**Может ли искусственный интеллект стать главным оружием хакеров?**

В Google накануне заявили о тревожной тенденции: злоумышленники активно используют Gemini AI, разработку компании, для усиления кибератак. Руководитель лаборатории исследований кибербезопасности компании «Газинформсервис» Вадим Матвиенко предупреждает, что нейросети позволяют киберпреступникам действовать быстрее, эффективнее и масштабнее. В условиях роста интеллектуализации атак традиционные методы защиты могут оказаться недостаточными, и на помощь в защите придут современные инструменты центров мониторинга информационной безопасности, таких как GSOC.

Группа анализа угроз Google (GTIG) выявила, что хакеры применяют Gemini AI на различных этапах атак. Интеллектуальные алгоритмы помогают киберпреступникам проводить разведку, выявляя уязвимости в системах потенциальных жертв, а также разрабатывать вредоносный код, ускоряя и упрощая процесс создания новых киберугроз.

**Вадим Матвиенко**, эксперт в области кибербезопасности, комментирует ситуацию: *«Большие языковые модели и искусственный интеллект в целом значительно повышают производительность многих специалистов. Эксперты предсказывали, что АРТ-группировки будут активно использовать ИИ, такие как Gemini от Google. Применение нейросетей в сфере киберпреступности значительно ускоряет все этапы проведения атак — от разведки и подготовки фишинговых писем до разработки новых шифровальщиков».*

Эксперт предлагает ответ на эти вызовы: *«Новые угрозы требуют новых подходов к обеспечению информационной безопасности. Аналитики из центра мониторинга безопасности "Газинформсервис" используют самые современные средства защиты информации, чтобы быстро выявлять атаки и оперативно реагировать на них».*

**Справка о компании:**

[ООО «Газинформсервис»](https://www.gaz-is.ru/) — отечественный разработчик программных и программно-аппаратных средств обеспечения информационной безопасности и комплексной инженерно-технической охраны. Компания специализируется на создании систем обеспечения информационной безопасности объектов и ИБ-систем для корпораций энергетической и транспортной отраслей, органов государственной власти, промышленных предприятий, а также учреждений финансового сектора и телекоммуникационных компаний.