

УДК 004.056.5

Роль генеративного ИИ в кибербезопасности

Лосев Никита Сергеевич

losevns@student.bmstu.ru

Глинская Елена Вячеславовна

glinskaya@bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Россия

Аннотация. Исследовано применение генеративного искусственный интеллект (ИИ) для повышения эффективности систем информационной безопасности. Показано, как такие модели улучшают выявление ранее неизвестных угроз, ускоряют реагирование на инциденты безопасности и снижают долю ложных срабатываний. Отдельное внимание уделено противодействию мошенничеству и использованию синтетических данных для обучения и тестирования защитной инфраструктуры.

Ключевые слова: информационная безопасность, генеративный ИИ, детектирование угроз, оперативное реагирование, предотвращение мошенничества, синтетические данные

Введение. Рост объема и изменчивости данных журналов безопасности, сетевого трафика и результатов мониторинга, а также усложнение тактик злоумышленников требуют методов, способных выявлять необычные закономерности без больших объемов заранее размеченных данных и с возможностью распознавать новые типы угроз. Генеративные модели, которые изучают нормальное поведение систем и характерные приемы атак, повышают чувствительность обнаружения и сокращают время принятия защитных мер [1].

Методы и материалы; результаты.

1. Детектирование неизвестных угроз.

Генеративные модели формируют представление о «нормальном» поведении трафика, журналов и действий пользователей. Любые отклонения от этой нормы выделяются и передаются на проверку. Дополнение обучения синтетическими примерами атак помогает учитывать редкие ситуации и снижает риск пропуска новых разновидностей угроз [2].

2. Оперативное реагирование и снижение ложных срабатываний.

На этапе анализа событий безопасности генеративные модели выполняют предварительную обработку: они объединяют похожие записи, удаляют повторяющиеся, восстанавливают точную цепочку действий. Это снижает количество ложных срабатываний и позволяет быстрее передавать реальные инциденты на обработку специалистам.

3. Предотвращение мошенничества.

В финансовой сфере и смежных областях генеративные модели отслеживают типичное поведение пользователей и выявляют подозрительные отклонения в транзакциях и заявках. Исследования показывают, что наилучший результат достигается при сочетании генеративных моделей с правилами оценки рисков и анализом связей между участниками операций [3].

4. Генерация синтетических данных.

Использование сгенерированных моделями синтетических данных повышает устойчивость детекторов к редким видам атак и помогает безопасно воспроизводить разнообразные сценарии тестирования систем безопасности на больших объемах информации. Однако это требует обязательной проверки и аудита самих моделей, контроля качества данных и масштабируемости инфраструктуры [4], а также участия специалистов на ключевых этапах принятия решений [5].

Заключение. Генеративные модели усиливают защиту информационных систем сразу по нескольким направлениям. Они помогают обнаруживать ранее неизвестные угрозы, обрабатывая отклонения от нормального поведения; снижают количество ложных срабатываний за счет фильтрации и восстановления контекста событий; повышают эффективность борьбы с мошенничеством благодаря выявлению аномалий в транзакциях и заявках; а также расширяют возможности обучения и тестирования систем безопасности с помощью синтетических данных.

Список источников

- [1] Generative AI and security: transforming cyber security defense and fraud prevention. International Research Journal of Modernization in Engineering Technology and Science, 2024, <https://doi.org/10.56726/irjmets60823>
- [2] Аменицкий А.В., Рухович И.В., Аменицкая Л.А., Аменицкий Д.А. и др. *Управление рисками кибербезопасности. В кн. Современная наука: актуальные вопросы, достижения и инновации*, Пенза, Наука и Просвещение (ИП Гуляев Г.Ю.), 2024, с. 88–99. EDN: TCHJBG.
- [3] Бабанская А.С., Ермольева Д.Р., Ефименко Н.А., Акулова С.А. Сравнительный анализ и возможности ИИ-технологий для предотвращения мошенничества в финансовом секторе. *Экономика. Информатика*, 2025, т. 52, № 1, с. 110–124. <https://doi.org/10.52575/2687-0932-2025-52-1-110-124>
- [4] Curran K., Curran E., Killen J., Duffy C. The role of generative AI in cyber security. *Metaverse*, 2024, vol. 5, no. 2, art. no. 2796. <https://doi.org/10.54517/m2796>
- [5] Попов А.С., Балакирев С.В., Егоров В.М. Искусственный интеллект в системах информационной безопасности. *Научный резерв*, 2024, № 2 (26), с. 31–36.