ВЫРАБОТАТЬ КОЛЛЕКТИВНЫЙ КИБЕРИММУНИТЕТ

МИРОВОЙ УЩЕРБ ОТ КИБЕРПРЕСТУПЛЕНИЙ ОЦЕНИВАЕТСЯ В $200 МЛРД — $1 ТРЛН В ГОД, И ЭТА ЦИФРА ПРОДОЛЖАЕТ РАСТИ. В РОССИИ, ПО ОЦЕНКАМ МИНЦИФРЫ, ПРЯМОЙ УЩЕРБ ОТ ДЕЙСТВИЙ КИБЕРПРЕСТУПНИКОВ В 2024 ГОДУ СОСТАВИЛ 160 МЛРД РУБЛЕЙ. В ЗОНЕ ПОВЫШЕННОГО РИСКА — ГОССТРУКТУРЫ, ФИНАНСОВАЯ СФЕРА, ПРОМЫШЛЕННОСТЬ И ЭНЕРГЕТИКА, ГДЕ АТАКИ МОГУТ ПРИВЕСТИ К СЕРЬЕЗНЫМ ЭКОНОМИЧЕСКИМ И ОПЕРАЦИОННЫМ ПОТЕРЯМ. ПО МНЕНИЮ ЭКСПЕРТОВ, ДЛЯ ЗАЩИТЫ БИЗНЕСА НЕОБХОДИМО ПЕРЕХОДИТЬ ОТ РЕАГИРОВАНИЯ К ПРОАКТИВНОЙ СТРАТЕГИИ. ИНВЕСТИЦИИ В КИБЕРУСТОЙЧИВОСТЬ СЕГОДНЯ СТАНОВЯТСЯ НЕ ПРОСТО НЕОБХОДИМОСТЬЮ, А КРИТИЧЕСКИМ ФАКТОРОМ КОНКУРЕНТОСПОСОБНОСТИ. ИРИНА КОВАЛЕВА

Эпоха первых масштабных кибератак началась с вируса LoveLetter, который в 2000 году причинил ущерб на $10 млрд. «Этот инцидент продемонстрировал, как быстро злоумышленники адаптируются к новым технологиям, особенно с появлением интернет-платежей»,— сказал CEO «Лаборатории Касперского» Евгений Касперский, выступая на прошедшей в апреле этого года конференции Kaspersky Future. Кроме того, знаковым моментом стала история с шифровальщиком GPCode в 2006 году. «Первоначально специалистам удалось взломать его криптографическую защиту, но авторы вируса быстро выпустили обновленную версию с 660-битным ключом. Однако и эта защита оказалась уязвимой из-за ошибки в алгоритме генерации ключей»,— уточнил господин Касперский.

Следующее десятилетие ознаменовалось появлением высокопрофессиональных киберпреступных группировок. Так, группа Carbanak установила новый стандарт, похитив около миллиарда долларов через атаки на банковские системы. Особенностью их методов было удаленное управление банкоматами без физического доступа. «Отдельной главой в истории кибербезопасности стала атака Stuxnet на иранские ядерные объекты в 2010 году. Этот сложный вредонос скрытно изменял работу центрифуг, одновременно фальсифицируя данные телеметрии, что привело к их физическому разрушению»,— отметил Евгений Касперский.

По словам эксперта, в настоящее время ежегодный ущерб от киберпреступлений оценивается в $200 млрд — $1 трлн в год, причем эта цифра продолжает расти. В России, в свою очередь, по оценкам Минцифры, прямой ущерб от киберпреступлений в 2024 году достиг 160 млрд рублей, а их количество выросло почти на треть по сравнению с 2023 годом.



ЕВГЕНИЙ ПАВЛЕНКО

ЭКСПЕРТЫ ОТМЕЧАЮТ, ЧТО В НАСТОЯЩЕЕ ВРЕМЯ НАБЛЮДАЕТСЯ УСИЛЕНИЕ УГРОЗ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИИ

НОВЫЙ УРОВЕНЬ УГРОЗ

Собеседники Guide отмечают, что рынок информационной безопасности будет продолжать адаптироваться под задачи, связанные с противодействием усложняющимся киберугрозам. Среди наиболее явных — рост атак на критически важную инфраструктуру, в том числе с применением APT-группировок, поддерживаемых различными государствами. По словам Елены Скалозубовой, ведущего архитектора по информационной безопасности MONS (ГК «КОРУС Консалтинг»), геополитическая нестабильность остается значимым фактором риска. «Это уже не просто инциденты информационной безопасности, а новый вид оружия, и в развитие инструментов для кибератак вкладываются значительные ресурсы»,— утверждает Евгений Дорофеев, управляющий директор по направлениям «ИБ и Доверенные цифровые решения» АО «Росатом Автоматизированные системы управления». В 2025 году он прогнозирует рост волны кибератак на объекты КИИ, особенно в крупной промышленности и энергетике. «При этом ахиллесовой пятой в этих отраслях остается проблема импортозамещения: импортное ПО несет в себе риски недекларированных возможностей, присутствия заложенного скрытого вредоносного функционала»,— считает он.

УВЕЛИЧЕНИЕ ЧИСЛА КИБЕРАТАК, ВКЛЮЧАЯ DDOS И ЦЕЛЕВЫЕ ВЗЛОМЫ, ЗАСТАВЛЯЕТ КОМПАНИИ ИСКАТЬ БОЛЕЕ НАДЕЖНЫЕ СПОСОБЫ ЗАЩИТЫ ДАННЫХ И ПЕРЕСМАТРИВАТЬ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

Госпожа Скалозубова подтверждает, что в 2024–2025 годах чаще других подвергались атакам государственные органы и объекты КИИ (в связи с геополитикой и высокой ценностью данных), финансовый сектор (из-за прямого доступа к денежным ресурсам и системам переводов), промышленность и энергетика (в этих отраслях распространены уязвимые SCADA-системы, а также слабая сегментация и высокая стоимость простоев). «Кроме того, часто атаковались организации здравоохранения (дефицит специалистов по ИБ, наличие персональных и медицинских данных, уязвимое ПО). Слабые стороны этих отраслей — недостаточное обновление систем, человеческий фактор, старое ПО и низкий уровень кибергигиены»,— указывает она.

Также в настоящее время наблюдается усиление угроз, связанных с использованием ИИ, вследствие чего возникает необходимость защищать сами ИИ-модели от потенциальных атак. «Кроме того, ИИ может применяться для анализа угроз и управления инцидентами безопасности, но с другой стороны — этими же технологиями могут пользоваться и злоумышленники»,— отмечает Антон Ведерников, руководитель направления продуктовой безопасности Selectel.

Среди наиболее распространенных методов атак 2024–2025 годов эксперты выделяют фишинг и социальную инженерию (особенно это касается мессенджеров и голосовых дипфейков), взлом VPN, RDP и других удаленных доступов (зачастую из-за слабых паролей или утечек), эксплуатацию уязвимостей в ПО — Log4Shell, ProxyShell, уязвимости в Outlook, Microsoft Exchange, Fortinet, атаки на цепочку поставок (через подрядчиков, облачные сервисы или библиотеки ПО), а также шифровальщики (Ransomware) — особенно в атакующих кампаниях на промышленные и муниципальные сети. При этом наиболее опасные уязвимости последних лет — это нулевые дни в VPN-решениях (например, FortiGate, Ivanti), уязвимости в веб-интерфейсах (CVE–2023–34362 в MOVEit), ошибки конфигурации облаков, а также уязвимости в Outlook/Exchange, позволяющие выполнение кода без взаимодействия с пользователем.

«Степень проработанности отдельных атак показывает высокий уровень квалификации, технических возможностей и слаженности организации хакерской группировки. Удаленный доступ к системам управления объектами КИИ, террористические кибератаки на производственные цепочки — все это обратная сторона динамичной эволюции цифрового мира»,— подчеркивает господин Дорофеев.

СТРАТЕГИИ КИБЕРЗАЩИТЫ

Увеличение числа кибератак, включая DDoS и целевые взломы, заставляет компании искать более надежные способы защиты данных и пересматривать подходы к обеспечению безопасности. По мнению Елены Скалозубовой, в условиях стремительных изменений в ИТ-инфраструктуре предприятиям необходимо переходить от «реакционной» модели защиты (когда компания реагирует на уже случившуюся атаку) к проактивной. «На первый план выходят подходы security by design (проектирование киберсистем, в которых меры безопасности интегрированы в архитектуру и программный код и являются его частью), включая безопасную разработку, а также обеспечение „наблюдаемости“ (observability) инфраструктуры для служб эксплуатации и безопасности для своевременного обнаружения атак»,— объясняет господин Ведерников.

Среди других методов госпожа Скалозубова выделяет подход Zero Trust (архитектура, не доверяющая по умолчанию ни одному пользователю или устройству), Threat Intelligence (постоянный анализ данных об угрозах, мониторинг даркнета, выявление признаков атак на ранних стадиях), сегментацию сети и контроль доступа для локализации инцидентов и ограничения распространения вредоносного кода, а также киберучения и симуляции атак (Red Teaming) для проверки готовность персонала и систем к вторжению. «Также ключевое значение приобретают инвестиции в устойчивость ИТ-инфраструктуры (резервное копирование, план реагирования, командные процедуры), поскольку важно не только предотвращение атак, но и минимизация их последствий»,— говорит она.

При этом не менее важным является обучение сотрудников — повышение их осведомленности о фишинге и социальных инженерных атаках помогает снизить риск успешных проникновений, заключает Артур Кондаков, руководитель направления разработки и внедрения систем ИБ в пакет приложений «МойОфис». ■