РБК+

ТЕМАТИЧЕСКОЕ ПРИЛОЖЕНИЕ К ЕЖЕДНЕВНОЙ ДЕЛОВОЙ ГАЗЕТЕ РБК

Пятница, 26 августа 2022 | № 93 (3586)

Решения

Как российская киберзащита заменяет западную

→ 4

Кибербезопасность

ТЕНДЕНЦИИ | **С чем связаны резонансные утечки данных в российских компаниях**

РОСТ КИБЕРПРЕСТУПНОСТИ *в России сопровождается* **ИЗМЕНЕНИЕМ** *характера* **КИБЕРУГРОЗ:** *фиксируется все* **БОЛЬШЕ** *целенаправленных, сложно организованных* **АТАК НА** *цифровую* **ИНФРАСТРУКТУРУ** *организаций.*

Хакеры становятся точнее

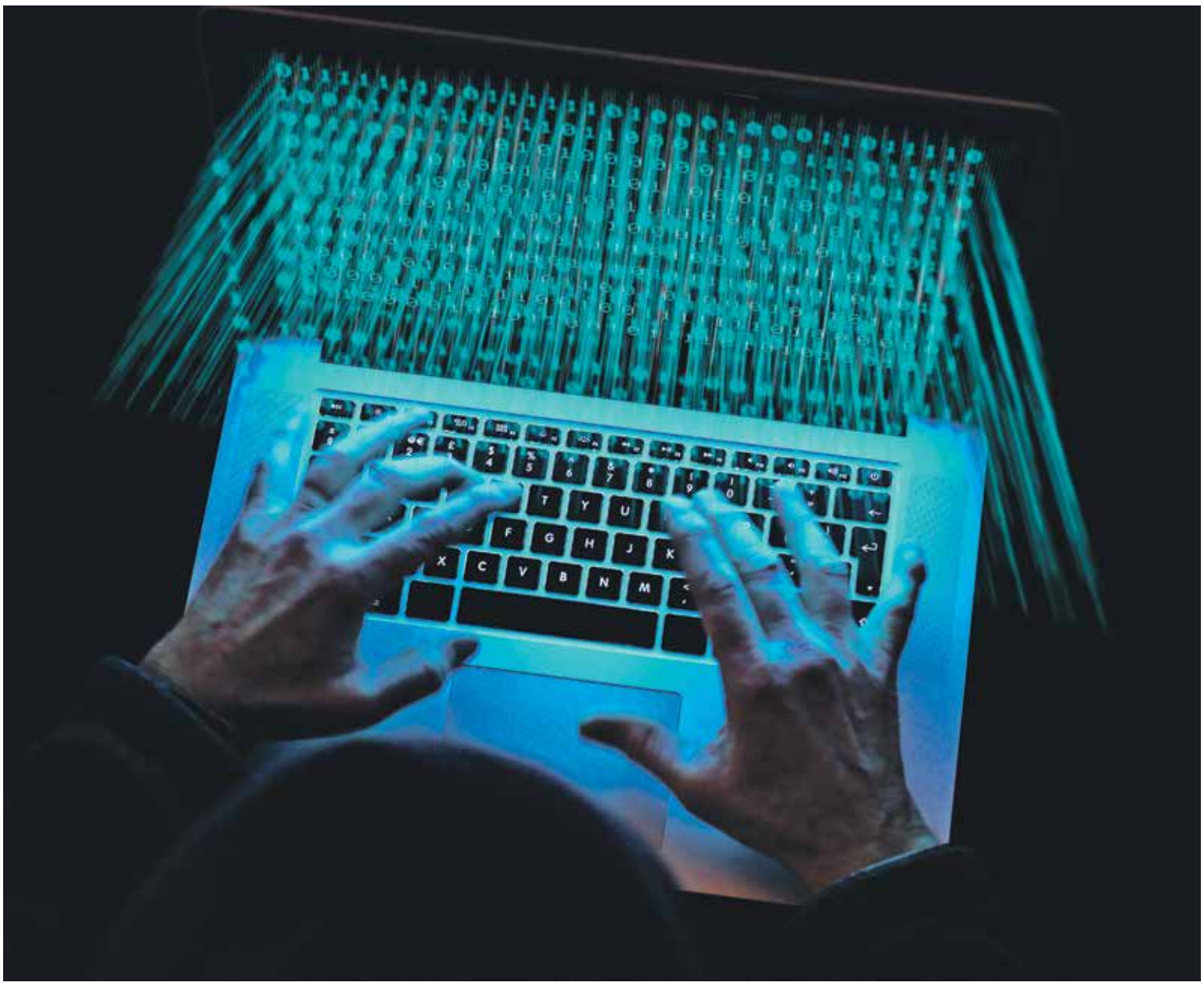

Фото: Getty Images Russia

МАТВЕЙ МИШИН

Рост киберпреступности отмечается в большинстве стран, в том числе и в России. Согласно данным исследования компании «Ростелеком-Солар», во втором квартале командой Solar JSOC было зафиксировано более 236 тыс. событий, связанных с информационной безопасностью (ИБ) российских компаний, что на 31% превышает показатель за аналогичный период прошлого года. В целом в первом полугодии 2022 года количество ИБ-инцидентов выросло практически на четверть.

Несомненно, геополитические обстоятельства привели к изменениям и в ландшафте киберугроз — прежде всего резко возросло их количество, отмечает руководитель службы исследований, кибераналитики и развития Группы Т1 Александр Новиков. Во втором квартале 2022 года, по его словам, значительно усилилась активность хактивистских групп. В результате их атак была нарушена работа многих российских онлайн-сервисов, в том числе критических, оказались скомпрометированы данные нескольких крупных российских компаний. Аналитики российского сервиса разведки утечек данных и мониторинга даркнета DLBI, проанализировав наиболее резонансные истории 2022 года, связанные с попаданием в открытый доступ баз данных компаний «Яндекс.Еда», СДЭК, «Гемотест», и ряд других инцидентов, пришли к выводу, что основным источником утечек стал взлом злоумышленниками серверов баз данных. На него приходится 68% в общем объеме утечек, при том что в прежние годы утечки были в основном инсайдерскими — связанными с действиями недобросовестных сотрудников. «Утечка данных наносит ощутимый удар по репутации и финансовому состоянию любой организации и потому является одной из самых опасных угроз в киберпространстве», — отмечает Александр Новиков.

БЬЮТ В ЦЕЛЬ

Эксперты отмечают смену вектора кибератак с массовых на целевые. «С начала года мы заметили всплеск сложных целенаправленных атак APT-группировок (от англ. advanced persistent threat — постоянная серьезная угроза. — РБК+)», — говорит руководитель исследовательской группы департамента аналитики ИБ компании Positive Technologies Екатерина Килюшева. Общее количество целевых атак в мире, по словам Александра Новикова, во втором квартале 2022 года в мире увеличилось на 16% год к году, в России — на 10%. Хотя Екатерина Килю-

→ 2

Тенденции

← 1

шева уточняет, что все же основной рост киберпреступности в основном пока происходит за счет массовых «простых» атак.

Злоумышленников, организующих целевые атаки, интересует конкретная компания, государственная или военная организация, а иногда и целая отрасль. «Подобные атаки обычно хорошо спланированы и включают несколько этапов — от разведки и внедрения до сокрытия следов присутствия. Как правило, в результате целенаправленной атаки злоумышленники закрепляются в инфраструктуре жертвы и остаются незамеченными в течение продолжительного времени», — поясняет Александр Новиков. По его словам, был отмечен резкий рост использования политической тематики при распространении фишинговых писем APT-группировками. В одной из атак APT-группировка, к примеру, использовала сайт, содержание которого имитировало ресурс Минздрава России. Также выявлены APT-атаки на компании финансового сектора, организованные известными преступными группами FIN7, Evilnum, Mummy Spider и RedCurl.

Как показывает статистика инцидентов от SOC (security operations center) компании КРОК, в последние месяцы хакеры стали все больше обращать внимание на средний бизнес, где уровень информационной безопасности, как правило, ниже, чем в крупных компаниях. «При этом основной целью злоумышленников становятся не финансовые подразделения организаций, а отделы закупок, производства», — поясняет руководитель центра мониторинга кибербезопасности КРОК Евгений Ляпушкин.

Директор по развитию облачных и инфраструктурных решений компании «МегаФон» Александр Осипов отмечает также изменение географии киберпреступности. «В части анти-DDoS, к примеру, мы можем отслеживать, с каких IP происходят запросы со зловредным трафиком. И если до февраля—марта атаки шли в подавляющем большинстве случаев из-за границы — Латинской Америки, Азии, Восточной Европы, то сейчас хакеры поняли, что мы научились достаточно легко шейпить (ограничивать пропускную способность каналов. — РБК+) иностранный трафик, фильтровать его по геопризнаку. Поэтому они начали поднимать сеть ботнетов внутри России», — делится информацией эксперт.

↑ Эксперты отмечают смену вектора кибератак с массовых на целевые

Фото: Getty Images Russia

НА ВЫДУМКИ ХИТРЫ

Одними из наиболее распространенных киберпреступлений являются распределенные DDoS-атаки на онлайн-сервисы и сайты частных и государственных организаций, имеющие целью перегрузить ресурсы запросами, чтобы они «упали». Согласно данным Cloudflare, наибольшее количество DDoS-атак в мире пришлось на авиационную и аэрокосмическую отрасль. Следом идут интернет-провайдеры, BFSI (банки, финансы и страхование), на четвертом месте — игровая индустрия. В России 45% DDoS-атак пришлись на банки, финансовые учреждения и страховые компании, второй по величине мишенью стала криптовалютная индустрия, за которой следуют СМИ.

Александр Новиков также отмечает усиление активности в отношении российских компаний со стороны шифровальщиков — вредоносного программного обеспечения, предназначенного для вымогательства после шифрования файлов в системе. Причем их целью, как говорит эксперт, далеко не всегда выступает непосредственная нажива, во многих случаях это стремление помешать работе бизнеса. По-прежнему в тренде у злоумышленников атаки класса supply chain (кибератака на цепочку поставок) и trusted relationship (использование расширенных прав доверенной компании, например подрядчика, партнера, интегратора, для доступа к инфраструктуре жертвы), продолжает Александр Новиков: «Привлекательной мишенью для них являются компании, занимающиеся разработкой ПО. Компрометация инфраструктуры такой организации создает угрозу проникновения в корпоративные сети множества клиентов».

В апреле—июне 2022 года был замечен ряд атак с использованием различных вредоносных библиотек с именами, схожими с легитимными популярными пакетами, рассказывает Александр Новиков: «Злоумышленники размещают их в официальных репозиториях и рассчитывают на невнимательность разработчиков, которые по ошибке могут добавить их в свои проекты». Также, по его словам, во втором квартале по отношению к январю—марту отмечено увеличение объема фишинга — остаются актуальными темы мошенничества, связанного с опросами, выплатами, поддельными сайтами, рассылками. Общее число выявленных подозрительных сайтов во втором квартале составило более 4 млн ресурсов, при том что количество новых проверенных доменов увеличилось по сравнению с первым кварталом на 8700%. При этом ресурсов с реально выявленным фишинговым контентом стало больше вдвое — 514 тыс. против 270 тыс. в январе—марте. Лидерами по популярности среди хостинг-провайдеров являются Reg-RU и Beget, отмечает представитель T1.

ОШИБКИ В ОБОРОНЕ

В целом уровень защищенности российских организаций от кибератак пока оставляет желать лучшего, говорят эксперты. «Например, в 2021 году во всех компаниях, где мы проводили проверки, исследователь мог взломать сетевой периметр, получить доступ к корпоративным ресурсам и полный контроль над инфраструктурой, — рассказывает Екатерина Килюшева. — Более того, когда перед нами стояла задача проверить возможность осуществления событий, которые крайне нежелательны для деятельности компании, например протестировать возможность кражи определенной суммы денег, проведения мошеннических операций, компрометации данных клиентов, в 71% случаев это удавалось сделать». В 2022 году ситуация не улучшилась, ссылается эксперт на оценки аналитиков Positive Technologies.

Как говорит директор департамента управления рисками компании ДРТ (ранее российский офис «Делойт») Алексей Яковлев, многие компании в ходе массового ускоренного внедрения разносторонних продуктов в цифре зачастую игнорируют базовые правила кибербезопасности. «С другой стороны, при внедрении экспериментальных прототипов и использовании новых технологий возникают дополнительные угрозы, в отношении которых в компаниях еще не выработаны меры противодействия. В ряде случаев это становится препятствием для реализации проектов цифровизации», — уточняет эксперт. Даже в крупных компаниях, по его словам, всегда актуален вопрос обоснования затрат на ИБ, поэтому профильные подразделения зачастую идут по пути наименьшего сопротивления, направляя усилия в понятные технические и прикладные меры. «В итоге мы часто видим, что оценка влияния рисков ИБ на деятельность бизнеса не происходит или происходит в ограниченном масштабе, отсутствует связь с целями компании, со стратегией развития и т.д.», — говорит Алексей Яковлев.

Екатерина Килюшева, впрочем, отмечает, что в последнее время в РФ наблюдается повышенный спрос на продукты, решения и услуги по киберзащите. Прежде всего бизнес интересуют решения для анализа сетевого трафика, мониторинга событий в инфраструктуре и выявления инцидентов, решения для защиты веб-приложений.

68%

утечек данных в компаниях происходит из-за взлома серверов хакерами, по данным DLBI. Еще недавно основная часть утечек была на совести сотрудников самих компаний

«КИБЕРБЕЗОПАСНОСТЬ» (18+)

Тематическое приложение к «Ежедневной деловой газете РБК»

Является неотъемлемой частью «Ежедневной деловой газеты РБК» № 93 (3586) от 26 августа 2022 г.

Распространяется в составе газеты

Материалы подготовлены редакцией партнерских проектов РБК+

Рекламно-информационный проект: ПАО «МегаФон»

Учредитель: ООО «БизнесПресс»

Издатель: ООО «БизнесПресс»

Директор ИД РБК: Ирина Митрофанова

Главный редактор партнерских проектов РБК+: Наталья Кулакова

Редактор РБК+ «Кибербезопасность»: Юрий Львов

Выпускающие редакторы: Алина Петракова, Марина Зубакова

Руководитель дизайн-департамента: Николай Реутин

Дизайнеры: Дмитрий Иванов, Сергей Пивоваров

Фоторедактор: Алена Кондюрина

Корректоры: Татьяна Поленова, Маргарита Тарасенко

И.о. главного редактора газеты: Петр Геннадьевич Канаев

Рекламная служба: 8 (495) 363-11-11, доб. 1342

Коммерческий директор издательства РБК: Анна Брук

Директор по продажам РБК+: Евгения Карлина

Директор по производству: Надежда Фомина

Адрес редакции: 115280, Москва, ул. Ленинская Слобода, д. 26, стр. 3

От первого лица

О возможностях российского бизнеса противостоять киберугрозам **РБК+** рассказал директор по развитию облачных и инфраструктурных решений компании **«МЕГАФОН»** **АЛЕКСАНДР ОСИПОВ**.

«Запрос на защиту вырос даже со стороны киберскептиков»

Насколько отечественный бизнес сегодня защищен от киберрисков, растущих на фоне цифровизации и меняющихся геополитических условий?

Многое зависит от степени цифровизации компаний: чем она выше, тем более развиты в ней средства защиты информации (СЗИ). В пример можно привести отечественные банки, телеком, цифровое производство, e-commerce, а также государственные сервисы, где киберзащите уделяется колоссальное внимание.

В то же время бизнес, который работает преимущественно в офлайне и не внедрил автоматизацию технологических и бизнес-процессов, особенно малый и средний, защищен от киберугроз значительно меньше. Мы всегда говорим, что даже рабочий компьютер главы компании является точкой уязвимости, которую нужно защищать, так как с него ведутся коммуникации, в нем находятся «эксели» с клиентами, бухгалтерия, информация, раскрытие которой может нести репутационные риски.

Затраты компаний на борьбу с киберрисками даже до пандемии росли на уровне 10–15% в год. COVID-19, переход на удаленку, текущее развитие событий в мире стали только катализаторами процесса. И сейчас, когда количество кибератак многократно увеличилось, запрос на защиту значительно вырос даже со стороны компаний-киберскептиков. Многие смогли убедиться, насколько внедрение средств защиты может быть эффективным. Правда, большинство поняли это, лишь подсчитав ущерб после кибератаки.

Как нарастают кибератаки?

В 2022-м, начиная с конца февраля, количество DDoS-атак (перегрузка сайтов компаний запросами с целью заблокировать их работу. — РБК+) выросло почти в десять раз, количество взломов, фишинговых атак (мошеннических способов получения конфиденциальной информации. — РБК+) — в два—пять раз. Почти 38% компаний понесли потери в той или иной форме из-за действий компьютерных злоумышленников. Для каждой пятой компании эти потери были финансовыми, превышающими 5 млн руб.

Согласно исследованию, проведенному компанией «МегаФон» среди своих действующих и потенциальных клиентов с января по март 2022 года, 90% из них подвергались кибератакам в 2021 году. Такой же процент опрошенных столкнулся с новыми видами уязвимостей, которые открыл переход бизнеса в онлайн.

При этом около 40% респондентов поделились информацией об эффективном срабатывании СЗИ, которые они устанавливали ранее, предвосхищая киберриски.

Как работает регулирование в этой сфере?

Регуляторика является одним из действенных драйверов внедрения средств кибербезопасности и защиты активов во всем мире. История с защитой персональных данных в РФ начала развиваться даже раньше, чем на Западе, — в 2006 году, когда появился ФЗ-152, который предполагает четыре уровня защищенности для различных категорий операторов персональных данных в зависимости от вида деятельности и пр. Так, для крупных компаний, в том числе банков и телеком-компаний, владеющих большим объемом данных, предусмотрено около 200 пунктов требований к их инфраструктуре киберзащиты.

Европейский аналог нашего закона GDPR (General Data Protection Regulation) вступил в действие только в 2018 году. В нем сразу были предусмотрены фискальные меры за утечку данных — взыскание оборотных штрафов, а также их увеличение в случае неуведомления регулятора.

Сейчас в Минцифры РФ подготовлен законопроект, который ужесточает ответственность компаний за утечку данных. Он предполагает

Фото: пресс-служба

введение с 2023 года оборотного штрафа в размере 1%. Документ готовился давно, но катализатором стали геополитические события в мире, которые усилили активность хакеров. Таким образом, помимо прямой угрозы от кибератак, бизнесу нужно помнить о рисках получения серьезных штрафов за ненадлежащее отношение к защите информации.

Можно также отметить указ президента РФ №250, призванный усилить информационную безопасность стратегических предприятий и организаций, находящихся сейчас под шквалом хакерских атак. Такие структуры должны быть эшелонированно защищены и находиться под постоянным мониторингом, ведь киберугрозы меняются.

При этом небольшим операторам персональных данных российское законодательство дает послабление: они могут не внедрять СЗИ, если для них это экономически нецелесообразно. Хотя им все равно нужно как минимум поставить недорогие средства защиты по сервисной модели (антиспам, антифишинг, антивирус) и главное — обучить сотрудников элементарным принципам цифровой гигиены.

Насколько у бизнеса получается угнаться за этим «прогрессом»?

К сожалению, не всегда менеджмент компаний успевает быстро понять тренды цифровой повестки. А внедрение любой цифровой инновации — это появление еще одной точки уязвимости, которую необходимо отслеживать и защищать.

Какой при этом может быть роль телекоммуникационной компании?

Мы идем в русле мировой практики, где 30% аутсорсинга информационной безопасности (Managed Security Services, MSS) приходится на долю телекома. В первую очередь это, конечно, сервисы, связанные с сетями связи.

Как один из крупнейших операторов связи, мы имеем высочайший уровень компетенций в части защиты от DDoS-атак, криптозащиты, криптошифрования, защиты данных и других направлений, но мы с радостью используем все компетенции группы компаний, среди которых и разработчики СЗИ, и команды пентестеров, и инженеры внедрения решений информационной безопасности. Логично, что нужно монетизировать то, что у тебя хорошо получается.

Нашим партнером в рамках холдинга USM Group (владеет и управляет активами в сфере телекоммуникаций, технологий и интернета, металлургии и горной добычи. — РБК+) является компания «Гарда Технологии», продуктами которой мы пользуемся сами и знаем, как их внедрять. К примеру, для контроля потоков конфиденциальной информации внутри компании существует решение Data Loss Prevention (DLP, предотвращение потери данных). Или, скажем, «Гарда» является одним из немногих российских вендоров, если не единственным, которые предоставляют решение для защиты баз данных DAM (Database Activity Monitoring). Эта программа отслеживает обращение пользователей к базам данных. Если пользователь запрашивает нетипичный для себя объем данных, обращается к ним, хотя его задачи этого не подразумевают, или же администратор разворачивает теневые базы, решение отправляет алерты ответственному сотруднику.

Мы делаем и собственные продукты, например голосовой антифрод, который позволяет банкам бороться с телефонным мошенничеством. У нас есть собственная платформа киберразведки — мы научились получать данные о зараженных серверах, фишинговых ссылках, можем предоставлять так называемые индикаторы компрометации: какие инструменты сейчас активно используются мошенниками, какие IP необходимо вносить в черные списки, какие ссылки являются фишингом и т.д. Подобные данные у нас покупают в формате сервиса, их можно скачать по АПИ или через вэб-интерфейс.

Также у «МегаФона» есть решение Security Awareness — обучающая платформа для повышения осведомленности сотрудников компаний-клиентов о правилах информационной безопасности. С ее помощью можно проверить готовность персонала к реальным кибератакам и даже имитировать фишинговую рассылку. Мы рекомендуем начинать борьбу с киберугрозами именно с цифровой гигиены.

> «История с защитой персональных данных в РФ начала развиваться даже раньше, чем на Западе»

Решения

Компании примеряют отечественную киберзащиту

Российские вендоры заполняют ниши в сфере кибербезопасности, освободившиеся после ухода западных поставщиков. По прогнозам, на импортозамещение в большинстве сегментов потребуется два-три года.

МАТВЕЙ МИШИН

Уход из РФ весной 2022 года западных вендоров — производителей средств защиты информации и соответствующих решений может иметь ключевое значение для отечественного рынка информационной безопасности (ИБ). По прогнозам аналитиков Центра стратегических разработок (ЦСР), в ближайшую пятилетку этот сегмент может вырасти в 2,5 раза — с 185,9 млрд руб. по итогам 2021 года до 469 млрд руб. в 2026 году. «При этом начиная с 2023 года практически весь бюджет заказчиков на средства защиты информации (СЗИ) в секторах b2g и b2b будет потрачен на продукцию российских вендоров, что даст возможность роста этой части рынка с 113 млрд руб. в 2021 году до 446 млрд руб. в 2026 году», — говорится в материалах ЦСР.

СВОИ НА ПОДХОДЕ

Опрошенные РБК+ эксперты отмечают, что на рынке уже появляются отечественные аналоги западных технологий в сфере ИБ. Однако многие из них нуждаются в доработке, добавляют наши собеседники.

Уход международных вендоров, несомненно, негативно отразился на защищенности российских компаний от киберугроз — на фоне кратного усиления кибератак они одномоментно потеряли значимую часть ИБ-инфраструктуры, говорит директор департамента управления рисками компании «Деловые решения и технологии» (ДРТ, ранее российский офис «Делойт») Алексей Яковлев. Неприятным обстоятельством, по его словам, является и ограничение доступа к международным передовым технологиям защиты информации в целом. Руководитель службы исследований, кибераналитики и развития Группы Т1 Александр Новиков подтверждает, что с весны текущего года российский бизнес столкнулся с критичными уязвимостями в продуктах компаний Microsoft, Google, VMware, Atlassian. «Многие ушедшие с российского рынка вендоры отключили доступ к репозиториям обновлений для пользователей из России. Компании встали перед выбором: отказаться от такого ПО или продолжать использовать потенциально уязвимый продукт и вводить компенсирующие меры средствами кибербезопасности», — объясняет он.

С другой стороны, отечественная индустрия кибербезопасности получила небывалый стимул к быстрой трансформации — перенаправление на внутренний рынок высвободившихся существенных финансовых ресурсов приведет к качественному росту отрасли за счет российских разработчиков, говорит Алексей Яковлев. Открылось много ниш по различным направлениям ИБ для российских вендоров, соглашается ведущий эксперт направления «Информационная безопасность» компании КРОК Антон Голубков: «Как ИТ-интегратор, мы все больше обращаем внимание на отечественные разработки. Альтернативы западным решениям имеются по большинству направлений: защита от DDoS-атак, межсетевые экраны нового поколения, мультифакторная аутентификация, системы класса SIEM, PAM, DLP, WAF, DAM и пр.».

Директор по развитию облачных и инфраструктурных решений компании «МегаФон» Александр Осипов также отмечает, что у российского бизнеса достаточно богатый выбор внутренних решений почти во всех категориях, связанных с кибербезопасностью. «Конечно, есть западные инновации, отсутствие которых пока не покрывает российский пул вендоров. Тем не менее базовые потребности в различных типах СЗИ можно удовлетворить — начиная от WAF (Web Application Firewall, файрвол веб-приложения — комплексное решение для обнаружения и блокировки атак на уровне приложений) и заканчивая защитой от DDoS, NGFW (Next-generation Firewall — межсетевой экран нового поколения), SIEM (Security Information and Event Management — система мониторинга событий информационной безопасности), криптошифрованием», — говорит Александр Осипов. Причем по многим СЗИ, отмечает он, присутствует реальная конкуренция между российскими поставщиками.

Одним из возможных путей преодоления проблем, связанных с ограничением к решениям по киберзащите из-за ухода западных компаний, руководитель центра мониторинга кибербезопасности КРОК Евгений Ляпушкин называет open source. «Открытое программное обеспечение позволяет экономить на лицензиях и вендорской поддержке, а в текущих условиях дает возможность организациям продолжить использование привычного софта», — говорит он. Но при этом предупреждает, что с начала года злоумышленники все чаще помещают зловредное ПО в код open source-решений, за счет чего получают беспрепятственный доступ к данным и плацдарм для дальнейших злонамеренных действий в ИТ-инфраструктуре компании.

По его словам, вопрос киберзащиты можно относительно быстро решить с помощью аутсорсинга, например за счет использования внешнего центра мониторинга кибербезопасности (SOC), который отвечает за оперативное отслеживание событий информационной безопасности и предотвращение инцидентов. Если для развертывания собственной масштабной ИБ-инфраструктуры необходимы значительные инвестиции и время — от года до трех лет, то SOC as Service предоставляет возможность подключиться к услуге всего за пару недель, говорит Евгений Ляпушкин. «Предприятия все чаще обращают внимание на такие сервисы, поскольку, например, для enterprise-бизнеса каждый час простоя из-за произошедшего инцидента обходится значительно дороже инвестиций в ИБ», — комментирует он.

НУЖНО ВРЕМЯ

Эксперты все же признают, что сил, возможностей и компетенций российским участникам индустрии кибербезопасности по ряду направлений пока не хватает. «Раньше большинство российских разработчиков ПО и поставщиков услуг не задумывались о продуктах в некоторых областях информационной безопасности, так как на рынке были крупные зарубежные представители, тягаться с которыми казалось бесперспективно и бессмысленно», — объясняет Алексей Яковлев. Проблемой, в частности, по его словам, остаются сетевые средства защиты, например NGFW, а также MFA (Multi-Factor Authentication — многофакторная аутентификация), SSO (Single Sign-On — технология единого входа). Многие российские аналоги СЗИ только начинают развиваться и пока не дотягивают до уровня западных конкурентов, решения отечественных вендоров не всегда отличаются богатым функционалом и стабильностью работы, добавляет Антон Голубков.

Разработка недостающих решений может занять до пяти лет, прежде чем российские ИБ-продукты выйдут на должный уровень качества, говорится в материалах ЦСР. Основная же часть освобождаемой доли рынка, по прогнозам ЦСР, будет освоена в течение ближайших двух-трех лет на существующих наработках и решениях российских вендоров.

В целом ситуация для российских вендоров выглядит неплохо, считают аналитики центра: «Они широко представлены на рынке, имеют солидный портфель продуктов и сервисов. Они быстро смогут заменить широкий ряд зарубежных решений и в течение ближайших лет забрать практически весь рынок». Доля зарубежных вендоров на российском рынке ИБ при этом в 2023 году сократится до минимальных 5% (с 39% по итогам 2021 года), прогнозируют в ЦСР, после того как с него окончательно уйдут компании Cisco, IBM, Fortinet, ESET и др. Аналитики центра, однако, предполагают, что положение отечественных вендоров может изменяться в зависимости от уровня параллельного (серого) импорта.

↑ Доля зарубежных вендоров на российском рынке ИБ в 2023 году сократится до 5% с 39% по итогам 2021 года, прогнозируют в ЦСР

446
млрд руб.
могут составить бюджеты российских организаций на средства защиты информации в 2026 году, прогнозируют в ЦСР

Фото: Getty Images Russia