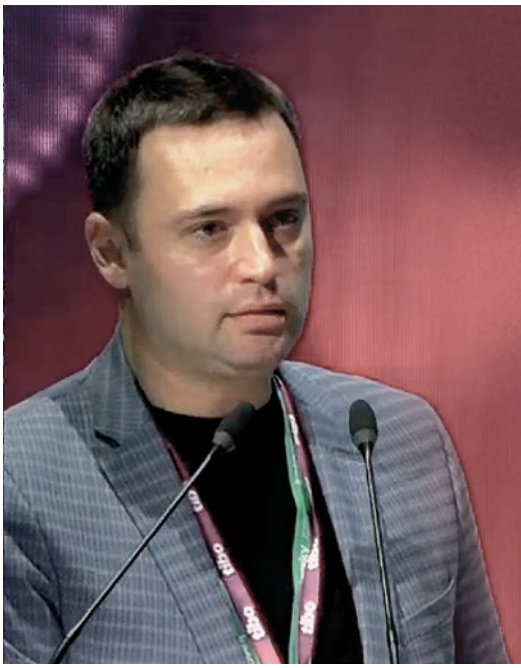
Кибербезопасность. ПРЕДЕЛ ТЕРПЕНИЯ



Спрос на решения в области кибербезопасности в глобальном и региональном масштабах стабильно растет. К сожалению, тема защиты от кибератак для многих организаций становится актуальной лишь тогда, когда они начинают подсчитывать убытки.

В целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз 14 февраля 2023 года Главой государства подписан Указ № 40 «О кибербезопасности». Суть документа заключается в создании национальной системы защиты от всех типов вредоносного ПО.

В связи с этим заслуживает внимания мнение представителя лидирующей в сегменте информационной безопасности компании Kaspersky в Беларуси Дмитрия КУДРЕВИЧА. Помимо комментария о направленности принятого документа, он отметил ряд других вопросов, не теряющих своей актуальности.

– Каким представляется положение дел в сфере кибербезопасности в Беларуси по итогам прошлого года?

– В 2022 году ряд иностранных вендоров в области кибербезопасности покинул белорусский рынок. Усложнение ландшафта киберугроз и необходимость оперативного перехода на альтернативное ПО для защиты цифровых активов подтолкнули организации различных отраслей к выбору надежных поставщиков из доступных на рынке вариантов. В 2022 году решения компании Kaspersky пользовались большим интересом со стороны представителей как малого и среднего, так и крупного бизнеса. Среди них можно отметить решение для защиты от целевых атак с передовой песочницей и актуальными сигнатурами, продукт для защиты конечных точек типа Endpoint Detection and Response.

Не меньшим вниманием пользуется и продукт для сбора и анализа событий безопасности класса SIEM. Важно учитывать, что проприетарные SIEM-платформы эффективнее и надежнее, чем SIEM на открытом исходном коде. Использование такого класса решений на Open Source возможно, но с этим связаны большие риски. Так, заказчик может не получить гарантий качества итогового решения, а также лишает себя уверенности в уровне надежности, поскольку в таких технологиях могут встречаться лишние элементы, включая вредоносный код, и содержаться уязвимости.

Стоит упомянуть и один из ключевых трендов на рынке – комплексный подход к информационной безопасности, в рамках которого компании стремятся защитить все элементы инфраструктуры и потенциальные точки входа в нее. Проявлением такого подхода являются набирающие популярность решения класса XDR – платформы, предоставляющие всеобъемлющую защиту от угроз любой сложности.

Все эти решения входят в портфолио Kaspersky, которое мы продолжаем активно усиливать в ответ на запросы рынка.

– Какова роль человеческого фактора в этом контексте?

– Роль человека в вопросах кибербезопасности сложно переоценить. Например, по данным ежегодного исследования Kaspersky «Информационная безопасность бизнеса», в 2021–2022 годах около 22 % всех утечек в секторе малого и среднего бизнеса во всем мире

произошли по вине сотрудников. Для сравнения: кибератака стала причиной утечки лишь в 9 % случаев. Сотрудники могут непреднамеренно спровоцировать серьезный инцидент кибербезопасности по разным причинам. Например, пользователи долго не обновляют корпоративное ПО, в котором могут быть уязвимости; используют слабые пароли от аккаунтов, которые легко угадать методом перебора; переходят по ссылкам из фишинговых писем или открывают вредоносное вложение; попадаются на уловки злоумышленников, которые применяют методы социальной инженерии. В большинстве случаев речь идет о низкой цифровой грамотности. Одними из наиболее действенных методов борьбы в этом случае являются регулярное проведение корпоративных тренингов по кибербезопасности среди сотрудников, повышение квалификации профильных специалистов и внедрение ряда защитных решений.

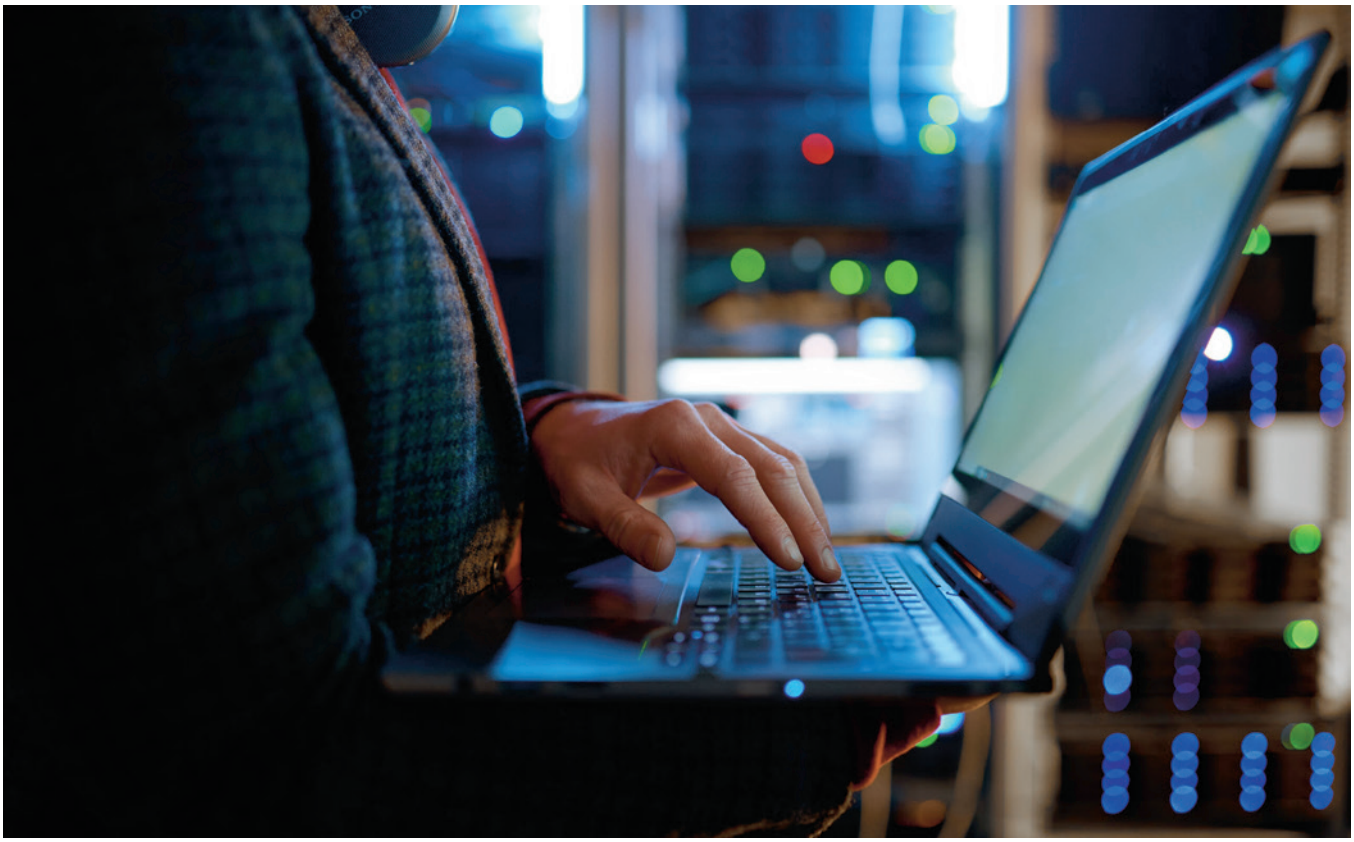
– Насколько может возрасти степень защиты от вредоносных программ при участии искусственного интеллекта? Какова ваша позиция в данном вопросе?

– Мы более 10 лет используем технологии машинного обучения в нашей работе, а также имплементируем их в наши продукты, в том числе для детектирования угроз. Это позволяет в разы эффективнее выполнять работу. Мы выявляем в день до 400 тысяч новых зловредных файлов. Работать с такими объемами только «руками» физически невозможно, потребовалось бы слишком много ресурсов. Поэтому в Kaspersky уже давно налажена автоматизация процессов с использованием инструментов искусственного интеллекта. До 99,9 % случаев вредоносной активности выявляются автоматическими методами. Однако, когда речь заходит о целевых продвинутых атаках на инфраструктуру, критических киберинцидентах, подключаются специалисты.

Также нейросети могут применяться в продуктах, помогающих обеспечивать безопасность предприятий. Существуют решения, которые физически защищают периметр объектов от проникновения на их территорию несанкционированных беспилотных летательных аппаратов: в них нейросети используются для классификации БПЛА. То есть система не использует базу данных беспилотников, а определяет тип и модель дрона, основываясь на своих «знаниях», проведенных ранее тестированиях.

– Что можно сказать о вирусной активности в Беларуси за минувшие месяцы текущего года? Какие структуры подвергаются наиболее агрессивным атакам?

– Процесс цифровизации в стране достаточно активен. Компании внедряют технологии, позволяющие автоматизировать процессы, ускорять работу, повышать эффективность. Например,

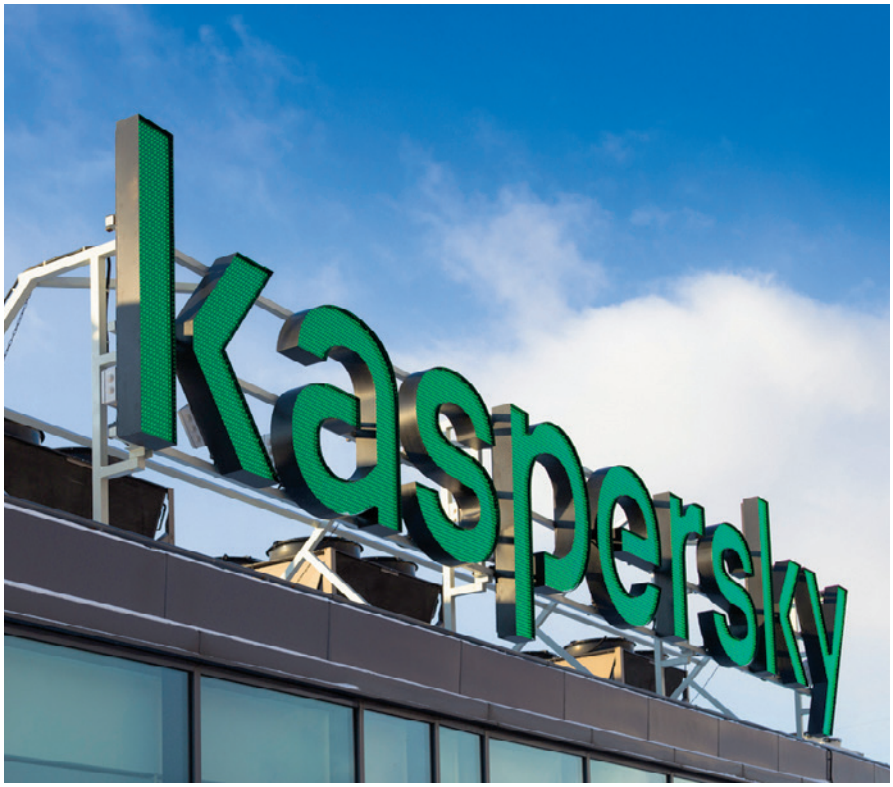


эта тенденция затрагивает финансовую и государственную сферы, медицину: те же организации в области здравоохранения переводят карты пациентов в удобный цифровой формат. Однако стоит понимать, что использование технологий так или иначе увеличивает количество потенциальных точек входа в инфраструктуру, и этим могут воспользоваться злоумышленники. Любой организации, независимо от ее масштаба, важно думать о комплексной защите своих цифровых активов, а также о безопасности персональных данных клиентов.

В 2023 году в Беларуси по сравнению с аналогичным периодом в прошлом году выросла доля корпоративных пользователей, столкнувшихся с локальными угрозами, которые составили более трети от общего числа. На их компьютерах были обнаружены вредоносные файлы, распространяющиеся, например, через съемные носители, в виде зашифрованных документов или в составе сложных инсталляторов. С этим же типом угроз сталкивались и те, кто использует продукты для защиты личных устройств, – их в первом полугодии 2023-го оказалось почти 40 %. С веб-угрозами – попытками заражения из интернета – столкнулось 15 % пользователей. Доля корпоративных пользователей, на чьих устройствах зафиксирована попытка заражения из интернета, – 23 %.

Не сбавляют обороты и фишеры: за первое полугодие текущего года защитные решения Kaspersky заблокировали около миллиона попыток белорусов перейти по подозрительным ссылкам. Такие, как правило, ведут на веб-ресурсы, где пользователи рискуют скомпрометировать свои конфиденциальные данные или потерять деньги.

При этом мы также наблюдаем рост доли корпоративных пользователей, атакованных программами-шифровальщиками. Только за первые 5 месяцев 2023 года в Беларуси этот показатель вырос на четверть.



Если говорить об угрозах в индустриальном секторе, то в 2023 году основным источником угроз остается интернет. Эта тенденция началась относительно давно, как минимум с 2017 года, и остается актуальной сейчас. Во втором полугодии 2022-го Беларусь стала одним из лидеров по наибольшему увеличению доли компьютеров систем автоматизации, на которых были отражены атаки: этот показатель вырос почти на 7 % по сравнению с первыми шестью месяцами. Преимущественно рост был связан с заметным увеличением доли компьютеров АСУ, которые были атакованы вредоносными объектами из интернета: по сравнению с первым полугодием она выросла на 13 процентных пунктов и составила 27,5 %.

Чтобы защититься от киберугроз, компаниям важно следовать принципам эшелонированной защиты своих активов.

– Каковы ваши прогнозы в связи с вступлением в силу указа № 40?

– Мы рады, что государство уделяет внимание рынку информационной безопасности и помогает ему развиваться. Как участник рынка в Беларуси, мы безусловно приветствуем совершенствование нормативно-правовой базы. Полагаем, что к концу 2023 года по всей стране будет запущено до 10 центров кибербезопасности, соответствующих требованию указа № 40, что позволит существенно усилить уровень защиты сложных инфраструктур в Беларуси, как крупных, так и малых, и, следовательно, обеспечить высокий уровень национальной безопасности Республики Беларусь. Мы оказываем и будем оказывать поддержку центрам кибербезопасности, в том числе за счет обеспечения нашими технологиями и использования многолетнего опыта построения подобных структур по всему миру. Определяющим для развития центров кибербезопасности в Республике Беларусь, на наш взгляд, будет 2024 год.