

АЛЛА МИХЕЕНКО,
РЕДАКТОР GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

В ПОИСКАХ ДОВЕРИЯ

Цифровая трансформация уперлась в ожидаемый барьер: люди готовы использовать технологии, но не готовы доверять им. Чтобы пройти этот кризис, вендорам и регуляторам придется думать не только о функционале, но и о психологии цифрового доверия. Потому что даже самый совершенный алгоритм бесполезен, если его боится тот, для кого он создан, и не внедряет его.

Технологии достигли высот: генеративный ИИ уже пишет код и принимает кадровые решения, агродроны сканируют поля с хирургической точностью, а биометрия заменяет пароли. Но парадокс цифровой эпохи в том, что чем совершеннее становятся технологии, тем глубже наша к ним настороженность. Компании внедряют ИИ-ассистентов, но сотрудники перепроверяют их работу. Фермеры, окруженные «умными» датчиками, по старинке щупают землю руками. А каждый взгляд в камеру с распознаванием лиц сопровождается неосознанным страхом: «А что если система узнает обо мне слишком много?»

Этот феномен выходит за рамки обычного техноскептицизма. Кажется, что рост затрат на кибербезопасность отражает не только реальные угрозы, но и коллективную цифровую тревожность. Мы строим многоуровневые системы защиты, но паникуем при запросе отпечатка пальца в мобильном банке. Впрочем, все меньше и меньше.

Корень проблемы, кажется, в разрыве между технологическим прогрессом и человеческой психологией. Цифровые решения предлагают эффективность, но их «галлюцинирование» не всегда дает адекватную картину происходящего. И в этом видится парадокс: чем активнее мы доверяем технологиям, используем их, тем быстрее они эволюционируют, а прогресс наступает, когда машины учатся не просто решать задачи, но предвосхищать человеческие сомнения.

↑
КОЛОНКА РЕДАКТОРА

ФИНАНСОВАЯ СТОРОНА ЦИФРОВОЙ ОБОРОНЫ

В УСЛОВИЯХ НАРАСТАЮЩЕЙ ГЕОПОЛИТИЧЕСКОЙ ТУРБУЛЕНТНОСТИ РАСХОДЫ КОМПАНИЙ НА ЗАЩИТУ ДАННЫХ ПРЕВРАЩАЮТСЯ В СТРАТЕГИЧЕСКИЙ ПРИОРИТЕТ. КАК ПОКАЗЫВАЮТ ИССЛЕДОВАНИЯ, ЗАТРАТЫ НА КИБЕРБЕЗОПАСНОСТЬ ВЫРОСЛИ НА 27%, А ДАЛЬНЕЙШИЙ ЕЖЕГОДНЫЙ ПРИРОСТ ПРОГНОЗИРУЕТСЯ В 14%. ОПРОШЕННЫЕ ЭКСПЕРТЫ И ПРЕДСТАВИТЕЛИ ВЕНДОРОВ ОТМЕЧАЮТ, ЧТО РОСТ ОБУСЛОВЛЕН УВЕЛИЧЕНИЕМ СЕБЕСТОИМОСТИ ПРОДУКТОВ, А ТАКЖЕ УЧАСТИВШИМИСЯ КИБЕРАТАКАМИ И УЖЕСТОЧИВШЕЙСЯ РЕГУЛЯТОРИКОЙ. ИВАН РАЗУМИХИН

По данным исследования АО «Квадрант Технологий» («СТРИМ Консалтинг»), российские корпоративные и частные пользователи в 2024 году потратили 339,1 млрд рублей на аппаратное и программное обеспечение информационной безопасности (ИБ), включая параллельный импорт, а также сопутствующие услуги. Это на 27% больше, чем в 2023 году. Эксперты агентства прогнозируют ежегодное увеличение в 14%, и в результате к 2029 году объем может составить 743 млрд рублей.

Аналитики в исследовании отмечают три ключевые причины роста объемов затрат: увеличение числа кибератак, импортозамещение (санкции США и ЕС, уход западных вендоров и запрет на экспорт технологий ускорили переход на отечественные решения), ужесточение регуляторики (введена персональная ответственность руководителей за обеспечение ИБ и предотвращение утечек данных). Спрос в основном формировали госорганы, финансовый сектор, телекоммуникационные компании и промпредприятия.

Если рассматривать сегментарно, то затраты на аппаратное обеспечение выросли на 28% в основном за счет спроса на межсетевые экраны, на ПО ИБ — 23% за счет спроса на решения защиты конечных точек, мониторинга событий и средств предотвращения утечек данных. Затраты на сервисы ИБ и сопутствующие IT-услуги (внедрение, интеграция, консалтинг, обучение) выросли на 29%.



ЕВГЕНИЙ ПАВЛЕНКО

ТРАНСФОРМАЦИЯ ПОДХОДОВ К ИБ ВЛЕЧЕТ ЗА СОБОЙ ВОЛНУ ИНВЕСТИЦИЙ В СОФТ, «ЖЕЛЕЗО» И СЕРВИСНУЮ ПОДДЕРЖКУ

В РАМКАХ ФОРМИРОВАНИЯ СЕБЕСТОИМОСТИ

Эксперты отмечают, что рост затрат вызван объективными причинами и связан с состоянием экономики и российского IT-рынка. Нельзя не отметить, что увеличивается себестоимость продуктов. Как поясняет менеджер по развитию NGFW UserGate Кирилл Прямов, она складывается из стоимости задействованных аппаратных компонентов, услуг подрядчиков, логистики, ФОТ, налогов, стоимости подвернутой инфраструктуры разработки и поддержи продукта, стоимости аренды офисов и т. д.

«Все эти составляющие становятся дороже. Официальная инфляция в 2024 году — 9,5%, рост номинальной зарплаты россиян — 21,9% (Росстат). Введен налог на высокий доход, что делает всех высококлассных дефицитных специалистов еще дороже. Отдельно стоит упомянуть высокую ключевую ставку. Из-за нее стоимость денег выросла, что осложнило развитие бизнеса: приходится больше рассчитывать на собственные средства, которых может не хватить, или закладывать стоимость кредитов в продукт. При этом бизнес должен достигать запланированных финансовых показателей: EBITDA, рентабельность, чистая прибыль и т. д. Все это способствует росту стоимости ПО и ПАК, так как затрагивает всех участников рынка»,— комментирует господин Прямов.

Также эксперт акцентирует, что российские вендоры столкнулись с требованием быстрого выхода на уровень зарубежных аналогов, десятилетиями оттачивавших свои решения при многомиллиардных бюджетах. Но для достижения мировых стандартов требуются значительные инвестиции. Компании активно наращивают штаты, разрабатывают собственные аппаратные платформы и смежные технологии, что неизбежно отражается на стоимости продуктов.

СТРАТЕГИЧЕСКАЯ НЕОБХОДИМОСТЬ С ОГОВОРКОЙ

Елена Скалозубова, ведущий архитектор ИБ, MONS (входит в ГК «КОРУС Консалтинг»), обращает внимание, что инвестиции в ИБ сегодня стали стратегической необходимостью. «Иногда затраты только на обеспечение ИБ доходят до 0,5% от выручки компании. Однако бизнесу важно быть устойчивыми — и с точки зрения непрерывности бизнес-процессов, и с точки зрения доверия клиентов. Поэтому многие вполне осознанно идут на дополнительные расходы»,— замечает она.

По ее словам, рост затрат на ИБ в 2024 году — вполне закономерный и оправданный тренд. После ухода иностранных вендоров компании оказались в ситуации, когда нужно было срочно перестраивать инфраструктуру, искать альтернативы, переобучать сотрудников, адаптировать рабочие процессы к новым реалиям. «Это полноценная трансформация всей ИБ-модели, что приводит к росту объема закупок ПО и оборудования, а также росту спроса на услуги по внедрению и поддержке»,— добавляет эксперт.

Параллельно выросло количество внешних атак, они стали сложнее. Поэтому компании начали обращать внимание на зрелые решения: мониторинг, SOC, Zero Trust, автоматизацию процессов реагирования.

«Киберпреступники активно используют автоматизацию и ИИ, что делает атаки более массовыми и изощренными,— добавляет Станислав Маслов, управляющий партнер ZeBrains.— Например, фишинг и атаки на цепочки поставок стали повседневной реальностью, а идеологически мотивированные хакерские кампании продолжают держать в напряжении крупные компании и госсектор. Вложения в NGFW, защиту конечных точек и SOC/MSS помогают компаниям быстрее реагировать на атаки, хотя человеческий фактор остается уязвимым».

Спикер прогнозирует, что рынок продолжит свой рост за счет облачных решений и локального ПО, но бизнесу стоит искать баланс между затратами и эффективностью, делая упор на обучение и автоматизацию. В перспективе число успешных атак может снизиться, но ущерб от них останется значительным.

ПЕРЕХОД К ОСОЗНАННОМУ УПРАВЛЕНИЮ

Фактически повышение затрат на программное и аппаратное обеспечение является отражением системных изменений в подходе бизнеса и государства к защите цифровых активов, резюмирует Николай Еритенко, научный сотрудник, специалист по информационной безопасности Университета ИТМО.

Так же, как и господин Маслов, он обращает внимание на осознанное управление рисками. «Закупка дорогостоящих решений не решает проблему, если не налажены процессы управления инцидентами, нет квалифицированных специалистов и не развита культура ИБ внутри организации. В некоторых случаях инвестиции совершаются исключительно ради соответствия требованиям регуляторов, без анализа эффективности и реального влияния на защищенность»,— говорит господин Еритенко.

Чтобы инвестиции приносили результат, по его словам, необходимо выстраивать систему оценки их эффективности, ориентируясь на ключевые метрики такие как, например, количество успешных атак, среднее время обнаружения и реагирования на инциденты, долю инцидентов, вызванных человеческим фактором, также совокупные потери от реализации угроз и другие. Такие подходы должны поддерживаться как внутренними стандартами компаний, так и внешним регулированием и отраслевыми практиками. ■