



КОМПАНИИ МЕНЯЮТ КИБЕРЩИТ

ЭКСПЕРТЫ ОТМЕЧАЮТ РОСТ ОТЕЧЕСТВЕННОГО РЫНКА РЕШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВО ВСЕХ СЕГМЕНТАХ — СЕГОДНЯ РЕЧЬ ИДЕТ О 90% РОССИЙСКИХ РАЗРАБОТОК НА ПРЕДПРИЯТИЯХ СТРАНЫ. ВЫРУЧКА КОМПАНИЙ, РАБОТАЮЩИХ НА РЫНКЕ КИБЕРБЕЗОПАСНОСТИ, УДВОИЛАСЬ И ДОСТИГЛА 220–230 МЛРД РУБЛЕЙ. РАЗВИТИЕ СЕГМЕНТА СВЯЗЫВАЮТ С УСИЛЕНИЕМ КИБЕРАТАК НА ФОНЕ САНКЦИЙ И УХОДА ЗАПАДНЫХ РАЗРАБОТЧИКОВ. СРАВНИТЕЛЬНО НОВЫЙ ТРЕНД — АТАКИ НА ПРОМЫШЛЕННЫЕ ПРЕДПРИЯТИЯ, КОТОРЫМ ПОТРЕБОВАЛАСЬ СРОЧНАЯ ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ. ОЛЬГА ГОЛОВИНА

К НАЧАЛУ АВГУСТА 2023 ГОДА В МИНЦИФРЫ РФ ОТЧИТАЛИСЬ, ЧТО ДОЛЯ ОТЕЧЕСТВЕННЫХ ПРОДУКТОВ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДОСТИГЛА 90%. ПО ИТОГАМ 2022 ГОДА ЭТОТ ПОКАЗАТЕЛЬ ДОХОДИЛ ДО 70%

По словам эксперта Института кибербезопасности и защиты информации Политеха Анны Селивановой, Россию покинуло свыше 100 зарубежных производителей систем кибербезопасности. «С февраля 2022 года страна стала, пожалуй, одной из самых атакуемых киберпреступниками стран мира», — констатирует госпожа Селиванова.

«Последние полтора года побили все рекорды по количеству кибератак на российские сайты», — подтверждает генеральный директор агентства DOT Глеб Иванюшкин. — Контроль исключительно внутри организации становится недостаточно. Многие наши клиенты сформировали новые отделы по информационной безопасности, частично делегировав вопросы защиты интернет-проектов диджитал-агентствам».

Среди делегируемых задач он назвал аудит внедренных систем кибербезопасности, обновление лицензий CMS «Битрикс», отслеживание свежих версий серверного ПО, свободных от ошибок и более устойчивых к взлому. «Это можно назвать созданием бастиона первичной защиты от атак DDoS», — говорит господин Иванюшкин.

К началу августа 2023 года в Минцифры РФ отчитались, что доля отечественных продуктов для информационной безопасности (ИБ) достигла 90% (для сравнения, по итогам 2022 года этот показатель доходил до 70%). Рынок российских разработок в сфере ИБ в 2022 году Центр стратегических разработок при правительстве РФ (ЦСР) оценил в 193,3 млрд рублей (+4% к 2021 году). В ЦСР прогнозируют, что к 2027 году его емкость достигнет 559 млрд при росте на 24% в среднем ежегодно. Интерес к решениям кибербезопасности отметили и на рынке IT-стартапов: по данным центра инноваций и инвестиций MTS StartUp Hub, в первом полугодии 2023 года стартапы в сфере ИБ вошли в топ-3 (6% от общего числа стартапов), при этом их количество удвоилось относительно 2022 года.

В ГК «Финам» оценили текущий оборот компаний, работающих на российском рынке кибербезопасности, в 220–230 млрд рублей. «Выручка лидирующих компаний уже сейчас растет почти вдвое за год: темпы прироста составляют 100%. Вполне вероятно сохранение таких темпов в течение двух-трех лет», — комментирует аналитик ГК «Финам» Леонид Делицин.

«Рынок ИБ сильно сегментирован. Сегментация происходит не только по заказчикам (b2b, b2c, b2g), но и по классам средств защиты информации: антивирусы, межсетевые экраны, защиты от несанкционированного доступа (НСД), утечек и т. д.», — говорит руководитель центра комплексной безопасности компании «Ланит» Дмитрий Дудко.

Лидерами рынка среди отечественных вендоров в сфере ИБ (в разных сегментах защиты) являются «Лаборатория Касперского», Positive Technologies, Dr.Web, BI.ZONE, «Ростелеком-Солар», «КриптоПро», «Код безопасности», Innostage, Angara Security.

КИБЕРБЕЗОПАСНОСТЬ С ГОСПОДДЕРЖКОЙ Несмотря на дефицит бюджета в несколько триллионов рублей, государство готово тратить деньги на кибербезопасность. Вероятно, поэтому в 2023 году расходы на федеральный проект «Информационная безопасность» (входит в нацпрограмму «Цифровая экономика», действующую с 2019 года) в 2023 году увеличились более чем на 7%, до 7,9 млрд рублей, в то время как в целом расходы на другие проекты цифровой нацпрограммы урезали на 35%.

Дотации, в том числе разработчикам решений по ИБ, выделяет Российский фонд развития информационных технологий (РФРИТ), «Сколково», Фонд содействия инновациям (ФСИ). На базе Фонда развития интернет-инициатив (ФРИИ) создали акселератор, где инвестируют в IT-стартапы (размер грантов — от 5 до 65 млн рублей, общий размер финансирования на ближайшие годы — по 750 млн в год). ФРИИ финансирует разработчиков решений в сфере криптографии, борьбы с вирусными или DDoS-атаками, защиты от мошенничества.

Кроме денежной поддержки кибербезопасности, разработчиков касаются все стандартные пакеты поддержки IT, включая сниженные страховые тарифы, льготные кредиты, льготную ипотеку, отсрочку от призыва на военную службу.

ПЕТЕРБУРГСКИЙ СЕГМЕНТ Всего, по оценкам экспертов, в Петербурге работает около 300 предприятий, оказывающих услуги в сфере кибербезопасности (включая офисы федеральных игроков). Самый заметный производитель решений в области ИБ — компания «Конфидент» (разрабатывает средства защиты от несанкционированного доступа, защиты виртуальной инфраструктуры и централизованного управления безопасностью). Также ИБ-системы, в том числе для производственных предприятий, производит «Ланит-Терком» (входит в ГК «Ланит»).

Совокупную выручку производителей ИБ-решений из Петербурга и Ленобласти господин Делицин оценивает примерно в 11 млрд рублей (где 9 млрд приходится на Петербург и 2 млрд — на Ленобласть). «Рынок кибербезопасности сильно фрагментирован, и даже доля крупных игроков, как правило, не превышает 5%», — сообщил эксперт. Господин Дудко считает, что оценивать рыночную долю петербургских компаний следует по классам средств защиты. «В таких сегментах, как защита виртуализации и защита от НСД, доля компаний Петербурга приближается к 50%», — подсчитал он.

Предприятия Петербурга и Ленобласти идут в фарватере федерального тренда в сфере ИБ из-за роста числа кибератак. «Мы наблюдаем увеличение спроса на услуги в области информационной безопасности», — делится региональный представитель компании NGR Softlab Андрей Личман. — По нашим оценкам, он составляет 20–25% в год. В ближайшие годы этот темп сохранится».

«Если раньше покупали в основном только антивирус и средства межсетевого экранирования, то сейчас растет спрос и на анализаторы трафика, средства обнаружения атак, средства защиты рабочих станций. Пользуются определенным спросом и системы мониторинга событий, оркестрации (управления сложными компьютерными системами)», — сообщили изданию в пресс-службе правительства Ленинградской области.

В руководстве региона отметили рост затрат организаций на ИБ в диапазоне 15–20%. Среди самых востребованных решений — высокопроизводительные межсетевые экраны (NGFW) и межсетевые экраны уровня приложений (WAF).

ПРОМЫШЛЕННОСТЬ ПОД УГРОЗОЙ

По словам госпожи Селивановой, в последнее время возросло число атак именно на промышленный сегмент. «Раньше в основном от кибератак защищались корпоративные компании, а в последнее время участились атаки на производственные корпорации. Соответственно, эти компании тоже начали серьезно заниматься безопасностью», — описала ситуацию эксперт.

О трендах к защите производств говорят и в «Лаборатории Касперского». Эксперт по кибербезопасности Kaspersky ICS CERT Владимир Дашенко обращает внимание, что одна из ведущих тенденций в сфере цифровизации предприятий — защита сегмента облачных технологий (OT-сегмент), поскольку технологическая инфраструктура все больше подключается к интернету. «Только во втором полугодии 2022 выросла доля компьютеров автоматизированных систем управления (АСУ), на которых блокировались попытки атак вредоносными объектами из интернета:

она увеличилась на 12 п. п. по сравнению с первым полугодием. Из-за этих факторов промышленные организации проявляют больший интерес к специализированным защитным решениям от киберугроз, которые учитывают специфику эксплуатируемых систем, долгий цикл использования оборудования и устаревших версий операционных систем, а также исключают воздействие на производительность и функциональную безопасность АСУ ТП», — комментирует господин Дашенко.

Эксперт уверен, что такие отрасли, как логистика, металлургия, тяжелое машиностроение и другие крупные игроки, будут продолжать активно интегрировать цифровые решения в производственные процессы, но внедрение потенциально увеличивает площадь поверхности кибератаки, а потому решения в сфере ИБ необходимы.

Его слова подтверждают и данные Cdo2day (ресурс АНО «Цифровая экономика», проект Минцифры): в ближайшие три года основная доля IT-затрат производственных предприятий РФ придется на кибербезопас-

ность (затраты на промышленную «цифру» в 2022 году составили около 600 млрд рублей).

«УДАЛЕНЩИКИ» НА ОСТРИЕ АТАКИ

Развитие интернет-среды перевело многие бизнес-процессы, включая работу с подрядчиками на удаленку. «Предоставление доступа к ресурсам компании, в том числе довольно широких прав к критически важным системам, для сотрудников подрядных организаций, внешних специалистов и консультантов стало сегодня стандартной практикой», — обращают внимание в компании «Ростелеком-Солар». Это выявило и новые риски.

«Атаки, реализуемые через поставщиков, в том числе IT-подрядчиков, являются наиболее рискованными для предприятий критической информационной инфраструктуры. Злоумышленники могут получить доступ к инфраструктуре компаний, воспользовавшись уязвимостями в системе информационной безопасности своих партнеров», — поясняет заместитель генерального директора Angara Security Руслан Косарим.

По словам киберэксперта компании «Код безопасности» Павла Коростелева, если у предприятия нет механизмов безопасного удаленного доступа, «злоумышленник может скомпрометировать „учетку“ легитимного пользователя, а затем украсть конфиденциальную информацию, удалить ее или начать распространять по сети. Также хакер может взломать систему и опять же получить доступ к внутренней сети». «Для взлома достаточно скомпрометировать от двух до пяти учетных записей, чтобы получить доступ к критичным цифровым активам», — раскрыл механику взлома господин Косарим. ■

Тематическое приложение к газете «Коммерсантъ» (онлайн-выпуск Санкт-Петербург, Business Guide «Цифровая экономика»)

Владимир Желонкин — генеральный директор АО «Коммерсантъ», главный редактор

Анатолий Гусев — автор дизайн-макета
Андрей Ершов — главный редактор СПб страниц
Александр Коряков — бильд-редактор
Валерий Грибанов — выпускающий редактор
Марина Шевченко — корректор
Василиса Сатирская — верстка
Марина Победенная — рекламная служба

Адрес редакции и издателя: 123112, г. Москва, Пресненская наб., д. 10 этаж 35. Тел. (495) 797-6970. Адрес редакции в Санкт-Петербурге: 191024, Харьковская ул., д. 8А, лит А. Тел. (812) 324-6949

Учредитель: АО «Коммерсантъ». Тематическое приложение к газете «Коммерсантъ», зарегистрировано Роскомнадзором, регистрационный номер и дата принятия решения о регистрации ПИ №ФС77-76923 от 11.10.2019 года

В печатном виде номер не выходит. Распространяется бесплатно. 16+

Графика на обложке: Арсений Блинов