01 июня 2025

Россия вошла в топ-10 по расходам на кибербезопасность

За последние два года Россия подвергается беспрецедентному уровню киберугроз и атак извне. Речь идет и о DDoS-атаках, и о краже персональных данных. Все это заставляет повышать расходы на кибербезопасность, которая по итогам 2024 г. выросла на 23% до 299 млрд руб. По этому показателю Россия вошла в первую десятку. Участники рынка продолжают развивать свои продуктовые линейки и надеются на поддержку государства, в частности, на прозрачный диалог по регулированию отрасли и упрощение процедур сертификации.

БЕСПРЕЦЕДЕНТНОЕ ДАВЛЕНИЕ

В 2024 г. Россия подверглась беспрецедентному уровню угроз по информационной безопасности (ИБ). Если в 2023 г. насчитывалось 14 прогосударственных APT-группировок (Advanced Persistent Threat — сложная продвинутая угроза), атакующих Россию и СНГ, то в 2024 г. их стало почти в 2 раза больше — 27. За 2024 г. было обнаружено 12 новых группировок: Unicorn, Dante, PhantomCore, ReaverBits, Sapphire Cat, Lazy Koala, Obstinate Mogwai, TaxOff и др.

Идеологически мотивированные группы хакеров — хактивисты — продолжают обмениваться опытом и прокачивают свои навыки. В 2024 г. не менее 17 таких группировок атаковали российские и белорусские организации, хотя еще годом ранее их было на четыре меньше. В своих атаках хактивисты используют различные методы — как DDoS-атаки (Distributed Denial of Service — распределенная атака типа «отказ в обслуживании»), так и шифрование и уничтожение данных, рассказывают в компании F6 (бывшей F.A.C.C.T).

При этом размываются привычные границы классификации преступных групп — хактивистов, прогосударственных APT-групп и киберпреступников. В частности, хактивисты-диверсанты все чаще атакуют государственные органы и компании России, используя в своих атаках программы-шифровальщики — излюбленное оружие финансово-мотивированных злоумышленников. А кибершпионы выкладывают украденные базы данных в публичный доступ в Telegram-каналах, чтобы нанести российским компаниям максимальный урон.

КРУПНЕЙШИЙ ХАКЕРСКИЕ АТАКИ И УТЕЧКИ

В октябре 2024 г. хакерской атаке со стороны группировки BO Team подверглась российская государственная автоматизированная система «Правосудие». Из-за этого в течение месяца были проблемы с доступом к сайтам арбитражных судов и судов общей юрисдикции.

В 2024 г. количество DDoS-атак в целом увеличилось минимум на 50% — как по количеству, так и по числу задействованных в ботнетах устройств. По данным компании F6, лидер по атакам — группировка IT Army of Ukraine, активизировавшаяся в феврале 2022 г. С весны 2024 г. аналитики фиксируют рост количества атак на региональных телеком-операторов. От киберпреступлений особенно страдают приграничные области — Курская и Белгородская.

В апреле 2025 г. DDoS-атаке подвергся интернет-провайдер Lovit, обслуживающий новостройки группы компаний ПИК. В результате атаки жильцы домов в течение недели оставались без услуг интернета и телевидения, аналогичная проблема была у арендаторов коммерческой недвижимости.

За 2024 г. специалисты F6 зафиксировали более 500 атак с использованием шифровальщиков в России — рост почти в 1,5 раза по сравнению с 2023 г. Суммы первоначального выкупа за расшифровку данных в 2024 г. для малого бизнеса составляли от 100 тыс. руб. до 5 млн руб., а для крупных и средних компаний, на которые приходится каждая пятая атака вымогателей, запросы преступников начинались с 5-10 млн руб.

Как сообщил руководитель подразделения киберразведки компании Bi.Zone Олег Скулкин, средний размер выкупа, который выплачивают российские компании киберпреступникам за расшифровку данных, вырос за последние 5 лет на порядок. Жертвами вымогателей чаще всего становились

производственные, строительные, фармацевтические и ИТ-компании, предприятия добывающей промышленности, военно-промышленного комплекса и организации из сферы услуг.

Утечки данных остаются одним из основных видов киберугроз. За 2024 г. было обнаружено 455 неопубликованных ранее баз данных компаний из России и Белоруссии (в 2023 г. их было 246). Количество строк в утечках превысило 457 млн.

В январе 2025 г. произошла утечка данных с корпоративных сайтов «Ростелекома». Параллельно хакеры заявили, что стали обладателями базы данных Федеральной службы государственной регистрации, кадастра и картографии РФ (Росреестр) размером 2 млрд строк, и выложили в открытый доступ 82 млн строк из них. С января по февраль 2025 г. Роскомнадзор зарегистрировал 19 случаев распространения в интернете баз данных, содержащих более 24 млн записей о россиянах.

Из наиболее крупных утечек последнего времени можно отметить утечки персональных данных клиентов «Бургер Кинга» и «Детского мира», о которых стало известно в конце 2024 г. В первом случае в сети были опубликованы номера телефонов почти 5 млн клиентов сети заведений быстрого питания, во втором случае было скомпрометировано около 1,2 млн клиентских аккаунтов. По данным InfoWatch, Россия в 2024 г. заняла второе место по количеству утечек — на российские организации пришлось 8,5% случаев компрометации данных, зарегистрированных в мире (первое место заняли США).

Дополнительные риски состоят в том, что, кроме публикации в открытом доступе, злоумышленники используют эти данные для последующего проведения каскадных атак на крупных игроков коммерческого и государственного секторов, отмечают эксперты.

РОССИЙСКИЙ РЫНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Все это вынуждает российских разработчиков ИБ-решений активнее включаться в работу, а заказчиков — тратить больше денег на защиту данных. По итогам 2024 г. объем российского рынка информационной безопасности достиг 299 млрд руб., увеличившись на 23% по сравнению с 244 млрд руб. в 2023 г. По расходам на информационную безопасность Россия вошла в первую десятку и находится на девятом месте среди других стран, следует из отчета группы компаний Б1. При этом в общем объеме ИТ-рынка его доля составила 14%.

Что касается глобального рынка информационной безопасности, его объем в 2024 г., по оценке Gartner, достиг $183,9 млрд. И в 2025 г. он вырастет, как ожидается, на 15,1% до $212 млрд. При этом доля мировых расходов на ИБ в общей доле ИТ-расходов по итогам прошлого года составила 3,6%.

Рынок информационной безопасности в России в прошлом году показал один из наиболее впечатляющих темпов роста в сравнении с другими ИТ-сегментами. Тем не менее, он оказался ниже ожидаемых 32%, обращает внимание руководитель департамента развития и архитектуры «Кросс Технолоджис» Евгений Балк. Первой причиной для этого является сформировавшийся тренд на секвестирование бюджета в блоках ИТ и цифровизации в целом, что связано с текущими макроэкономическими показателями и, в частности, значениями ключевой ставки Центрального банка России.

Вторая причина заключается в том, что за год на рынке не появилось достаточного числа вендорских продуктов в том качестве, которого от них ожидают компании, проводящие импортозамещение. «Соответственно, ряд планов на новые внедрения, равно как и бюджеты, заложенные под них, были сокращены либо перенесены на более поздний период по мере развития необходимых решений», — говорит Евгений Балк.

По данным Б1, российский рынок информационной безопасности на 70% состоит из продуктов и на 30% — из услуг. Крупнейшие подсегменты среди продуктов ИБ по итогам 2024 г. — сетевая и облачная безопасность (42% от всех продуктов), решения анализа, контроля и реагирования на угрозы ИБ (17% от продуктов) и защита конечных точек (17% от продуктов). Сегмент услуг ИТ представлен подсегментами проектных услугу ИБ (63%) и услуг аутсорсинга и управляемых услуг ИБ (37%).

Для ИБ-продуктов характерен тренд на формирование платформенных решений, а также растущие требования к зрелости продукта и объему инвестиций в разработку и маркетинг. Ключевыми сегментами рынка являются сетевая и облачная безопасность, защита конечных точек, анализ угроз и реагирование.

На рынке ИБ-услуг отмечается рост сегмента управляемых услуг информационной безопасности (Managed Security Services — MSS), что связано с расширением поля атак на организации менее крупного размера, нехваткой и дороговизной ИБ-компетенций, а также необходимостью повышения скорости реакции на инциденты, оптимизации операционных и капитальных затрат, обеспечения гарантий защиты, получения гибкости в условиях оплаты. Сегментами данного рынка являются проектные услуги, MSS и аутсорсинг.

На рынке разработчиков ИБ-продуктов лидерами являются «Лаборатория Касперского», Positive Technologies, «Инфотекс» и «Код безопасности». На рынке поставщиков ИБ-продуктов лидеры — «Солар» (входит в «Ростелеком»), «Инфосистемы Джет», Innostage, Softline и Angara Security. На рынке ИБ-услуг крупнейшими компаниями являются «Солар», «Инфосистемы Джет», Innostage и Angara Security. На рынке аутсорсинга ИБ и MSS — «Солар», «Инфосистемы Джет» и Innostage. Всего на рынке информационной безопасности в России работают более 300 местных компаний, в том числе 190 разработчиков.

ПРИЧИНЫ ДЛЯ ДАЛЬНЕЙШЕГО РОСТА

В 2025 г. на рынке информационной безопасности в России начнут меняться критерии выбора решений, указывает генеральный директор разработчика систем аутентификации Roox Алексей Хмельницкий. «Вступая в фазу экономии бюджетов, компании теперь все чаще ищут системы, объединяющие управление доступом, учетными данными и авторизацией в единый продукт, способный работать с разнородными сценариями — от сотрудников до клиентов и партнеров, — говорит он. — Параллельно продолжается процесс импортозамещения: организации отказываются от зарубежных решений в пользу российских альтернатив, причем даже ранее популярные open source-варианты вроде Keycloak теряют позиции».

По оценке IBS, в 2025 г. объем рынка информационной безопасности в России составит 345-373 млрд руб. При этом эксперты компании считают эту оценку сдержанной и подверженной влиянию высокой ключевой ставки и нехваткой зрелых отечественных решений для удовлетворения всего спроса по импортозамещению.

В «Лаборатории Касперского» прогнозируют рост российского рынка ИБ в 2025 г. на уровне более 20%, объясняя это растущим числом угроз и повышением понимания среди различных сегментов бизнеса необходимости защиты. «Даже небольшим организациям придется уделять более

пристальное внимание безопасности своей компании, чтобы, не стать источником угрозы в рамках атак на цепочки поставок. Для этого требуется комплексная защита инфраструктуры. Кроме того, нехватка ИБ-специалистов может способствовать востребованности сервисов управляемой защиты», — отметил руководитель отдела по работе с клиентами малого и среднего бизнеса «Лаборатории Касперского» Алексей Киселев.

По оценке Б1, среднегодовой темп роста российского рынка информационной безопасности в период с 2024 по 2030 гг. составит 15%. В то же время остается высокой доля иностранных ИБ-продуктов — 10-20% для отдельных классов программного обеспечения и до 40-50% в сегменте сетевой безопасности. Важными факторами в дальнейшем росте рынка станут увеличение числа киберпреступлений, расширение круга атакуемых отраслей и компаний, в том числе атаки через поставщиков. А также усложнение механик атак, развитие искусственного интеллекта, снижающего порог входа для киберпреступников, развитие облачных технологий, увеличение уровня ответственности за инциденты, регуляторные требования и усилия государства по развитию национальной ИБ-инфраструктуры.

Как отмечает Евгений Балк из «Кросс Технолоджис», существует несколько причин для роста рынка ИБ. Первая причина — это импортозамещение: заказчики перестали ждать возвращения иностранных вендоров, плюс усложняется ежедневное использование ряда решений: приходится устанавливать обновления с использованием обходных и не всегда безопасных и надежных путей, количество которых постоянно сокращается.

«Организации понимают, что пересидеть уже не получится и нужно начинать переходить на отечественные решения, не подверженные рискам неблагоприятной внешней конъюнктуры, — говорит Балк. — У многих уже даже заканчиваются переходные периоды тестирования импортозамещенных компонентов, и организации переходят к полномасштабному внедрению».

Второй причиной является возросшее число кибератак. Российские предприятия стали своего рода полигоном для испытания различных инструментов хакеров и отработки навыков ведения кибервойны. Это заставило отечественных разработчиков обращать внимание на практическую кибербезопасность вместо того, чтобы слепо стремиться к соответствию регуляторным требованиям. В частности, все большее распространение получают методы безопасной разработки программного обеспечения (DevSecOps, SSDLC и т. д)., продолжает эксперт.

Третья причина — введение оборотных штрафов за утечки персональных данных. Соответствующий закон был принят в конце 2024 г. и вызвал бурное обсуждение. За повторное нарушение закона «О персональных данных» на юридические лица может быть наложен штраф в размере 1-3% от выручки, но не менее 20 млн руб. и не более 500 млн руб. Также вводится уголовная ответственность за незаконное распространение персональных данных — до 10 лет.

ТЕХНОЛОГИЧЕСКИЕ ТРЕНДЫ

Количество кибератак будет возрастать, что вызовет рост спроса на интеллектуальные системы детектирования угроз, которые используют алгоритмы искусственного интеллекта и машинного обучения для обнаружения необычного поведения пользователей или отклонений в работе системы. Второй важный тренд — эшелонированная защита, подразумевающая использование нескольких дополняющих друг друга ИБ-решений, и, главное, глубокую интеграцию между эшелонами защиты, рассказал директор по продуктам разработчика решений для защиты от кибератак Servicepipe Михаил Хлебунов.

В качестве первого и второго эшелонов могут использоваться решения для защиты от сетевых DDoS-атак и атак на уровне приложений. Третьим эшелоном может стать защита от ботов, которая обезопасит веб-сайты и API (программные интерфейсы) мобильных приложений от парсеров, сканеров уязвимостей, массовых регистраций и фейковых заявок. Четвертым эшелоном будет межсетевой экран уровня веб-приложений, который защищает от эксплуатации уязвимостей веб-приложений и API. «Количество эшелонов может варьироваться в зависимости от степени критичности сервиса и особенностей его архитектуры», — говорит эксперт.

Кроме того, в 2024 г. на рынке стал развиваться новый класс решений — ITDR (Identity Threat Detection and Response — выявление угроз учетным данным и

реагирование на них). Он объединяет защиту идентификационных данных с предиктивной аналитикой, помогая выявлять и устранять угрозы, связанные с компрометацией учетных записей, рассказывает генеральный директор компании «Индид» Алексей Баранов.

ОЖИДАНИЯ БИЗНЕСА ОТ ГОСУДАРСТВА

В сфере информационной безопасности бизнес ждет от государства четкой нормативно-правовой базы, которая позволила бы обеспечить адекватную защиту информации и киберпространства, учитывая современные угрозы и технологические изменения; стандартизацию, подразумевающую введение единых стандартов кибербезопасности для всех участников рынка; содействия инновациями, создающее стимулы для внедрения передовых технологий и решений в области киберзащиты, а также мониторинг и надзор за соблюдением действующего законодательства, делится руководитель департамента аудита компании «Кросс Технолоджис» Антон Исупов.

Индустрии не хватает обратной связи с регулятором. Отсутствует диалог с отраслью, и это ведет к проблемам, отмечает руководитель группы защиты инфраструктуры ИТ-решений компании «Газинформсервис» Сергей Полунин. «От разработчиков решений в сфере ИБ есть запрос на упрощение дорогостоящих и длительных процедур сертификации решений. Кроме этого, зачастую требования Федеральной службы по техническому и экспортному контролю РФ, Федеральной службы безопасности РФ, Министерства

цифрового развития связи и массовых коммуникаций РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ и Центрального банка РФ противоречат друг другу или дублируются. Возникает идея «единого окна», где можно узнать единые требования к безопасности в том или ином кейсе», — делится Полунин.

С необходимостью упрощения и ускорения процедур сертификации согласна Елена Скалозубова, ведущий архитектор по информационной безопасности компании MONS (входит в группу «Корус Консалтинг»). К действенным мерам поддержки компаний, которые смогли бы помочь им адаптироваться к быстро меняющимися рыночным условиям, она также относит снижение бюрократических барьеров, развитие системы обучения и повышения квалификации, урегулирование вопросов со страхованием бизнеса от рисков, связанных с использованием данных.

Ключевым вызовом для отрасли остается дефицит квалифицированных кадров, добавляет Алексей Баранов из «Индид». В 2027 г. общая потребность рынка в ИБ-специалистах может увеличиться до 235-261 тыс. человек. «Ситуация усугубляется ростом кибератак на российскую инфраструктуру, что требует не просто увеличения числа сотрудников, но и их глубокой экспертизы в области кибербезопасности, — говорит он. — Сократить разрыв между потребностями рынка и наличием профессиональных кадров позволят только совместные усилия государства, образовательных учреждений и бизнеса».