входящие в профессию, сразу начинали свой карьерный путь с банком.

Конечно, ситуация последних лет на рынке была несколько разбалансированной под влиянием ряда крупных участников рынка, которые активно привлекали IT-специалистов различных профилей в свои создаваемые продуктовые трайбы, зачастую целыми командами. Это создавало давление на рынок и привело в отдельных областях к дефициту кадров, к активному росту зарплат IT-специалистов. Один из трендов, который четко проявился в прошлом году,— уравнивание зарплат по регионам и в Москве. То есть для IT-специалистов перестала существовать разница, где работать: можно работать на московскую зарплату абсолютно из любого региона, а сейчас еще и не только из России.

В то же время сегодня я не вижу предпосылок для серьезного дефицита кадров. Могу сказать, что ряд крупнейших организаций пересматривает свой подход к найму. В предыдущие годы крупные компании закупали IT-ресурсы «на перспективу». Сейчас все больше проектов и задач рассматривается с точки зрения реальной эффективности. И это в том числе отчасти снижает запрос на привлечение большого количества IT-специалистов, делая его более прагматичным.

С другой стороны, мы понимаем, что возрастает спрос на специалистов, которые будут или уже заняты в программах импортозамещения. Это касается и банков, и других организаций.

Все эти разнонаправленные факторы, на мой взгляд, приведут нас к становлению более сбалансированного рынка, хотя пока на нем еще чувствуется неопределенность. Идет перемещение между задачами, проектами, командами и компаниями. Многие банковские, и не только банковские, организации взяли курс на внутреннюю разработку, на увеличение IT-штата за счет сокращения привлечения внешних команд. Мы в «Ренессанс Кредит» в том числе нацелены на развитие внутренних центров экспертизы. Это тоже приводит к перераспределению ресурсов на рынке. Поэтому пока ситуация несбалансированная, но нельзя сказать, что она критическая.

— Какие IT-специальности востребованы банками, и в частности банком «Ренессанс Кредит», внутри?

— Востребованы почти все IT-специальности, просто в разной мере. В предыдущие два года у нас активно шло формирование и усиление центра экспертизы по нашим бэкофисным системам. Но это не та зона развития, в которой нам нужно большое количество людей. Мы активно набираем людей на фронтальную разработку, Java-разработчиков, разработчиков, которые будут заниматься развитием микросервисов, интеграционным слоем, дата-инженеров и дата-сайентистов. Это профили, которые действительно очень востребованы, поскольку эти зоны роста с технологической точки зрения способствуют развитию банка. Java-разработчики, разработчики мобильных приложений, интеграционные слои, процессные движки, Low-Code платформы — это то, что позволяет достаточно быстро строить новые бизнес-модели, быстро их адаптировать и двигаться дальше.

Здесь важна внутренняя экспертиза. Мы верим в то, что внутренняя разработка должна превалировать, а внешние ресурсы могут привлекаться время от времени как вспомогательный ресурс.

— В какие цифровые направления банки точно не прекратят вкладывать деньги в ближайшие годы?

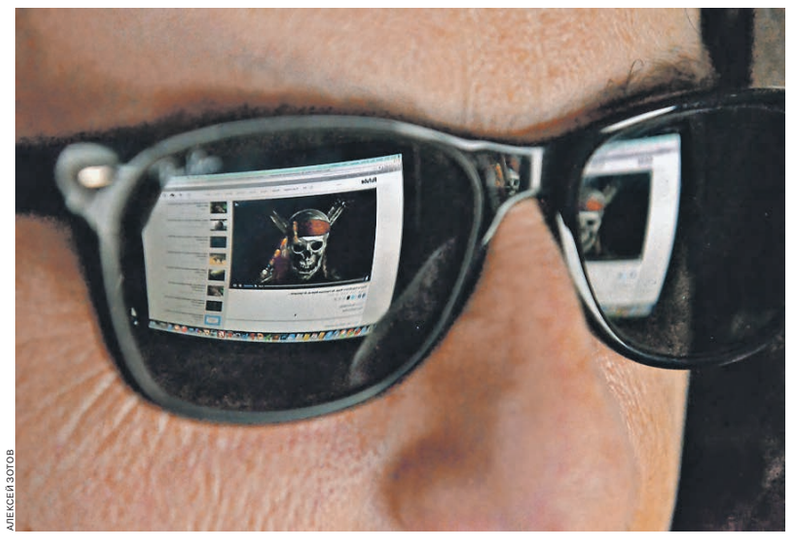
— Как и ранее, это работа с данными в том или ином виде. Цифровизация банковских сервисов, дальнейшее развитие дистанционных каналов привлечения и обслуживания — всего, что связано с возможностью неявки клиента в офис, удаленного обслуживания. Вопросы, связанные с эффективностью бизнеса и дальнейшей цифровизацией основных процессов, в том числе сокращением затрат на обслуживание тех или иных операций.

Интервью взяла
Марина Эфендиева

Пират от души

— пиратство —

В России снова растет интерес к нелегальному контенту на фоне приостановки работы в стране иностранных кинопрокатчиков и стриминговых платформ. Запросов на скачивание пиратских приложений все больше, а их разработчики думают о размещении в NashStore и RuStore. «Яндекс» по итогам лета удалил более 9 млн ссылок на пиратский контент, это рост на 42% год к году. Что говорят эксперты о перспективах этой серой индустрии и насколько эффективно антипиратское законодательство?



АЛЕКСЕЙ ЗОТОВ

Новые вводные

Уход из России зарубежных стриминговых платформ, заморозка мировых кинопремьер в отечественных кинотеатрах, невозможность оплаты иностранных подписок подогревают интерес к нелегальному контенту, который и до этого был довольно высоким. По данным Group-IB, число запросов в популярных поисковых системах на просмотр бесплатных фильмов и сериалов еще по итогам 2021 года увеличилось на 8,5% и составило 12,8 млрд.

Эксперты уверены: количество пиратского контента продолжит расти, поскольку интерес к продукции ушедших с рынка зарубежных игроков никуда не денется. Вдобавок продукты таких иностранных правообладателей оказались без должного представительства на территории РФ, а это создает проблемы с точки зрения их защиты. Ведь чтобы что-то защищать, надо получить полномочия от правообладателей, поясняет адвокат МКА «Клишин и партнеры» Владимир Энтин.

Однако к перспективе размещения пиратских приложений в официальных российских сторах эксперты относятся со скепсисом, хотя и не исключают ее. IT-юрист Анна Рязанова напоминает, что Россия все еще участник международных соглашений по защите авторских прав. «Без изменений действует четвертая часть Гражданского кодекса, посвященная интеллектуальной собственности. Размещение априори пиратских сервисов в сторах будет нарушать действующие правовые нормы»,— отмечает она.

«Я допускаю, что приложения с пиратским зарубежным контентом могут быть размещены в сторах, но их статус останется серым. Никакого официального разрешения от площадок ждать не стоит. Хотя бы формально они будут бороться с подобными нарушениями»,— считает Владимир Калугин, операционный директор Group-IB департамента Digital Risk Protection. «Не одним пиратством можно привлечь пользователей: есть множество бесплатных легальных приложений развлекательного характера, а также продуктов, которые работают по freemium или рекламной модели»,— напоминает гендиректор ассоциации «Интернет-видео» Алексей Бырдин. Так что даже в целях продвижения у российских маркетплейсов нет особой необходимости связываться с пиратской продукцией.

Более того, пиратские приложения находятся «на карандаше» и у российских правообладателей, поскольку часто нелегально распространяют их контент. Пираты могут создавать продукты только с иностранным контентом, но даже так они рискуют. «Зачастую их серверы, а у некоторых и администраторы находятся за рубежом, и до них могут дотянуться правообладатели,— рассказывает господин Калугин.— Прецеденты уже были — например, в конце 2019 года в Нидерландах закрыли серверы крупнейших на тот момент пиратских CDN-сервисов Moonwalk и HDGO».

Наконец, важно помнить, что пиратский контент — это контрафакт. По данным Group-IB, почти на 23% русскоязычных сайтов с аудиовизуальным пиратским контентом есть вирусы, которые могут привести к утечке персональных данных и другим неприятным последствиям. «Поэтому, например, крупные и даже средние предприятия вряд ли пойдут на установку пиратского ПО. Если „пираты“ придумают механизмы защиты пользователей от неблагоприятных последствий, ситуация может измениться»,— отмечает Виктор Миронов, управляющий директор консультационной группы ТИМ».

Параллельный импорт контента

О возможности легализации параллельного импорта эксперты пока тоже отзываются с сомнением. Механизм параллельного импорта строится на принципе исчерпания прав на товары, если они были произведены и введены в оборот самим правообладателем или с его согласия за рубежом, а потом ввезены на территорию России. В таком случае продавец может свободно продавать здесь свой товар.

Для произведений существует механизм национального исчерпания прав, когда распространение оригинала или других экземпляров допускается без согласия правообладателя и выплаты ему вознаграждения, если они были правомерно введены в гражданский оборот на территории России, объясняет Владимир Калугин. Теоретически можно расширить этот механизм и разрешить ввоз произведений, введенных в оборот за рубежом, но возникает ряд проблем.

«С физическими носителями все понятно: законно ввезти один экземпляр (например, DVD-диск) и его же продать, а купить один экземпляр и сделать с него несколько копий — уже нет,— продолжает господин Калугин.— В случае с цифровой дистрибуцией границы экземпляра размыты, поэтому, согласно Договору ВОИС по авторскому праву от 20 декабря 1996 года, принцип исчерпания авторских прав не применим к цифровым копиям произведений. Более того, доступ к ним часто предоставляется по лицензии, без отчуждения прав, а значит, такие копии не могут перепродаваться». Поэтому введение «параллельного импорта» в отношении цифровых произведений сомнительно.

В долгосрочной перспективе, если предположить, что санкции утратят свою силу, многие крупные зарубежные компании вернутся на российский рынок, и официальным российским сторам придется налаживать с ними контакт. «Вряд ли это получится сделать быстро, если будут использоваться пиратские версии их контента»,— добавляет господин Миронов.

Для пиратов закон написан

Под антипиратским законодательством сегодня подразумевается ряд норм гражданского и уголовного права, которые предусматривают ответственность за неправомерное использование охраняемого контента. Правообладатель может обратиться в судебные и правоохранительные органы, Роскомнадзор, Минцифры, к хостинг-провайдерам с требованием прекратить такое использование и возместить убытки. При нарушении исключительного права можно требовать компенсацию в размере от 10 тыс. до 5 млн руб., уточняет Анна Рязанова.

Скачивание пиратского контента незаконным не считается. Если оставить за скобками потребителей, схема пиратства состоит из таких частей: пиратский сервис (сайт, приложение), его администратор или команда, инфраструктура, средства продвижения контента (поисковые сервисы, соцсети, реклама) и монетизация.

Правообладатели и государство научились бороться против самого сервиса с помощью блокировок, обеспечивают давление на средства монетизации и взаимодействуют с поисковыми сервисами через механизмы Меморандума о сотрудничестве в сфере охраны исключительных прав и DMCA, объясняет Владимир Калугин. Но есть явные пробелы с привлечением к ответственности владельцев пиратских сервисов и информационных посредников, предоставляющих инфраструктуру под размещение пиратских проектов: «Посредник освобождается от ответственности, если он в случае обращения правообладателя своевременно принял необходимые и достаточные меры для прекращения нарушения интеллектуальных прав. Но перечень этих мер нигде не установлен, и многие компании ограничиваются пересылкой обращения администратору пиратского ресурса».

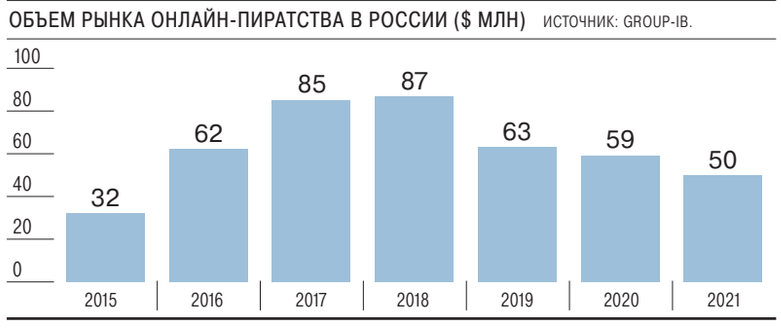
Лазейкой для пиратов остается и возможность оперативного переноса контента с одного доменного имени на другой или даже изменение поддомена сайта. «Например, был заблокирован пиратский сайт pirat1.ru, а завтра он вновь доступен для пользователей с доменом pirat2.ru. Да, есть институт внесудебной блокировки „зеркал“, но для этого правообладателю нужно вновь прикладывать усилия»,— отмечает Анна Рязанова.

«Для эффективного применения правовые инструменты требуют наличия конкретного ответчика и должны быть направлены на конкретный эпизод пиратства. А текущие способы распространения нелегального контента позволяют пиратам легко скрывать конечных бенефициаров таких сервисов и с относительной легкостью открывать новые сайты и сервисы, если предыдущие были заблокированы. Поэтому борьба с таким контентом — процесс постоянный и требующий ресурсов»,— соглашается Глеб Ситников, партнер адвокатского бюро «Юрлов и партнеры».

Юрист Павел Кугач считает, что в ближайшее время не стоит ждать коренных изменений в способах борьбы с пиратством. «Однако законодатели могут уделить внимание развитию цифровой культуры соблюдения авторских прав пользователей, а также информированию владельцев сайтов и информационных посредников о требованиях закона и ответственности за их несоблюдение».

Татьяна Петрущенкова

ОБЪЕМ РЫНКА ОНЛАЙН-ПИРАТСТВА В РОССИИ ($ МЛН) ИСТОЧНИК: GROUP-IB.



информационные технологии

+|T1

IT-фабрика в каждую компанию

Объемы софтверной разработки в мире за последние десять лет возросли многократно. Как утверждают представители бизнеса, размер кодовой базы в компаниях в мегабайтах и по числу репозиториев увеличился более чем в 100 раз по сравнению с 2010-ми, а почти в каждой пятой компании показатели выросли в 500 раз. Это привело не только к развитию языков программирования и архитектур, но и к появлению нового класса индустриальных систем для взаимодействия разработчиков друг с другом. Почему сегодня без этих инструментов невозможно организовать создание цифровых продуктов, рассказывает первый заместитель генерального директора Группы Т1 **Кирилл Булгаков**.

— экспертное мнение —



ПРЕДОСТАВЛЕНО Т1 КОНСАЛТИНГ

Конвейер для кода

Широко распространенный сегодня Agile-подход подразумевает, что IT-функция чутко реагирует на запросы бизнеса и оперативно вносит изменения в ПО, которое является костяком любой современной компании и обеспечивает гибкость операционных процессов. Это касается систем, отвечающих в том числе за взаимодействие с клиентами и партнерами, процессов, отражающих выполнение регуляторных правил и многих других.

Необходимость постоянной IT-эволюции и прогрессирующее усложнение систем требуют усилий огромной армии разработчиков, которые зачастую находятся в разных городах. А между ними нужно быстро распределять задачи, открывать людям допуск к различным данным, проверять написанный код и выводить его на релиз. В сложных информационных системах релизы идут на ежедневной основе. В этих условиях необходимо увязывать разрозненные средства производства в одну платформу для организации сквозного процесса разработки ПО и эффективного управления им. Но главное — для сокращения показателя Time-to-Market.

Первопроходцами на рынке производственных платформ стали иностранные системы типа Jira и Confluence, которые получили распространение и в России. С отставанием, но все-таки стали появляться и отечественные сервисы, которые автоматизировали отдельные элементы технологического процесса, например управление задачами или тестирование. Однако полноценной платформы с необходимым технологическим стеком до недавнего времени не было. Это означает, что для российских IT-компаний открылась емкая ниша, так как в условиях импортозамещения все инструменты, упрощающие и ускоряющие создание цифровых продуктов, приобретают все большую ценность. Наибольшего успеха в автоматизации софтверной разработки достигнут те компании, которые опираются именно на платформенный подход и хорошо знают болевые точки отечественного бизнеса, запускающего внутри IT-фабрику.

Для бизнес-клиентов тонкие настройки не менее важны, чем набор высокотехнологичных инструментов. Это нам в Т1 хорошо известно, так как последние 20 лет мы внедряем лидерам российского рынка корпоративные CRM-системы и вот уже более четырех лет разрабатываем собственные цифровые продукты. Именно продажа преднастроенного решения, где есть, например, возможность получать содержательную отчетность в различных срезах, всегда дает конкурентное преимущество.

Именно поэтому, создавая производственную платформу ПО «Сфера», Т1 сфокусировалась на методологии, чтобы у пользователя не возникало необходимости в кастомизации платформы и долгой адаптации к работе с ней.

Образно говоря, мы смогли организовать производство средств производства. «Сфера» позволяет сделать «токарный» станок для IT, на котором «IT-токари» могут выточить свой программный продукт. В частности, продукт, соответствующий еще одному тренду на IT-рынке — Low-Code и No-Code: создаваемое программное обеспечение клиент может использовать с относительно ограниченным как с точки зрения числа, так и компетенций человеческим ресурсом.

Задача состояла в том, чтобы выстроить бесшовный процесс создания программного продукта не для одной команды, а для команды команд. К примеру, у одного из наших заказчиков несколько сотен стримов (команд) разработки. Этой армии нужен удобный инструментарий для совместной работы и взаимодействия. Впрочем, и маленькому коллективу в десять человек тоже надо планировать задачи, следить за их выполнением, тестировать код, поэтому мы рассчитываем, что платформа будет интересна компаниям разного формата, а общее число конечных пользователей достигнет в скором времени 200 тыс. человек.

Сейчас «Сфера» — это более 40 инструментов «из коробки». Самые востребованные из них — те, что используются для управления задачами, знаниями, тестовыми данными, а также для мониторинга бизнес-процессов. Если попытаться собрать аналог из решений разных вендоров, интеграция такой системы может занять год, «Сфера» разворачивается в пределах одного квартала. В настоящее время идут пилотные внедрения у ключевых клиентов Т1, на основании которых мы получаем продуктивную обратную связь по доработке платформы.

Наука продавать

Грамотная организация процесса разработки — один из важнейших факторов быстрого появления зрелых отечественных решений. Задача «за несколько лет создать аналог программных продуктов», которые разрабатывались и совершенствовались почти 40 лет, очень амбициозная.

Пазл «спрос—предложение» сложится только в том случае, если государство предпримет усилия по поддержке цифровой миграции. Со стороны предложения — анонсируя гранты на разработку ПО, которое признается критически важным. Со стороны спроса — проявляя готовность кредитовать по льготной ставке участников проектов внедрения. Для обеих сторон вопрос финансовой ограниченности — один из основных. Несмотря на появление множества претендентов занять IT-ниши западных вендоров, дефицит ресурсов, экспертизы и времени серьезно замедляет создание продуктов в сегменте комплексных ERP-систем enterprise-сегмента.

Образно говоря, бизнесу нужен конструктор, к которому прилагаются понятные инструкции, готовые к применению разными заказчиками

Крупнейшим российским заказчикам IT-решений, которые обязаны перевести критически важные системы на отечественное ПО, придется сделать существенные инвестиции. В условиях растущих экономических рисков и сокращения доходной базы такое решение принимать гораздо сложнее, поэтому реальная миграция на российский софт идет в тех секторах, где уже совсем невмоготу. Например, крупнейшие авиаперевозчики переходят на российские системы бронирования: во-первых, есть риски отключения существующих платформ от западных вендоров, во-вторых, растет желание хранить клиентские данные, которые намного ценнее информационной инфраструктуры, в собственных системах.

Конечно, на нашем рынке есть отечественные решения, которые уже завоевали свое место — например, потому что исторически развивались с учетом регуляторной специфики. Из-за законодательных барьеров почти 100% информационных банковских систем — это отечественные решения. Именно учет отечественной специфики обеспечил лидерство 1С. Похожая история с разработками элементов искусственного интеллекта. Хотя BI-решения на однозначно лидерской позиции на рынке еще нет, инструментов machine learning разработано достаточно много.

IT-компаниям придется много поработать на аренах улучшений, чтобы побороть не всегда оправданные предубеждения против российских продуктов. Отчасти они объясняются тем, что на уже внедренные системы потрачены миллиарды рублей, и пока они неплохо работают. Теперь же бизнесу требуется инвестировать в разработку и инсталляцию отечественного ПО часть своей прибыли, которую в текущей ситуации хотелось бы сэкономить.

Еще одна задача — развеять психологическую привязанность нашего бизнеса к западным вендорам, которые на российском рынке включали маркетинговые машины на полную мощь. Отечественным компаниям предстоит учиться работать с таким же лоском — с качественными маркетинговыми материалами, затратами на презентационную часть. Чем раньше компании поймут, что эволюция их бизнес-модели требует изменений по всем направлениям, тем раньше будет достигнут результат. Возросшая востребованность отечественных решений вселяет в нас осторожный оптимизм, что с вызовами справимся.

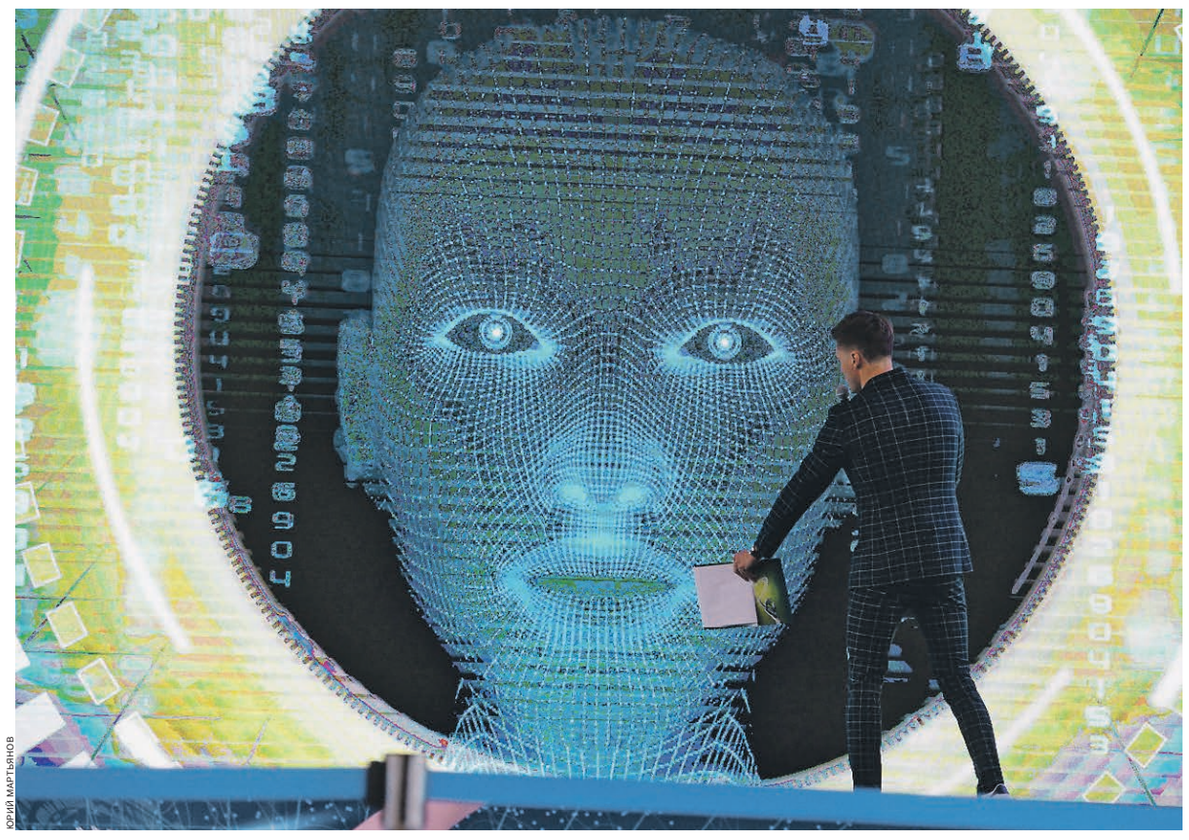
Во-первых, потому что государство принимает в этом процессе деятельное участие, подталкивая бизнес к разработке и внедрению отечественных программных продуктов — в ряде случаев ограничительно, а в ряде случаев поощрительно, путем субсидий.

Параллельно с количеством будет идти и качество: мы полагаемся на отечественную школу программистов, одну из сильнейших в мире. Посмотрите, каким спросом пользуются российские разработчики на глобальном рынке. Наши команды могут интенсивно создавать программный продукт за счет того, что умеют писать качественный код и обладают высокой культурой производства. Это и стоит монетизировать.

Дрон-опылитель, бот-судья и виртуальный блогер

— искусственный интеллект —

Сегодня решения на основе искусственного интеллекта (ИИ) распространены в финтехе, ритейле, медицине, логистике, промышленности, маркетинге и других индустриях. «Умные» алгоритмы просчитывают маршруты, следят за износом оборудования, помогают ставить диагнозы и настраивать рекламу. И хотя технология далека от зрелости, ее можно встретить практически в любой, даже самой неожиданной сфере: от интеллектуальных зубных щеток до синтезированных вкусов пива.



ЮРИЙ МАРТЬЯНОВ

До чего дошел ИИ

С прошлого года в одном из лучших университетов Китая учится виртуальная студентка-бот. Этим летом подобного «специалиста» крупный разработчик игр назначил директором филиала. Тогда же искусственный интеллект впервые самостоятельно составил обвинительное заключение в суде.

Казалось бы, недалеко и до голливудского «Скайнета», однако в реальности за пределы лабораторий и единичных экспериментов вышел только так называемый узкий, или слабый, ИИ. Он не способен переключаться на кардинально новые задачи, но в отдельных сферах уже превосходит человека. Так, например, в конце 2020 года нейросеть AlphaFold предсказала структуру сотен тысяч белков с точностью до атома — это необходимо для разработки важнейших лекарств, и над этой задачей ученые бились десятки лет.

Заметные успехи «узкий» ИИ демонстрирует и в компьютерном зрении, обработке естественного языка, рекомендательных системах, а порой его способности находят себе очень нетривиальное применение. Так, ИИ судит не только преступников — как подсказывают специалисты компании-разработчика EORA, существуют «умные» системы поддержки судейства в гимнастике, футболе и боевых искусствах. Высокоскоростные лидары отслеживают движения спортсменов во время соревнований и тренировок, формируют трехмерные изображения, алгоритмы делают выводы и тем самым нейтрализуют человеческий фактор.

«Нейросети давно используют в агропромышленности, но ученые пошли дальше и разрабатывают заменителей пчел: роботы смогут самостоятельно передвигаться между грядками, находить созревшие цветы и опылять их с помощью воздушных импульсов,— перечисляет эксперт по цифровой трансформации Сергей Лукашкин.— ИИ уже помогает с селекцией парфюма, разработкой новых вкусов и рецептов. Даже открылся первый в мире ресторан с виртуальным шеф-поваром».

Инновации облегчают жизнь и студиям продакшна, продолжает эксперт: «Свежий клип „Age of Illusion“ группы Die Antwoord сгенерировали нейросети, как и иллюстрации к песне Егора Летова „Все идет по плану“. Быстро развиваются и дипфейки: все видели, как нарисованный Брюс Уиллис рекламирует российского сотового оператора». Теперь от создателя контента требуются лишь интересная идея и грамотный запрос — все остальное возьмут на себя «умные» сервисы, считает профессор Высшей школы бизнеса ВШЭ Евгений Зараменских. В качестве примера он приводит энтузиаста Фабиана Штельцера, который занимается фантастическим сериалом «Salt»: видеоряд, звуки, текст создает ИИ, а зрители голосуют за лучшие образы и сюжетные повороты.

Продвинутые чат-боты проводят сеансы психотерапии, поддерживают людей с серьезными заболеваниями вроде болезни Альцгеймера: дают упражнения для памяти, напоминают о ежедневных делах, беседуют на отвлеченные темы. «Современные нейросети обучены на терабайтах данных — от „Википедии“ до интернет-форумов — и способны генерировать грамматически корректный, связный и релевантный текст, и в итоге получается реалистичный диалог. Более того, с ботами можно построить отношения: пользователи делятся, что достигают взаимопонимания, особой связи и даже интимной близости, а некоторые рассказывают о ссорах и абьюзе,— указывает Дарима Мызленова, инженер-исследователь Just AI.— Учитывая, что появляются сервисы, с помощью которых можно „оживить“ фотографию и синтезировать нужный голос, возможности открываются захватывающие: от дискуссии с Илоном Маском до встречи с Галилео Галилеем».

Искусственных инфлюенсеров и звезд можно встретить уже не только в личных переписках. «В Южной Корее появилась музыкальная группа Eternity, участницы которой — технологическое чудо,— добавляет президент агентства Invite Роберто Панчвидзе.— У самого популярного в мире виртуального блогера Лу-ду-Магалу 6 млн подписчиков в Instagram. Другой ИИ-персонаж, Лил Микела, работает моделью, сотрудничает с именитыми домами мод вроде Chanel и Gucci и постоянно общается с пользователями в комментариях, причем делает это не по-машинному. Так, однажды Лил рассказала о том, что до нее домогались в такси, чтобы осветить проблему насилия и поддержать пострадавших».

ИИ как человек

В 2015 году в продвинутой на тот момент нейросети ResNet было заложено около 60 млн параметров — меньше, чем нейронов у обычной домовой мыши. У M6 — одной из самых развитых современных сетей — 10 трлн параметров. Это много, но все еще далеко от человеческого мозга: в нем около 86 млрд нейронов, между которыми, по разным оценкам, от 100 триллионов до триллиарда связей. Кроме того, с увеличением числа параметров растет «замусоренность» системы и вероятность сбоев.

Впрочем, электронный разум все же способен вскоре потеснить рынок труда: под ударом окажутся копирайтеры, дизайнеры, видеоредакторы, разработчики и многие другие, предупреждает господин Зараменских. «Считать продукт, выданный алгоритмом, за искусство или плагиат — второй вопрос. Но если программа за секунды и копейки генерирует логотип, то зачем компании нанимать иллюстратора? Вот о чем стоит подумать в первую очередь,— рассуждает профессор.— И пострадают не только доходы новичков».

Остается и вопрос ответственности, напоминает господин Лукашкин: «Кто отвечает за ошибки ИИ? Пока то, что мы называем „искусственным интеллектом“, не обладает ни свободой воли, ни субъектностью. В то же время не всегда честно призвать к ответу разработчиков. Думаю, в скором времени у нас будут прецеденты: этой осенью нью-йоркской художнице удалось получить авторские права на комикс, созданный с помощью машины».

Главная опасность кроется в злоупотреблении технологией. В качестве примера Николай Янковский, продакт-менеджер Volkswagen Digital Solutions, указывает на уязвимость потребителей: «Большинство персональных данных не слишком тщательно защищают. Узнав ваши предпочтения, ИИ может моментально подобрать товары или услуги, от которых практически невозможно будет отказаться. Представьте, что производители условной газировки находят такой вкус напитка, на который покупатель точно подсядет вне зависимости от того, полезный он или вредный».

Наравне с предостережениями эксперты говорят о возможностях: беспилотный транспорт, эффективные и безопасные лекарства, генетически улучшенная еда… Ведущий инженер Huawei Дмитрий Хизбуллин рассчитывает, что скоро ИИ от концепт-артов и дизайна перейдет к инженерным решениям, проектированию и производству техники, мебели и зданий. Медиаисследователь Юлия Загитова указывает на то, что анализ больших данных поможет добывать важные статистические данные: «По расходам в аптеках можно понять, какие регионы больше нуждаются в госзакупках для льготников. Рабочие места можно сопоставить с программами подготовки кадров. Рождение детей — с планами строительства детских садов. А уж индекс роста цен ИИ наверняка вычислит гораздо быстрее и правдивее, чем сотрудники Росстата».

ИИ всемогущий

«Когда алгоритмы будут способны принимать решения, опираясь не только на исторические данные, но и на синтезированные ими варианты будущего — тогда можно будет говорить о невероятном прорыве, технологической сингулярности»,— считает Руслан Ахтямов, директор по стратегии и сооснователь Napoleon IT. Скорее всего, универсальный и мощный искусственный интеллект, наделенный самосознанием и стремлением к саморазвитию, появится не раньше начала следующего века — и тогда у человечества будет шанс получить ответы на вечные вопросы. «Быть может, именно машина скажет человеку, в чем состоит смысл жизни? Или, что куда практичнее, смоделирует какие-то чрезвычайно сложные процессы вроде развития цивилизаций или угасания звезд»,— предполагает преподаватель школы программистов МШП Василий Лысов.

Масштабы вычислительных потребностей такого супер-ИИ потребуют пересмотра современных носителей информации: вероятно, «разум будущего» не обойдется без квантовых технологий. «В части задач квантовый компьютер неизмеримо быстрее классического, и предел совместной мощи искусственного интеллекта и квантов нам только предстоит осознать. Вполне возможно, что предела и нет,— размышляет Алексей Федоров, основатель QBoard и руководитель научной группы „Квантовые информационные технологии“ в РКЦ.— Вопросов тут масса. И, пожалуй, самый важный — как доверять решениям машины, если мы не можем проверить результаты? Иными словами, как понять, когда система ведет себя как разумная, а когда на самом деле разумна?»

За появлением «всесильного» ИИ последуют глобальный слом в цепочке создания ценностей и пересмотр самих ценностей, уверен господин Ахтямов: «Ритм жизни сейчас задает человек, а появлением ИИ „из кино“ наша роль кардинально изменится, и об этом стоит думать уже сейчас». В любом случае важно помнить, что искусственный интеллект не живое существо, по крайней мере в традиционном понимании, добавляет Константин Панченко, генеральный директор Quatromatic. А значит, станет искусственный интеллект «худшим или лучшим событием в истории человечества» — решать только нам.

Варвара Краснова

Тематические страницы газеты «Коммерсантъ» («Информационные технологии»). | **Владимир Желонкин** — генеральный директор АО «Коммерсантъ», главный редактор | **Сергей Вишневский** — руководитель фотослужбы | **Рекламная служба:** Тел. (495) 797-6996, (495) 926-5262 | **Владимир Лавицкий** — директор «Издательского синдиката» | **Роман Рожков** — выпускающий редактор | **Ольга Еременко** — редактор | **Сергей Цомык** — главный художник | **Галина Кожеурова, Екатерина Репях** — фоторедакторы | **Екатерина Бородулина** — корректор | Ограничение: 16+