ОФИЦЕРЫ КИБЕРБЕЗОПАСА

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? ТАТЬЯНА ИСАКОВА

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 «G» 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».

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. 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.

ФОТО: ИГОРЬ ИВАНКО

КИБЕРБЕЗОПАСНОСТЬ — ОТРАСЛЬ, ДЛЯ КОТОРОЙ ОСНОВНЫМ ДРАЙВЕРОМ СТАНУТ ПРОИСХОДЯЩИЕ В МИРЕ СОБЫТИЯ

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.

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.

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 «G» 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 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. ■