УДК: —
МРНТИ: —

[1] Толетаев Бауыржан Толетаевич*, Түлкібай Дінмұхамед Әбділдаұлы

[1]Қазақстан Республикасының Ұлттық қорғаныс университеті,

**toletaevbauyrzan@gmail.com*

ПРИМЕНЕНИЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ ДЛЯ АВТОМАТИЗАЦИИ ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ КИБЕРУГРОЗ В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация. Аннотация. Аннотация. В статье рассматриваются возможности применения больших языковых моделей (Large Language Models, LLM) для автоматизации процессов обнаружения, анализа и классификации киберугроз в корпоративных сетях. Актуальность исследования обусловлена стремительным ростом объема событий информационной безопасности, усложнением методов кибератак и ограниченностью человеческих ресурсов центров мониторинга безопасности (SOC). Проведен анализ современных подходов к использованию искусственного интеллекта в системах киберзащиты, рассмотрены преимущества интеграции больших языковых моделей с платформами SIEM и SOAR. Особое внимание уделено вопросам автоматической интерпретации журналов событий, выявления аномалий, классификации инцидентов и формирования рекомендаций по реагированию. Рассмотрены основные риски внедрения LLM, включая генерацию ложных выводов, утечки конфиденциальных данных и возможность манипуляции моделями со стороны злоумышленников. По результатам исследования предложена концептуальная модель интеллектуальной системы обнаружения угроз на основе больших языковых моделей.

Ключевые слова: большие языковые модели, кибербезопасность, искусственный интеллект, корпоративные сети, обнаружение угроз, SIEM, SOAR, анализ журналов, автоматизация безопасности.

[1] Толетаев Бауыржан Толетаевич, Түлкібай Дінмұхамед Әбділдаұлы

[1]Қазақстан Республикасының Ұлттық қорғаныс университеті,

КӘСІПОРЫН ЖЕЛІЛЕРІНДЕ КИБЕРҚАУІПТЕРДІ АНЫҚТАУ МЕН ЖІКТЕУДІ АВТОМАТТАНДЫРУ ҮШІН ҮЛКЕН ТІЛДІК МОДЕЛЬДЕРДІ ҚОЛДАНУ

Аңдатпа. Түйіндеме. Мақалада Қазақстанның қазіргі заманғы цифрлық инфрақұрылымындағы киберқауіпсіздік мәселелері кешенді түрде қарастырылады. Зерттеудің өзектілігі қоғамның жаппай цифрландырылуы жағдайында киберқылмыстардың трансшекаралық сипат алуымен және олардың әдіс-тәсілдерінің күрделенуімен негізделеді. Жұмыс барысында «Қазақстанның киберқалқаны» тұжырымдамасының тиімділігіне талдау жасалып, Эстония мен Оңтүстік Корея сияқты жетекші елдердің тәжірибесімен салыстыру жүргізілді. Мақалада киберқылмыстың экономикалық және әлеуметтік аспектілері, соның ішінде интернет-алаяқтық, SQL-инъекциялар және DDoS-шабуылдардың техникалық алгоритмдері егжей-тегжейлі сипатталған. Автор халықаралық стандарттар мен отандық заңнамалық базаны зерделей отырып, ақпараттық қауіпсіздікті нығайтудың жаңа моделін ұсынады. Зерттеу нәтижелері мемлекеттік ақпараттық жүйелердің төзімділігін арттыруға және халықтың цифрлық сауаттылығын стратегиялық дамытуға бағытталған.

Түйінді сөздер: киберқауіпсіздік, цифрлық экожүйе, киберқылмыс, Қазақстанның киберқалқаны, интернет-алаяқтық, ақпараттық қауіпсіздік.

[1] Толетаев Бауыржан Толетаевич, Түлкібай Дінмұхамед Әбділдаұлы

[1]Қазақстан Республикасының Ұлттық қорғаныс университеті,

THE USE OF LARGE LANGUAGE MODELS TO AUTOMATE THE DETECTION AND CLASSIFICATION OF CYBER THREATS IN CORPORATE NETWORKS

Abstract. Abstract. The article provides a comprehensive examination of cybersecurity issues in Kazakhstan's modern digital infrastructure. The relevance of the study is grounded in the cross-border nature of cybercrimes and the increasing complexity of their methods amidst the massive digitalization of society. The paper analyzes the effectiveness of the "Cyber Shield of Kazakhstan" concept and provides a comparative study with the experiences of leading countries such as Estonia and South Korea. The economic and social aspects of cybercrime are described in detail, including the technical algorithms of Internet fraud, SQL injections, and DDoS attacks. By examining international standards and the domestic legal framework, the author proposes a new model for strengthening information security. The findings of the research are aimed at improving the resilience of state information systems and the strategic development of digital literacy among the population.

Keywords: cybersecurity, digital ecosystem, cybercrime, information technologies, Cyber Shield Kazakhstan, Internet fraud, information security.

Введение. Современные корпоративные сети представляют собой сложные распределенные информационные системы, включающие локальную инфраструктуру, облачные сервисы, мобильные устройства и удаленные рабочие места сотрудников. Цифровая трансформация бизнеса привела к значительному увеличению количества подключенных систем и объемов обрабатываемых данных. Одновременно возросло число киберугроз, направленных на получение несанкционированного доступа к корпоративным ресурсам, кражу конфиденциальной информации и нарушение непрерывности бизнес-процессов.

Согласно международным исследованиям в области информационной безопасности, значительная часть организаций ежедневно сталкивается с тысячами подозрительных событий, требующих анализа со стороны специалистов SOC. Традиционные методы мониторинга, основанные на сигнатурном анализе и ручной обработке журналов событий, все чаще оказываются недостаточными для своевременного выявления сложных атак. В таких условиях особый интерес представляет применение технологий искусственного интеллекта, способных автоматизировать обработку больших объемов данных и повысить эффективность принятия решений.

Появление больших языковых моделей открыло новые возможности для анализа информации в сфере кибербезопасности. В отличие от классических алгоритмов машинного обучения, LLM способны работать с неструктурированными текстовыми данными, понимать контекст событий и формировать аналитические выводы на естественном языке. Это делает их перспективным инструментом для автоматизации обнаружения и классификации киберугроз в корпоративных сетях.

Методы исследованияДля достижения поставленной цели использовался комплексный подход, включающий анализ научной литературы, сравнительное исследование современных решений в области кибербезопасности и моделирование процессов обработки событий безопасности с применением больших языковых моделей.

Системный анализ позволил определить основные этапы жизненного цикла инцидента информационной безопасности и выявить точки интеграции LLM в существующие процессы мониторинга.

Сравнительный анализ был проведен между традиционными средствами обнаружения угроз и интеллектуальными системами, использующими методы обработки естественного языка.

Метод моделирования применялся для построения концептуальной архитектуры автоматизированной системы анализа угроз, включающей сбор телеметрии, обработку журналов событий, классификацию инцидентов и генерацию рекомендаций по реагированию.

Результаты исследования. Проведенный анализ показал, что большие языковые модели могут быть эффективно использованы на нескольких этапах процесса обеспечения информационной безопасности:

1. Автоматический анализ журналов событий

Корпоративные сети ежедневно генерируют огромные объемы логов, поступающих от серверов, рабочих станций, сетевого оборудования, средств защиты информации и облачных платформ. Традиционный анализ таких данных требует значительных временных затрат.

Большие языковые модели способны автоматически интерпретировать текстовые записи журналов, выявлять подозрительные последовательности действий и формировать краткие аналитические отчеты для специалистов по безопасности.

Например, при обнаружении многократных неудачных попыток аутентификации, последующего успешного входа и скачивания большого объема данных модель может объединить эти события в единый сценарий потенциальной

компрометации учетной записи.

2. Классификация киберугроз

Одной из наиболее трудоемких задач является определение типа и уровня опасности обнаруженного инцидента.

Большие языковые модели способны автоматически относить события к определенным категориям угроз:

- фишинговые атаки;
- вредоносное программное обеспечение;
- атаки программ-вымогателей;
- эксплуатация уязвимостей;
- внутренние угрозы;
- атаки типа DDoS;
- попытки повышения привилегий;
- несанкционированный доступ к данным.

Использование контекстного анализа позволяет повысить точность классификации по сравнению с традиционными методами поиска сигнатур.

3. Поддержка аналитиков SOC

Одним из наиболее перспективных направлений является применение LLM в качестве интеллектуального помощника аналитика.

Модель может автоматически:

– объяснять значение обнаруженного события;

– определять возможные последствия атаки;

– предлагать рекомендации по реагированию;

– формировать отчеты для руководства;

– выполнять первичный анализ инцидентов.

Это позволяет существенно сократить время обработки инцидентов и снизить нагрузку на персонал центра мониторинга безопасности.

4. Интеграция с платформами SIEM и SOAR

Исследование показало высокую эффективность интеграции больших языковых моделей с системами класса SIEM и SOAR.

В подобной архитектуре SIEM выполняет сбор и корреляцию событий безопасности, а LLM обеспечивает интеллектуальную интерпретацию полученных данных. После классификации угрозы SOAR-платформа может автоматически инициировать необходимые действия:

• блокировку подозрительного IP-адреса;

• изоляцию зараженного узла;

• отключение скомпрометированной учетной записи;

• создание заявки для специалистов безопасности.

Подобный подход позволяет реализовать концепцию полуавтоматического или полностью автоматизированного реагирования на инциденты.

Обсуждение. Полученные результаты свидетельствуют о высокой перспективности использования больших языковых моделей в корпоративной кибербезопасности. Вместе с тем внедрение подобных технологий сопровождается рядом ограничений и рисков.

1. Проблема достоверности выводов

Большие языковые модели способны генерировать убедительные, но ошибочные заключения. В сфере информационной безопасности подобные ошибки могут привести к ложным срабатываниям или пропуску реальных атак.

Поэтому критически важные решения должны проходить дополнительную проверку специалистами по безопасности либо подтверждаться другими средствами обнаружения угроз.

2. Конфиденциальность данных

Для анализа инцидентов модели получают доступ к журналам событий, сетевой телеметрии и другой чувствительной информации.

Использование публичных облачных моделей может привести к утечке корпоративных данных. В связи с этим многие организации рассматривают возможность развертывания локальных LLM внутри собственного защищенного контура.

3. Атаки на искусственный интеллект

С ростом популярности LLM появляются новые методы воздействия на модели.

Злоумышленники могут использовать специально сформированные запросы для обхода защитных механизмов, генерации ложных рекомендаций или сокрытия признаков атаки.

Это требует разработки специальных механизмов контроля качества ответов и защиты моделей от манипуляций.

4. Перспективы развития

В ближайшие годы ожидается активное развитие концепции «AI for Cybersecurity», предполагающей использование искусственного интеллекта на всех этапах управления безопасностью.

Особый интерес представляют следующие направления:

• мультимодальный анализ угроз;
• интеллектуальная корреляция событий;
• прогнозирование атак;
• автономные системы реагирования;
• самообучающиеся платформы киберзащиты.

В перспективе большие языковые модели могут стать ключевым элементом цифровых центров мониторинга безопасности нового поколения.

Заключение. Проведенное исследование показало, что большие языковые модели обладают значительным потенциалом для автоматизации обнаружения и классификации киберугроз в корпоративных сетях. Их применение позволяет существенно повысить скорость обработки событий безопасности, улучшить качество анализа инцидентов и сократить нагрузку на специалистов SOC.

Наиболее эффективным направлением является интеграция LLM с существующими платформами SIEM и SOAR, что обеспечивает интеллектуальную обработку данных и автоматизированное реагирование на угрозы. Вместе с тем внедрение подобных технологий требует решения вопросов конфиденциальности данных, повышения достоверности выводов моделей и защиты самих систем искусственного интеллекта от внешних воздействий.

Большие языковые модели являются одним из наиболее перспективных инструментов развития корпоративной кибербезопасности и могут стать важной составляющей интеллектуальных систем защиты информации в условиях постоянно растущего количества и сложности киберугроз.

СПИСОК ЛИТЕРАТУРЫ

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016.

2. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020.

3. NIST Cybersecurity Framework 2.0. – National Institute of Standards and Technology, 2024.

4. ISO/IEC 27001:2022 Information Security Management Systems – Requirements.
5. OWASP Foundation. OWASP Top 10 Web Application Security Risks. – 2023.
6. Alon A., Raviv L. Large Language Models for Cybersecurity Applications // Journal of Information Security. – 2024.
7. Microsoft Security Copilot Technical Documentation. – Microsoft Corporation, 2024.
8. ENISA Threat Landscape Report. – European Union Agency for Cybersecurity, 2024.
9. MITRE ATT&CK Framework Documentation. – MITRE Corporation, 2024.
10. IBM X-Force Threat Intelligence Index. – IBM Security, 2024.