

ВАЛЕРИЙ ГРИБАНОВ,
РЕДАКТОР GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

ДВИГАТЕЛИ ПРОГРЕССА С ПОБОЧНЫМ ЭФФЕКТОМ

Цифровизация в России идет даже быстрее, чем планировали в федеральном правительстве пять лет назад. По плану, к настоящему времени уровень Digital IQ (уровень цифрового развития) экономики РФ должен был достигнуть 64,2%, а в реальности сейчас составляет 74,4%. Жизнь обгоняет мечту: Россия сегодня входит в топ-10 стран по диджитализации государственных услуг.

Но с таким уровнем вовлеченности цифровых сервисов во все сферы жизни неизбежно возникает и угроза кибератак. И чем более цифровизирована экономика — тем опаснее для нее становятся киберугрозы. С ростом уровня диджитализации пропорционально повышается и число хакерских атак. Преступления связаны как с мошенническими практиками, так и с попытками воздействовать на объекты критической информационной инфраструктуры страны.

В таких условиях расходы на защиту от хакерских атак растут внушительными темпами: в прошлом году рынок кибербезопасности России увеличился более чем на треть и достиг двухсот с половиной миллиардов рублей.

Казалось бы, необходимость тратить большие средства на противодействие цифровым преступлениям бьет по экономике и тормозит ее развитие — сотни миллиардов рублей пригодились бы и для вложения в производства, строительства инфраструктуры и прочих объектов.

Но если поглядеть с расстояния, выходит, что и киберпреступники, и киберзащитники двигают прогресс. Необходимость постоянно находиться в тонусе, быть в вечном поиске решений для создания надежного щита порождает неожиданные побочные продукты, которые могут оказаться полезными и в других сферах. Это как с «Виагрой»: изначально искали лекарство от ангины, но побочный эффект принес гораздо большие прибыли.

↑
КОЛОНКА РЕДАКТОРА

КИБЕРУГРОЗЫ ПРОДЛИЛИ ТРЕНД

В РОССИИ ЗА 2023 ГОД КОЛИЧЕСТВО АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ (КИИ) УВЕЛИЧИЛОСЬ НА 16% И ДОСТИГЛО 65 ТЫСЯЧ. ВЛАДИМИР КОЛОДЧУК

Такие данные приводит Национальный координационный центр по компьютерным инцидентам (НКЦКИ). По его информации, одна из самых частых причин уязвимостей — использование иностранного программного обеспечения без технической поддержки и обновлений. Эксперты указывают, что основные прошлогодние тренды сохранились в первой половине 2024-го. Среди них — увеличение количества крупных хакерских атак и рост скорости несанкционированного проникновения в IT-инфраструктуру; развитие российскими вендорами новых продуктов, у которых ранее не было особых перспектив из-за доступности качественных западных аналогов; сосредоточение отечественных решений по обеспечению информационной безопасности (ИБ) в сегменте облачных сервисов.



ЕВГЕНИЙ ПАВЛЕНКО

ОБЪЕМ ОТЕЧЕСТВЕННОГО РЫНКА КИБЕРБЕЗОПАСНОСТИ СОСТАВИЛ В 2023 ГОДУ ОКОЛО 252 МЛРД РУБЛЕЙ, ЧТО НА 35% БОЛЬШЕ 193 МЛРД В 2022-М

ПЕРЕХОД НА ОТЕЧЕСТВЕННОЕ

Полгода назад правительство РФ установило сроки перехода на отечественный софт для госкорпораций и компаний с госучастием. Согласно методическим рекомендациям Минцифры от 12 января, российские операционные системы, офисные пакеты, системы виртуализации и антивирусные программы обязательны к использованию с 1 января 2025 года, а системы управления базами данных (СУБД) — с 1 января 2026-го. Ранее это относилось только к объектам критической информационной инфраструктуры.

Исходя из указа президента Владимира Путина от 30 марта 2022 года, госорганам и компаниям с госучастием с 1 января 2025-го запрещается применять на объектах КИИ иностранное программное обеспечение (ПО). Переход же на доверенные программно-аппаратные комплексы (ПАК) должен завершиться к 1 января 2030 года. Кроме того, как следует из постановления кабмина от 14 ноября 2023 года № 1912, субъекты КИИ не смогут использовать на значимых объектах недоверенные ПАК, если те приобретались после 1 сентября.

К субъектам КИИ относятся юрлица, которым на праве собственности, аренды или ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления в сферах здравоохранения, науки, транспорта, в топливно-энергетическом комплексе, банковском секторе и других значимых отраслях экономики.

По данным Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий, доля отечественного ПО в закупках госкомпаний в 2022 году составляла 87,1% в количественном выражении и 54,2% в денежном. При этом 89% всех контрактов общей стоимостью 1,9 млрд рублей приходилось на российскую СУБД Postgres Pro. До ухода с отечественного IT-рынка зарубежных компаний, в 2021 году в сегменте СУБД лидером была американская корпорация Oracle с портфелем в 84% от общего числа контрактов (около 4 млрд рублей).

«У субъектов КИИ осталось совсем немного времени для перехода на отечественные решения, и пока складывается ощущение, что от истории с импортозамещением выиграют только те из вендоров ИБ, кто успел включить свои продукты в Реестр отечественного оборудования и ПО, а также получил сертификаты регуляторов. При этом самим вендорам не хватает времени на развитие продуктов, заказчики же требуют качества и цен, сопоставимых с теми, которые предлагали ушедшие с рынка западные компании»,— говорит генеральный директор облачного провайдера НУБЕС (Nubes) Василий Степаненко.

В целом объем отечественного рынка кибербезопасности составил в 2023 году около 252 млрд рублей, что на 35% больше 193 млрд в 2022-м. Заметим, что общий объем по продуктам и услугам ИБ в 2022 году вырос менее чем на 4% в сравнении с показателями 2021-го.

Господин Степаненко поясняет, что выручка самых крупных ИБ-вендоров России за 2023 год составила около 110 млрд рублей, игроков поменьше — приблизительно 50 млрд. Продление ежегодных лицензий — около 32 млрд рублей. При этом интеграционные услуги на рынке ИБ, по словам эксперта, оценить сложно, так как зачастую это сервисное обслуживание, оказываемое из года в год без дополнительных продаж. Поэтому с учетом интеграции объем рынка кибербезопасности в России может быть значительно больше, чем 250 млрд рублей, уточняет спикер.

ТРЕНДЫ И ПРОБЛЕМЫ

Эксперт по информационной безопасности компании Axenix Евгений Качуров выделяет на российском рынке ИБ два важных тренда последнего полугодия.

Первый — резкий взлет количества крупных хакерских атак и сопутствующий ему рост скорости, с которой злоумышленники проникают в IT-инфраструктуру жертвы. Тенденция, по словам эксперта, обусловлена появлением у хакеров новых навыков, увеличением финансирования (реализация масштабной атаки требует огромных средств), а также тем, что отечественные программные продукты, которыми заказчики замещают зарубежные, часто недостаточно исследованы на уязвимости.

Снизить риск крупным компаниям помогает тщательная проверка IT-контура, в том числе с помощью пентестов, усиление средств защиты и использование услуг SOC, отмечает господин Качуров.

Более революционным он называет второй сохраняющийся с прошлого года тренд — фейковые коммуникации с помощью искусственного интеллекта (ИИ). По словам представителя Axenix, злоумышленники так умело применяют ИИ-технологии, что, например, «могут подделать голосовое сообщение или видеозвонок, таким образом заставив жертву перевести им деньги или выдать персональные данные».

«Для защиты от этой угрозы пользователям мессенджеров и соцсетей нужно проявлять максимальную бдительность, стараться замечать признаки аномального поведения коллег и друзей»,— говорит эксперт.

В свою очередь, господин Степаненко относит к основным тенденциям ИБ в первом полугодии развитие российскими вендорами новых продуктов, лишенных ранее особых перспектив из-за доступности качественных западных аналогов. В этой группе решения класса NGFW, WAF, сканеры уязвимостей и прочее.

«На отечественном рынке тем временем продолжают осваиваться азиатские ИБ-вендоры. Их продуктов нет в квадрантах Gartner, и они пока не вкладывают огромные деньги в рекламу на территории РФ, но это крупнейшие вендоры ИБ в Китае и Индии, которым явно интересен рынок России»,— отмечает спикер.

Еще одним трендом 2023–2024 годов он считает сосредоточение отечественных вендоров на разработке и выпуске полноценных облачных версий своих продуктов. Долгое время SECaaS («ИБ как услуга») заключался лишь в помесячной оплате, а мультитенантность решений оставалась в бэклогах.

Из проблем на рынке ИБ эксперт выделяет бездумное использование решений с открытым исходным кодом.

«На рынке появляются IT-стартапы, которые пытаются решить задачи ИБ на базе opensource-разработок. Среди таких задач, например, защита контейнерных сред (kubernetes); безопасность новых почтовых систем; обеспечение бэкапа и так далее. При этом многие угрозы являются следствием бездумного использования opensource-решений. Теперь потенциальный нарушитель — это разработчик, выкладывающий в opensource свой код, но в какой-то момент начинающий встраивать в него зловредный функционал для пользователей из конкретных стран, для носителей языков и так далее»,— уточняет господин Степаненко.

По мнению ведущего инженера CorpSoft24 Михаила Сергеева, предотвращение кибератак требует комплексного подхода с использованием целого ряда инструментов и методов. Тем самым компания создаст надежную систему защиты от угроз и минимизирует риск утраты и компрометации данных.

К полезным инструментам специалист относит антивирусное ПО («Касперский», Dr Web); системы обнаружения и предотвращения вторжений (Snort, Suricata, Palo Alto Networks); межсетевые экраны (pfSense, Windows Firewall); многофакторную аутентификацию (Google Authenticator, Microsoft Authenticator, Яндекс Ключ) и сегментацию сети (разделение ее на сегменты для ограничения распространения угроз).

Господин Сергеев рекомендует не забывать и о резервном копировании и шифровании данных, а также об обучении сотрудников основам кибербезопасности. ■