Review **Технопром**

Информация под защитой отечества

С февраля 2022 года на российские компании обрушилась волна кибератак. При этом каких-то принципиально новых инструментов у злоумышленников не появилось. Преступники по-прежнему используют DDoS-атаки, APT, социальную инженерию, программы-вымогатели, фишинг, скам и телефонное мошенничество. Изменилось лишь количество попыток взлома — их по итогам первого полугодия 2022-го стало в 15 раз больше, чем в аналогичный период прошлого года. Самыми атакуемыми отраслями стали финансовый сектор, ритейл и логистика. Ситуацию осложнил уход из России крупнейших международных компаний — разработчиков систем защиты информации. Однако, по мнению экспертов, это сделает российскую сферу кибербезопасности одной из наиболее привлекательных с точки зрения инвестиций отраслей.

ВЛАД НЕКРАСОВ

Сложившаяся ситуация с уходом иностранных компаний сферы кибербезопасности для российских вендоров выгодна, так как спрос на эти продукты уверенно растет

—Конъюнктура —

В первом полугодии 2022-го по СФО зарегистрировано 29,8 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, рассказали в Генпрокуратуре РФ по Сибирскому федеральному округу (СФО). Это на 15% меньше, чем в прошлом году (за шесть месяцев 2021 года — 35,4 тыс.), из них совершенных с использованием расчетных (пластиковых) карт — 9,5 тыс. (–34,1% в сравнении с годом ранее), компьютерной техники — 1,2 тыс. (–36,6%), интернета — 22 тыс. (–4,9%), средств мобильной связи — 12,4 тыс. (–23,5%).

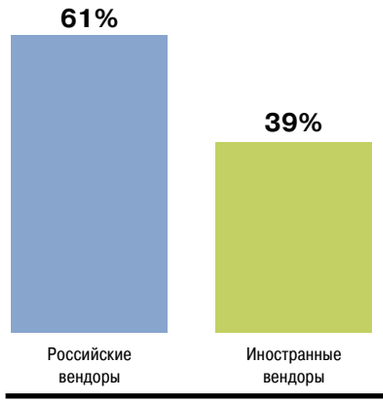
Количество предварительно расследованных преступлений за шесть месяцев 2022 года составило 8,2 тыс., оставшихся нераскрытыми — 21,1 тыс. «Доля преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, от общего количества преступлений составляет 21,4%, по итогам 2021-го — 24,3%»,— говорит начальник управления Генпрокуратуры РФ по Сибирскому федеральному округу Юрий Русанов.

В то же время общее количество кибератак в России по итогам первого полугодия 2022-го в сравнении с тем же периодом прошлого года выросло в 15 раз, сообщила компания StormWall. Самыми атакуемыми отраслями стали финансовый сектор (32% от общего числа атак), ритейл (14%), логистическая сфера (10%), страховая отрасль (8%) и государственный сектор (18%). Также DDoS-атакам подверглись образовательный сектор (7%), сфера развлечений (5%), туристическая индустрия (4%) и другие отрасли (2%).

Число DDoS-атак на государственный сектор в этот период увеличилось в 17 раз, на логистику — в 16 раз, в страховой отрасли число атак выросло в 15 раз, в финансовом секторе — в 12,8 раз, в ритейле — в 11 раз. Увеличилась длительность атак: в начале 2022 года их период составлял в среднем 7 часов, в 2021-м — около 3 часов, сейчас некоторые из них длятся неделями.

ДОЛЯ РОССИЙСКИХ И ЗАРУБЕЖНЫХ ВЕНДОРОВ СРЕДСТВ ЗАЩИТЫ ПО РЕЗУЛЬТАТАМ 2021 ГОДА

ИСТОЧНИК: ЦСР



21 июля 2022 года «Лаборатория Касперского» сообщила о самой продолжительной DDoS-атаке в России. Она началась в мае 2022 года и длилась почти 29 дней.

Подсчеты профильных аналитических компаний противоречат официальным данным правоохранителей из-за нежелания некоторых компаний обращаться к ним с проблемами взлома, считают эксперты. «Так, например, потерпевшие не знают процедур обращения по факту совершения кибератак или полагают, что атакующие находятся вне юрисдикции российского законодательства. Помимо этого, компании могут не обращаться в органы из желания скрыть выявленные атаки и утечки данных, а также из-за отсутствия выстроенных механизмов выявления и регистрации кибератак. Еще один немаловажный фактор — отсутствие обученных кадров, способных провести внутреннее расследование для выявления причин инцидента»,— считает заместитель директора департамента консалтинга группы компаний Innostage Данияр Исхаков.

Резкий всплеск попыток взлома эксперты объясняют нестабильной политической ситуацией в мире. «Особенность последнего времени — в атаках участвует все больше так называемых хактивистов, чья главная цель — не финансовая нажива, как было раньше, а нанесение максимального ущерба организациям и их процессам. Особую опасность это представляет для промышленных предприятий и объектов критической информационной инфраструктуры (КИИ), нарушение работы которых может повлечь серьезные последствия, в том числе для населения. Тем не менее организации, не связанные с критической инфраструктурой, тоже подвержены риску атак»,— говорит руководитель российского исследовательского центра «Лаборатории Касперского» Мария Наместникова.

Наиболее защищенными при этом оказались госструктуры и финансовый сектор, отмечает директор по развитию бизнеса центра противодействия кибератакам Solar JSOC компании «РТК-Солар» Алексей Павлов. «Наиболее уязвимыми отраслями стали здравоохранение и образование»,— считает эксперт.

Хакер по телефону

Никаких новых механизмов взлома программных продуктов в 2022 году придумано не было, изменилось лишь количество попыток взлома, подчеркивает сооснователь и директор сервиса облачной автоматизации бизнеса Altapp Филипп Щиров. «В основном это были DDoS-атаки на правительственные и частные сервисы на территории России и дефейс (смена одной веб-страницы на другую) сайтов госорганов и российских компаний»,— комментирует он.

Для рядовых пользователей по-прежнему актуальны традиционные угрозы: фишинг, скам, телефонное мошенничество, которые тоже показывают рост. С января по июнь жители Новосибирской области направили в Банк России 120 жалоб на кибермошенничество. Это в 1,5 раза больше, чем за аналогичный период прошлого года.

«Социальная инженерия остается одним из самых опасных методов взлома, используемых киберпреступниками, в основном потому, что она основана на человеческих ошибках, а не на технических уязвимостях. Это делает эти атаки еще более опасными — гораздо проще обмануть человека, чем взломать систему безопасности»,— считает эксперт в области информационной безопасности компании OCS Distribution Светлана Корягина.

В 2022 году нарушения безопасности со стороны третьих лиц стали еще более серьезной угрозой, поскольку компании все чаще обращаются к независимым подрядчикам для завершения работы, которую раньше выполняли штатные сотрудники, отмечают аналитики.

«Вторая по значимости угроза — программы-вымогатели. Они были заметной угрозой в течение последних нескольких лет и, похоже, в ближайшее время никуда не денутся. В 2021 году средняя стоимость атаки программ-вымогателей составила $4,62 млн. Во многих случаях, когда происходили взломы систем защиты на малых и средних предприятиях, компании были вынуждены закрыться навсегда, поскольку они не могли оправиться от такой серьезной атаки»,— рассказывает Светлана Корягина.

Атаки программ-вымогателей уникальны тем, что они работают довольно медленно. Это означает, что как только хакеры получают доступ к системе, они работают в течение нескольких недель, а иногда и месяцев, чтобы зашифровать конфиденциальную информацию, прежде чем требовать выкуп, объясняет эксперт.

Рынок готовит «свое»

Проблемы с информационной защитой у российских пользователей в 2022 году возникли в том числе из-за ухода крупнейших международных компаний — разработчиков систем защиты информации. О прекращении деятельности в России заявили Cisco, IBM, Imperva, Fortinet, Microsoft, Norton, Avast и др. На них приходилось 39% общего объема рынка по состоянию на 2021 год, по итогам 2022 года их доля на рынке сократится до 12%. «Системные интеграторы, клиенты и заказчики сейчас в срочном порядке ищут замену данным производителям»,— комментирует госпожа Корягина.

Сложившаяся ситуация для российских вендоров выгодна, так как спрос на решения, обеспечивающие кибербезопасность, уверенно растет. Он обусловлен изменившейся геополитической обстановкой и мерами, предпринимаемыми правительством (регуляторами) и бизнесом для укрепления кибербезопасности, считают аналитики Центра стратегических разработок (ЦСР).

Российский рынок информационной безопасности уже несколько лет занимается импортозамещением. С уходом зарубежных вендоров наполненность некоторых сегментов снизится, что позволит другим игрокам занять свободное пространство, а общий фон позволяет предсказать, что показатели роста рынка информационной безопасности могут даже превысить ожидания аналитиков, считает Светлана Корягина.

«Это сделает российскую кибербезопасность одной из наиболее привлекательных с точки зрения инвестиций отраслей. В ближайшем будущем можно ожидать появления новых игроков, слияний и поглощений, расширения бизнеса и выхода ИБ-разработчиков на рынок капитала»,— добавляет она.

По оценкам аналитиков Центра стратегических разработок (ЦСР), в ближайшие пять лет российский рынок кибербезопасности вырастет в 2,5 раза — с 185,9 до 469 млрд руб. При этом начиная с 2023 года практически весь бюджет заказчиков на средства защиты информации 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.

Также на рынок кибербезопасности значительное влияние окажет активная позиция регуляторов и органов власти в части необходимости импортозамещения (обеспечения технологической независимости) технических решений, связанных с обеспечением безопасного функционирования объектов критической информационной инфраструктуры, считают аналитики.

С 31 марта 2022 года указом президента в России запрещена закупка зарубежного программного обеспечения для использования на значимых объектах КИИ, а с 1 января 2025 года запрещается использование зарубежного программного обеспечения на таких объектах.

Доля рынка зарубежных вендоров продолжит сокращаться, считают эксперты. «Ожидается что доля зарубежных вендоров на отечественном рынке стабилизируется на уровне 5%, однако может вырасти до 8% в 2026 году. Далее доминантное положение отечественных вендоров может изменяться в связи с вероятным серым импортом»,— говорится в исследовании ЦСР.

Расходы бизнеса на информационную защиту в то же время начали расти, отмечают представители отрасли. «Учитывая, что количество кибератак и их интенсивность увеличились в десятки раз, затраты бизнеса на кибербезопасность должны быть существенными — предположительно „в несколько раз“. Полагаю, что более точные цифры мы получим, когда о своей прибыли отчитаются компании, которые специализируются в области информационной безопасности. Большинство коммерческих организаций, которые не могут защититься от кибератак самостоятельно, обратились именно к таким организациям»,— говорит Филипп Щиров.

18% из 500 руководителей, опрошенных KPMG в 2021 году, заявили, что риск кибербезопасности будет самой большой угрозой для роста их организаций в ближайшие три года. Это почти в два раза больше, чем 10% руководителей, которые сказали то же самое в середине 2020 года,— значительное изменение отношения всего за шесть месяцев.

«Компании начали более внимательно относиться к собственной кибербезопасности. Они все чаще занимаются инвентаризацией ИТ-периметров и стараются повысить защиту за счет внедрения новых технологий и процессов. Все большим спросом пользуются решения для защищенного удаленного доступа. Также популярнее становится услуга киберразведки. Она предполагает как мониторинг упоминания компании в даркнете и профильных хакерских телеграм-каналах (например, если кто-то хочет заказать атаку на организацию), так и получение информации об известных уязвимостях периметра (например, если уязвимые серверы компании опубликованы в открытом доступе)»,— рассказывает Алексей Павлов.

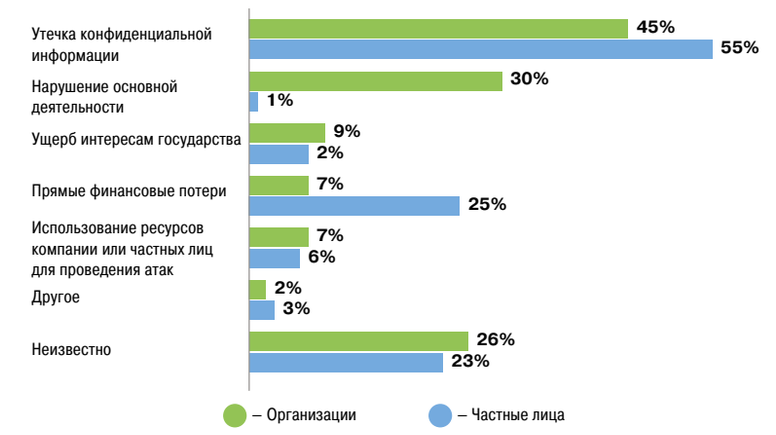
По итогам года расходы на облачную безопасность вырастут на 41,2%, в то время как расходы на безопасность данных — на 17,5%, на защиту инфраструктуры — на 16,8%, на управление доступом к идентификационным данным — на 15,6%, на комплексное управление рисками — на 12,6% и на услуги безопасности — на 11,4%, полагает Светлана Корягина.

Проблема кибербезопасности в ближайшие годы будет наиболее актуальной как для рядовых пользователей, так и для компаний. Квалификация киберпреступников при этом продолжит расти. Последствия атак будут напрямую зависеть от уровня подготовки специалистов и развития систем ИИ в России.

Лолита Белова

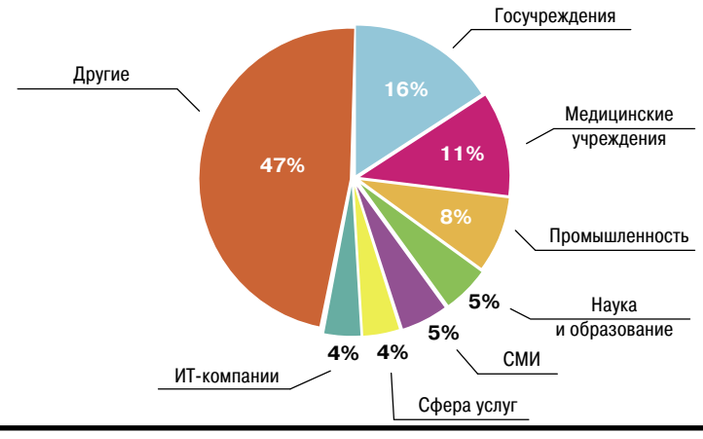
ПОСЛЕДСТВИЯ КИБЕРАТАК (ДОЛЯ) ЗА I КВАРТАЛ 2022 ГОДА

ИСТОЧНИК: POSITIVE TECHNOLOGIES



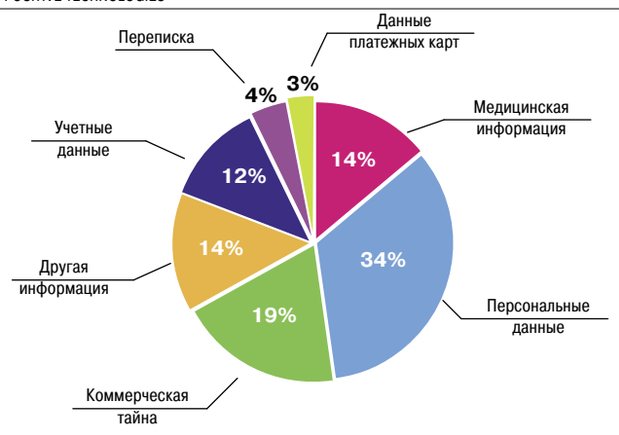
ОРГАНИЗАЦИИ, СТАВШИЕ «ЖЕРТВАМИ» КИБЕРАТАК

ИСТОЧНИК: POSITIVE TECHNOLOGIES



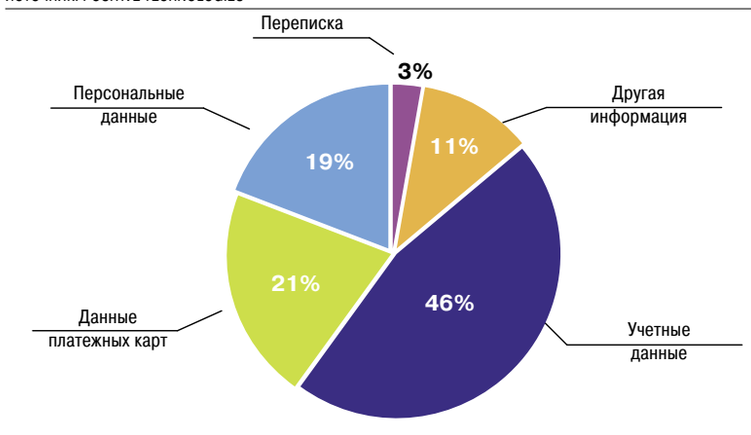
ТИПЫ УКРАДЕННЫХ ДАННЫХ (В АТАКАХ НА ОРГАНИЗАЦИИ) ЗА I КВАРТАЛ 2022 ГОДА

ИСТОЧНИК: POSITIVE TECHNOLOGIES



ТИПЫ УКРАДЕННЫХ ДАННЫХ (В АТАКАХ НА ЧАСТНЫХ ЛИЦ) ЗА I КВАРТАЛ 2022 ГОДА

ИСТОЧНИК: POSITIVE TECHNOLOGIES



СПОСОБЫ РАСПРОСТРАНЕНИЯ ВРЕДОНОСНОГО ПО В АТАКАХ НА ОРГАНИЗАЦИИ ЗА I КВАРТАЛ 2022 ГОДА

ИСТОЧНИК: POSITIVE TECHNOLOGIES