

**МАРИЯ КУЗНЕЦОВА,**
РЕДАКТОР GUIDE
«ЭКОНОМИКА И ЦИФРОВИЗАЦИЯ»

## ПРОЯВИТЬ КИБЕРНАСТОЙЧИВОСТЬ

**Сегодня киберугрозы перестали быть исключительно технической проблемой, превратившись в один из ключевых операционных рисков для бизнеса любого масштаба. Как отмечают эксперты, потенциальные последствия атак становятся сопоставимы с традиционными финансовыми рисками, нанося ущерб не только производственным процессам, но и репутации компаний. Закономерно, что подход к информационной безопасности смещается в область стратегического управления.**

**При этом в настоящее время основной вызов заключается не столько в количественном росте киберугроз, сколько в изменении их характера. Повышается уровень целевого и подготовленного воздействия, сохраняется роль человеческого фактора как фактора уязвимости, а инструменты искусственного интеллекта позволяют злоумышленникам масштабировать атаки и повышать их эффективность. Причем мошенники не ограничиваются лишь фишинговыми письмами. Нередко они используют сгенерированные аудио- и видеозаписи, имитирующие руководителей, пытаясь получить чувствительную информацию от сотрудников для дальнейшего ее использования. Расширяется и экосистема рисков из-за интеграции с подрядчиками и облачными сервисами.**

**Таким образом, современная кибербезопасность перестает быть вспомогательной функцией и становится одним из ключевых элементов системы корпоративного управления. А инвестиции в нее должны расцениваться не с позиции затрат, а как вклад в устойчивость бизнеса и защиту активов компании.**



# ОБЛАЧНО, ВОЗМОЖНЫ АТАКИ

**ЛАНДШАФТ КИБЕРУГРОЗ В 2025 ГОДУ ХАРАКТЕРИЗУЕТСЯ НЕ ТОЛЬКО КОЛИЧЕСТВЕННЫМ РОСТОМ, НО И КАЧЕСТВЕННОЙ ЭСКАЛАЦИЕЙ. КАК ОТМЕЧАЮТ ЭКСПЕРТЫ, ДЕЙСТВИЯ ЗЛОУМЫШЛЕННИКОВ СТАНОВЯТСЯ БОЛЕЕ РАЗРУШИТЕЛЬНЫМИ, А ИХ ИНСТРУМЕНТАРИЙ АКТИВНО ДОПОЛНЯЕТСЯ ТЕХНОЛОГИЯМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА. О ТОМ, КАКИМ БУДЕТ ЛАНДШАФТ КИБЕРУГРОЗ В 2026 ГОДУ, О ВЫБОРЕ СТРАТЕГИЙ ЗАЩИТЫ И ДИНАМИКЕ РАСХОДОВ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ — В МАТЕРИАЛЕ GUIDE.** ИРИНА РОМАНОВА

**БИТВА ЗА ПЕРИМЕТР** По данным портала киберразведки (Threat Intelligence) «Лаборатории Касперского», в 2025 году российские компании сталкиваются с атаками десятков хакерских группировок — их число росло на протяжении года. «Главным образом это связано с текущей геополитической ситуацией. Основную угрозу представляют хактивисты и APT-группы, проводящие сложные и часто скоординированные киберкампании. Мы также выделяем объединения гибридного хактивизма, которые имеют уникальный почерк. Они достигли высокого технического уровня и активны в публичном поле»,— отмечает Кирилл Митрофанов, руководитель команды аналитики Cyber Threat Intelligence в «Лаборатории Касперского». По словам господина Митрофанова, в числе основных векторов атак злоумышленников остаются фишинг и эксплуатация уязвимостей.

«В 2025 году действия группировок стали более разрушительными: активно применялись программы-шифровальщики и вайперы, то есть вредоносное ПО для уничтожения инфраструктуры. В некоторых случаях группировки использовали сразу оба зловреда в одной атаке. Злоумышленники заметно эволюционировали: все чаще они разрабатывают собственные инструменты, в том числе с применением ИИ, и объединяются для проведения совместных операций, что усложняет атрибуцию атаки конкретной группировке и исследование инцидентов»,— объясняет эксперт.

Во многих случаях инциденты начинались с простых вещей: писем «от бухгалтерии», сообщений «от службы поддержки», ссылок на поддельные сервисы или просьб срочно что-то проверить. «Злоумышленники подстраивались под конкретную компанию, роль сотрудника и текущие события. Люди сами выходили на контакт, переходили по ссылкам или звонили по номерам из писем. После этого атака быстро развивалась и могла приводить к краже доступов или остановке систем»,— уточняет Алина Ледяева, эксперт StopPhish.

Она солидарна с коллегой в том, что во многом это связано с геополитической обстановкой. «Российские компании становились целями атак как по идеологическим, так и по финансовым причинам, а сценарии были направлены на остановку бизнеса. Зоны риска расширялись из-за подрядчиков, облаков, интеграций и внешних сервисов. Базовые меры — бэкапы, доступы, сегментация — не всегда успевали за уровнем угроз. Ситуацию усугубляет и ИИ: фишинговые письма стали дешевле, быстрее и правдоподобнее»,— говорит эксперт.

При этом злоумышленники используют ИИ не только для генерации персонализированных фишинговых писем, но и для создания убедительных дипфейков и клонирования голоса. «Было отмечено множество случаев, когда с помощью сгенерированных аудио- и видеозаписей мошенники имитировали руководителей и пытались получить от сотрудников чувствительную информацию для ее дальнейшего использования в личных целях»,— говорит Алексей Протасов, старший специалист по информационной безопасности BPMSoft (IT-холдинг Lansoft).

Отдельная и очень важная тенденция — использование массивов данных из старых утечек. «На их основе сформировались подробные нелегальные цифровые профили граждан и сотрудников. В сочетании с ИИ это дает более таргетированные, выверенные атаки: от компрометации учетных записей до подмены реквизитов и мошенничества „под конкретного человека“»,— говорит Евгений Семенов, архитектор национальных систем цифровой идентичности, генеральный директор «РТК Софт Лабс». → 4



ИГОРЬ ИВАНКО

ЗЛОУМЫШЛЕННИКИ ИСПОЛЬЗУЮТ ИИ НЕ ТОЛЬКО ДЛЯ ГЕНЕРАЦИИ ПЕРСОНАЛИЗИРОВАННЫХ ФИШИНГОВЫХ ПИСЕМ, НО И ДЛЯ СОЗДАНИЯ УБЕДИТЕЛЬНЫХ ДИПФЕЙКОВ И КЛОНИРОВАНИЯ ГОЛОСА