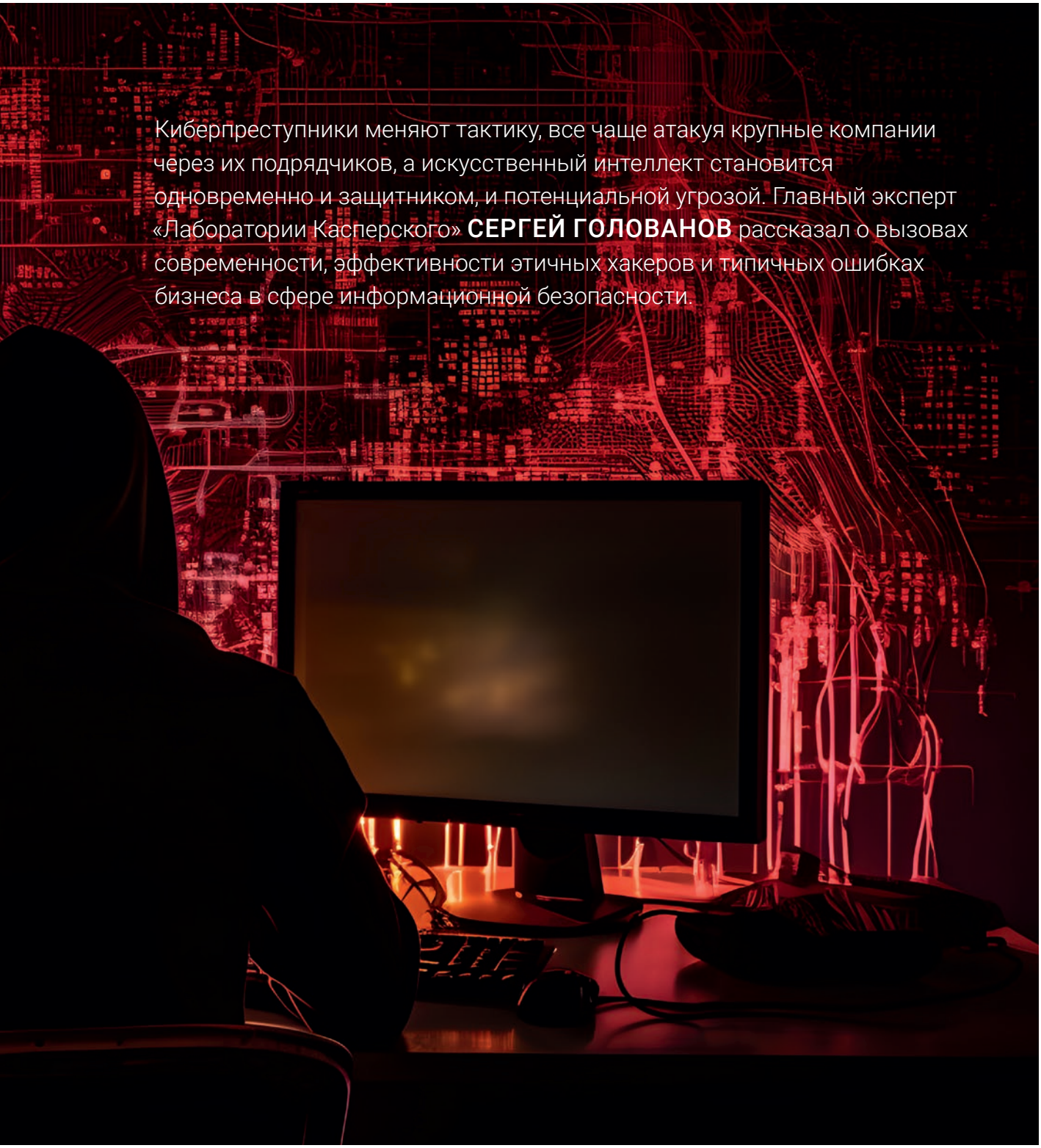
Где рвется цепь безопасности?



Киберпреступники меняют тактику, все чаще атакуя крупные компании через их подрядчиков, а искусственный интеллект становится одновременно и защитником, и потенциальной угрозой. Главный эксперт «Лаборатории Касперского» **СЕРГЕЙ ГОЛОВАНОВ** рассказал о вызовах современности, эффективности этичных хакеров и типичных ошибках бизнеса в сфере информационной безопасности.

— Сергей, что сегодня в тренде у киберпреступников. Как изменился ландшафт угроз по сравнению с предыдущими годами?

— В 2025 году продолжился тренд, который начался и развивался в 2023–2024 годах. Крупные компании становятся жертвами атак через подрядчиков. Крупные организации сегодня уже инвестируют в информационную безопасность. Но у любой крупной фирмы есть контрагенты из числа среднего бизнеса. И вот у последних не всегда достаточно ресурсов, чтобы обеспечить качественную киберзащиту. При этом компании сотрудничают: у них могут быть настроены связи между сетями, объединены данные. Поэтому самые громкие взломы, самые крупные хищения персональных данных часто как раз происходят через атаку на поставщиков. В таких инцидентах уязвимости подрядчика становятся уязвимостью заказчика, у которого, казалось бы, в плане кибербезопасности мышь не проскочит. Именно с уязвимостей, как правило, и начинаются атаки. На втором месте традиционно стоят слабые пароли.

Что еще нового? Вернулось не так уж и хорошо забытое старое — финансовые атаки на юридических лиц. Массовой эта история была около десяти лет назад, но потом кибермошенники перешли на обычных граждан. Теперь снова фиксируются атаки на юридических лиц именно через систему электронного документооборота. И цель злоумышленника — не завладеть персональными данными, не уничтожить их, не остановить бизнес-процессы, а украсть деньги.

> Злоумышленники переориентировались на корпоративный сектор, где обнаружили более доступные для себя мишени

— Воздействовать на физлиц сейчас все сложнее и сложнее. Видимо, поэтому мишень изменилась?

— Действительно, ситуация развивается именно так. В России в последнее время много сделано на законодательном уровне для защиты физических лиц. Появились инструменты противодействия телефонному мошенничеству и социальной инженерии. Работает защита от подмены телефонных номеров. Введена ответственность для дропперов, ответственность за использование сим-боксов. У нас появились периоды охлаждения при оформлении кредитов, даже самозапреты на кредиты и оформление сим-карт.

В результате злоумышленники переориентировались на корпоративный сектор, где обнаружили более доступные для себя мишени. Сейчас мы видим интересную динамику: количество случаев телефонного мошенничества в абсолютных цифрах постепенно снижается и растет сумма ущерба в корпоративном секторе.

— То есть мы сейчас говорим о законодательных пробелах? Нужны механизмы защиты и для юрлиц?

— Это сложный вопрос. Все-таки нападения на юрлиц — это пока бедствие не такого масштаба, как это было с телефонным мошенничеством. Кроме того, ограничительные меры бизнес может не воспринять. Например, все платежи B2B должны проходить моментально. Те же периоды охлаждения в данном случае неуместны.

— Неуместны. Но проблема цепочки поставщиков нарастает. Что с этим делать?

— От этого риска юридические лица должны и в силах защищать себя сами. Сейчас важно применять комплексный подход к решению этой проблемы. Первое — это документальное оформление всех отношений с подрядчиками. В случае инцидентов компании могут расторгнуть контракт и переложить ответственность за ущерб на партнера.

Второе направление — внедрение технических решений. Если раньше подрядчики имели достаточно свободный доступ к корпоративным системам, могли самостоятельно настраивать и изменять их, то сейчас ситуация кардинально изменилась. Ком-

пании значительно ужесточили контроль. Теперь любое действие подрядчика требует специального разрешения и оформляется документально. Для получения доступа необходимо согласование руководителя, четкое обоснование необходимости и строго определенные полномочия. Современная защита строится на сочетании организационных мер и технических ограничений доступа. Такой подход позволяет существенно снизить риски проникновения злоумышленников через цепочку поставщиков.

— Искусственный интеллект — друг или враг службам кибербезопасности? Ведь он может и помочь в защите, и стать источником угрозы.

— Если мы говорим про инциденты, которые связаны с нарушением инструкций безопасности, то здесь возрастает опасность использования дипфейков. В последние полтора-два года дипфейк-атаки стали массовыми. Злоумышленники активно используют современные нейронные сети для создания поддельных аудио- и видеоматериалов. Якобы от имени руководителей компаний рассылаются срочные указания подчиненным. Такие сообщения часто содержат призывы к немедленным действиям — например, к срочной финансовой помощи или другим операциям.

С другой стороны, AI может стать и защитником. Например, современные системы безопасности активно используют нейронные сети для анализа входящей корреспонденции. Практика показывает впечатляющие результаты: более 80 процентов вредоносных сообщений успешно выявляются автоматическими системами.

Однако у этой технологии есть свои ограничения. Основная проблема заключается в ошибках первого и второго рода. Из-за того, что принципы работы нейронных сетей не всегда прозрачны, система может как пропустить легитимное письмо, так и не заметить потенциально опасное сообщение.

Несмотря на эти недостатки, внедрение подобных систем остается оправданным решением. Главное преимущество заключается в относительно низких затратах на внедрение и возможности развернуть систему на собственном оборудовании организации. При этом важно понимать, что даже самые современные алгоритмы не гарантируют 100 процентов защиты и требуют дополнительного контроля со стороны специалистов.

НЕ БОЛТАЙ!

Согласно отчету компании BitDefender (документ недоступен на территории России, но опубликован на профильном портале), руководители многих компаний систематически запрещают специалистам по информационной безопасности разглашать сведения о выявленных уязвимостях в корпоративных IT-системах.

Исследование охватывает внушительную выборку: в опросе приняли участие свыше 600 специалистов по кибербезопасности из разных стран. Кроме того, аналитики изучили более 700 тысяч киберинцидентов. Полученные данные демонстрируют тревожную тенденцию: 58% опрошенных безопасников хотя бы раз получали от руководства указание не афишировать обнаруженные утечки и слабые места в защите.

Ситуация усугубляется — за двухлетний период (2023–2025) число случаев, когда руководство требовало от безопасников молчать о происшествиях, выросло почти на 40% (то есть более чем на треть).

Подобная политика хоть и позволяет компаниям временно сохранить репутацию, в долгосрочной перспективе чревата серьезными последствиями. В отчете подчеркивается: замалчивание проблем с кибербезопасностью неизбежно подрывает доверие как со стороны сотрудников, так и со стороны клиентов организации.

— Есть риск, что искусственный интеллект выйдет из-под контроля? Например, переобучится и начнет самостоятельно взаимодействовать с другими системами, представляя потенциальную угрозу?

— В сфере искусственного интеллекта сейчас уделяется большое внимание концепции безопасности агентов. Важно понимать, что нейронная сеть не способна к самостоятельным действиям — она может только обрабатывать информацию и отвечать на запросы пользователей.

Чтобы AI мог выполнять конкретные задачи, используются специальные механизмы — агенты, которые дают нейросети возможность взаимодействовать с внешним миром. Однако именно здесь кроется определенная опасность: эти агенты могут вести себя непредсказуемо, подобно людям, и иногда выдавать неожиданные результаты.

Несмотря на то что нейросеть действует в пределах заложенной в нее программы, она способна принимать решения, которые могут выходить за рамки ожидаемого поведения. Именно поэтому разрабатываются специальные защитные механизмы, предотвращающие возможный ущерб.

Примером служит использование AI в биржевой торговле. Когда нейросеть принимает решение о покупке или продаже активов, за ее действиями следит специальный постоянный внешний контроль, который не позволяет системе совершить критические операции — например, вложить все средства или полностью распродать активы. Подобные ограничения являются обязательным элементом работы с искусственным интеллектом.

— А что вы думаете о белых хакерах? Стоит ли компаниям привлекать их для проверки безопасности своих систем? Может ли такое сотрудничество быть опасным? Насколько вообще оправданно их использование сегодня?

— Институт этичных хакеров — это вполне легитимное и востребованное направление в сфере кибербезопасности. Такие специалисты работают как в крупных компаниях, так и в специализированных организациях, предоставляющих услуги по тестированию систем безопасности. Конечно, существуют определенные опасения: и со стороны самих хакеров, и со стороны их клиентов. Специалисты беспокоятся о возможной юридической ответственности, из-за чего требуют четкой правовой защиты своей деятельности. Заказчики видят риск, что белый хакер может перейти на «темную сторону» и начать использовать свои знания о компании ей во вред.

Однако подобные случаи крайне редки. Профессиональное сообщество выработало строгие критерии отбора специалистов: как правило, кандидат должен иметь не менее трех лет опыта работы, соответствующие сертификаты и высшее образование. Все эти опасения на практике оказываются скорее мифами, чем реальностью.

— Ваше видение — какие критические ошибки чаще всего допускают компании в сфере информационной безопасности? Какие типичные просчеты в организации защиты приводят к серьезным инцидентам?

— Самая популярная причина успешной атаки связана с человеческим фактором и организационными недочетами. Люди недосмотрели, не подумали, не учли. Типичный сценарий развития событий выглядит так: система защиты сигнализирует о потенциальной угрозе, но ответственный специалист в отпуске, его коллега не в курсе ситуации или просто не придает значения тревожному сигналу. В результате цепочка недосмотров и недопонимания приводит к серьезным последствиям. Когда начинаешь разбираться, часто выясняется, что каждый участник событий действовал вроде бы правильно, но мелкие упущения и недочеты в совокупности привели к проблеме. Тут даже вопрос не в компетенциях конкретного сотрудника, он теорию знает на сто процентов и умеет приложить ее к практике, но вот в подходах где-то ошибся.

— Положился на русский авось.

— Русский авось — страшная вещь. Порой, когда разбираешься с инцидентом, понимаешь, что корень зла не в том, что люди не делали положенного. Им просто не разрешали делать: «Не трогай, сломаешь. У нас бизнес порушится, если ты эту железку вытащишь». То есть часто руководство компаний не вникает в вопросы безопасности. Все хорошо, привычно, надежно, авось и дальше так пойдет. А вот не срабатывает…

Подготовила
Светлана Мартыненко