Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Уральский Федеральный университет имени первого

Президента России Б.Н.Ельцина»

Институт Радиоэлектроники и информационных технологий – РТФ

Кафедра школа бакалавриата

ОТЧЕТ

по теме:

“LLM для кибербезопасности”

|  |  |
| --- | --- |
| Студент:  Группа: | Нижник Е.И.  РИ-231002 |
|  |  |
|  |  |
|  |  |

Екатеринбург

2024

# Содержание отчёта

[Содержание отчёта 2](#_5fclim7lyey9)

[1. Введение 3](#_gaq3iuca3nx5)

[2. Состояние технологии 5](#_s20up25m7pai)

[3. Перспективы технологии 7](#_u7bkje6j90h9)

[5. Производители 9](#_q8g51q5r6k55)

[6. Заказчики 11](#_4eidcaev1rn1)

[7. Выводы 14](#_tjwfts1yccle)

# 

# 1. Введение

Определение LLM в контексте кибербезопасности  
Большие языковые модели (Large Language Models, LLM) – это сложные нейронные сети, обученные на больших массивах текстовых данных, способные решать задачи анализа, обработки и генерации текстовой информации. Эти модели, включая архитектуры вроде GPT, BERT и их аналоги, выделяются способностью понимать контекст и семантические связи, что делает их эффективным инструментом для работы с неструктурированными данными.

В сфере кибербезопасности LLM играют ключевую роль в автоматизации процессов анализа угроз, выявления уязвимостей и улучшения взаимодействия специалистов с информационными системами. Они способны обрабатывать текстовые отчёты о кибератаках, выявлять вредоносные паттерны в логах, противодействовать фишингу и мошенничеству, а также предлагать решения по устранению уязвимостей в программном коде.

Роль больших языковых моделей в обеспечении безопасности информационных систем

1. Автоматизация анализа инцидентов: LLM позволяют быстро анализировать логи, отчёты об инцидентах, сообщения и другую текстовую информацию, чтобы находить подозрительные действия или закономерности, связанные с кибератаками.
2. Фишинг и социальная инженерия: За счёт способности анализировать контекст, большие языковые модели могут выявлять признаки мошеннических сообщений и предупреждать пользователей.
3. Анализ уязвимостей кода: С помощью LLM можно находить уязвимости в программном обеспечении, генерировать безопасные исправления и обучать разработчиков безопасным практикам кодирования.
4. Поддержка в принятии решений: Модели могут служить интеллектуальными помощниками, резюмируя данные, предоставляя рекомендации и автоматизируя рутинные задачи.
5. Обнаружение аномалий в системах безопасности: Анализируя сетевые потоки и поведение пользователей, LLM помогают в обнаружении необычной активности.

Значение LLM для кибербезопасности

Большие языковые модели (Large Language Models, LLM) играют важную роль в современных системах обеспечения кибербезопасности. Эти мощные инструменты способны обрабатывать огромные массивы текстовых данных, включая логи событий, отчёты об инцидентах, коммуникации и техническую документацию, что делает их незаменимыми для анализа, обнаружения угроз и автоматизации процессов защиты.

Применение LLM в кибербезопасности

1. Обнаружение угроз  
   LLM способны анализировать логи сетевой активности, события на устройствах и отчёты о вредоносной активности, выявляя аномальные паттерны и скрытые угрозы. Например, они могут находить фишинговые атаки, интерпретируя стилистические особенности текста и контекст сообщений.
2. Защита данных  
   Модели помогают выявлять утечки данных и несанкционированный доступ, анализируя данные о взаимодействии пользователей с системами и изменениях в файлах. LLM также используются для классификации и управления конфиденциальными данными, предотвращая их утечку.
3. Анализ инцидентов  
   После кибератаки LLM ускоряют процесс расследования, автоматически интерпретируя логи, выявляя ключевые события и предоставляя аналитикам рекомендации для дальнейших действий. Например, модели могут резюмировать инциденты и классифицировать их по уровням критичности.
4. Автоматизация киберзащиты  
   В системах автоматизированного реагирования (SOAR) LLM участвуют в разработке сценариев реагирования, генерируют отчёты о проделанной работе и помогают управлять инцидентами. Это снижает нагрузку на аналитиков и минимизирует человеческий фактор.

Преимущества использования LLM

* Повышение скорости обнаружения и реагирования на инциденты.
* Снижение нагрузки на специалистов по безопасности.
* Обработка неструктурированных данных, включая текстовые отчёты и сообщения.
* Адаптация к новым угрозам благодаря обучению на актуальных данных.

# 2. Состояние технологии

В последние годы большие языковые модели (LLM) стали играть значительную роль в области кибербезопасности, предлагая новые подходы к анализу угроз, предсказанию атак и улучшению мониторинга безопасности. Рассмотрим текущие тенденции, технологические достижения и ключевые методы применения LLM в кибербезопасности.

Текущие тенденции в использовании LLM для кибербезопасности

LLM активно применяются для автоматизации анализа угроз, предсказания кибератак и повышения эффективности мониторинга безопасности. Они способны обрабатывать большие объемы данных, выявлять аномалии и предлагать рекомендации по реагированию на инциденты. Однако с ростом использования LLM появляются и новые уязвимости, требующие внимания специалистов по безопасности.

1. Обнаружение угроз и анализ уязвимостей

LLM используются для выявления уязвимостей в программном обеспечении и анализа вредоносных программ. Они способны обрабатывать большие объемы данных, идентифицируя потенциальные угрозы и аномалии. Систематический обзор литературы показывает, что LLM применяются для обнаружения уязвимостей, анализа вредоносных программ, обнаружения сетевых вторжений и фишинга.

2. Автоматизация реагирования на инциденты

LLM способствуют автоматизации процессов реагирования на инциденты, включая генерацию отчетов и рекомендации по устранению угроз. Это позволяет ускорить реагирование на кибератаки и повысить эффективность операций по обеспечению безопасности.

3. Противодействие фишингу и социальной инженерии

LLM применяются для распознавания фишинговых атак и других методов социальной инженерии, анализируя текстовые сообщения и выявляя подозрительные паттерны. Это помогает предотвращать атаки, направленные на получение конфиденциальной информации.

4. Улучшение защиты данных

Использование LLM позволяет улучшить защиту данных путем анализа и прогнозирования уязвимостей, а также разработки стратегий их устранения. Это способствует повышению общей безопасности информационных систем.

5. Вызовы и риски

Несмотря на преимущества, LLM могут быть использованы злоумышленниками для создания более сложных атак, таких как генерация фишинговых писем или вредоносного кода. Это подчеркивает необходимость разработки мер по защите самих моделей и предотвращению их злоупотребления.

6. Использование LLM в России

В России также активно исследуется применение LLM в кибербезопасности. Эксперты Positive Technologies отмечают, что машинное обучение и LLM становятся ключевыми трендами, влияющими на развитие кибербезопасности в средне- и долгосрочной перспективе.

Технологические достижения

Интеграция искусственного интеллекта и машинного обучения в процессы обработки больших данных позволяет значительно повысить точность анализа аномалий и обнаружения угроз. Современные методы машинного обучения, включая глубокое обучение и нейронные сети, применяются для создания моделей, способных адаптироваться к новым видам атак и быстро реагировать на изменяющиеся угрозы.

Основные технологии и методы LLM для кибербезопасности

Ключевые методы применения LLM в кибербезопасности включают:

* Обработка естественного языка (NLP): Используется для анализа текстовых данных, таких как журналы событий, сообщения электронной почты и другие источники, с целью выявления потенциальных угроз и аномалий.
* Классификация угроз: LLM обучаются распознавать различные типы угроз, что позволяет автоматизировать процесс их идентификации и приоритизации.
* Анализ уязвимостей: Модели помогают в обнаружении и оценке уязвимостей в системах, предлагая рекомендации по их устранению и предотвращению возможных атак.

# 3. Перспективы технологии

Большие языковые модели (LLM) играют все более значимую роль в сфере кибербезопасности, предлагая новые подходы к защите данных и обнаружению угроз. Рассмотрим перспективы их развития, прогнозы роста, а также возможные вызовы и ограничения.

Ожидаемые тренды в развитии LLM для кибербезопасности

* Повышение эффективности защиты данных и обнаружения угроз: LLM способны анализировать большие объемы данных, выявляя аномалии и потенциальные угрозы. Их применение позволяет улучшить процессы обнаружения и реагирования на инциденты безопасности.
* Интеграция с облачными решениями и IoT: С развитием облачных технологий и Интернета вещей LLM будут все чаще использоваться для мониторинга и защиты распределенных систем, обеспечивая проактивную защиту и быстрое реагирование на возникающие угрозы.

Прогнозы роста и популярности

* Рост рынка LLM для кибербезопасности: Российский рынок кибербезопасности будет расти со среднегодовым темпом прироста в 23,6%, достигая значительных объемов к 2028 году. Ожидается, что большая часть этого объема придется на отечественных производителей.
* Снижение затрат на киберзащиту: Автоматизация процессов обнаружения и реагирования на угрозы с помощью LLM может привести к снижению затрат на кибербезопасность, повышая эффективность и снижая необходимость в ручном вмешательстве.

Возможные вызовы и ограничения

* Обработка больших данных: LLM требуют значительных вычислительных ресурсов для обработки и анализа больших объемов данных, что может стать препятствием для их широкого внедрения.
* Необходимость обучения на актуальных данных: Для обеспечения эффективности LLM необходимо регулярное обновление и обучение на актуальных данных, что требует постоянного мониторинга и поддержки.
* Сложности с интерпретацией результатов: Результаты, предоставляемые LLM, могут быть сложными для интерпретации, что затрудняет принятие решений на их основе и требует дополнительной экспертизы.

4. Рыночная ниша

Большие языковые модели (LLM) играют все более значимую роль в кибербезопасности, предоставляя новые инструменты для обнаружения угроз, анализа уязвимостей и автоматизации процессов защиты. Рассмотрим рыночную нишу LLM в контексте кибербезопасности по следующим аспектам:

Целевая аудитория и сегментация рынка

Основными потребителями LLM в сфере кибербезопасности являются:

* Финансовый сектор: Банки и финансовые учреждения используют LLM для обнаружения мошенничества, анализа транзакций и защиты клиентских данных.
* Государственные структуры: Органы государственной власти применяют LLM для защиты критической инфраструктуры, анализа киберугроз и обеспечения национальной безопасности.
* Крупный бизнес: Корпорации внедряют LLM для защиты корпоративных сетей, предотвращения утечек данных и управления рисками.

Отрасли, использующие LLM для кибербезопасности:

* Телекоммуникации: Использование LLM позволяет операторам связи обнаруживать аномалии в сетевом трафике и предотвращать кибератаки.
* Здравоохранение: Медицинские учреждения применяют LLM для защиты конфиденциальных данных пациентов и предотвращения несанкционированного доступа.
* Энергетика: Компании энергетического сектора используют LLM для защиты инфраструктуры от киберугроз и обеспечения стабильности поставок.

Примеры компаний внедривших LLM:

1. Microsoft

Компания Microsoft интегрировала LLM в свои продукты безопасности, такие как Microsoft Defender и Azure Sentinel. Это позволяет автоматизировать обнаружение угроз, анализировать инциденты и предоставлять рекомендации по их устранению. Использование LLM способствует повышению эффективности реагирования на кибератаки и снижению нагрузки на специалистов по безопасности.

2. IBM

IBM внедрила LLM в свою платформу кибербезопасности QRadar. Это позволяет анализировать большие объемы данных, выявлять аномалии и предсказывать потенциальные угрозы. LLM помогают улучшить точность обнаружения инцидентов и ускорить процесс реагирования на них.

3. Palo Alto Networks

Компания Palo Alto Networks использует LLM в своих решениях для предотвращения угроз, таких как Cortex XDR. LLM помогают анализировать сетевой трафик, выявлять подозрительную активность и автоматически принимать меры по ее блокировке.

4. Positive Technologies

Positive Technologies разрабатывает решения, интегрирующие LLM для повышения эффективности обнаружения и предотвращения кибератак. Использование LLM позволяет компании предоставлять клиентам более точные и своевременные данные о возможных угрозах.

5. Сбербанк

Сбербанк применяет LLM для анализа транзакций и выявления мошеннических операций. Это позволяет повысить безопасность финансовых операций и защитить клиентов от потенциальных угроз.

Эти примеры демонстрируют, как крупные компании интегрируют большие языковые модели в свои системы кибербезопасности для повышения эффективности защиты и автоматизации процессов реагирования на угрозы.

# 5. Производители

В последние годы большие языковые модели (LLM) стали ключевым инструментом в области кибербезопасности, предоставляя новые возможности для обнаружения и предотвращения угроз. Многие компании по всему миру, включая Россию, активно разрабатывают и внедряют решения на основе LLM для усиления защиты информационных систем.

Ключевые игроки на рынке LLM

*Международные компании:*

* OpenAI: Разработчик модели GPT-4, широко применяемой в инструментах кибербезопасности для анализа и генерации текстов, а также для обнаружения фишинговых атак.
* Google DeepMind: Предлагает модели, используемые для анализа больших объемов данных и выявления аномалий в сетевом трафике.
* Microsoft: Интегрирует LLM в свои продукты безопасности, такие как Microsoft Defender, для улучшения обнаружения угроз и автоматизации ответных мер.

*Российские компании:*

* Positive Technologies: Активно исследует применение LLM в своих продуктах, таких как MaxPatrol SIEM, для генерации описаний процессов и анализа безопасности смарт-контрактов.
* Лаборатория Касперского: Разрабатывает решения, использующие LLM для анализа вредоносного кода и обнаружения сложных угроз.
* BI.ZONE: Внедряет технологии искусственного интеллекта и LLM для мониторинга и анализа киберугроз в реальном времени.
* Сбербанк (GigaChat): Разрабатывает собственную LLM GigaChat, которая адаптирована для обработки текстов на русском языке и может быть применена в задачах анализа угроз, автоматизации общения с клиентами и обнаружения фишинговых сообщений.
* Нейронные сети Тинькофф: Компания исследует применение языковых моделей для анализа подозрительных транзакций и обнаружения мошеннических действий.
* Центр компетенций НТИ по ИИ: Разрабатывает LLM для применения в национальных проектах, включая кибербезопасность и обработку данных в защищенных средах.

Уникальные предложения и инновации

* PentestGPT: Инструмент, использующий LLM для автоматизации процесса пентестинга, способный автономно выявлять уязвимости, включая SQL-инъекции и XSS-атаки.
* BlackMamba: Полиморфный кейлоггер, генерируемый с помощью LLM, который изменяет свою нагрузку для обхода средств обнаружения и извлекает данные через вебхуки.
* Solidity AI: Плагин для VS Code от Consensys Diligence, использующий LLM для анализа смарт-контрактов на языке Solidity, выявления уязвимостей и предоставления пояснений по коду.
* GigaChat от Сбербанка: Используется для анализа большого объема текстовых данных, обработки сообщений, проверки содержимого на наличие киберугроз и предложений по автоматизации.
* Тинькофф AI: Модели для анализа финансовых угроз, включая анализ платежей и подозрительных паттернов в клиентских действиях.
* LLMSecCode: Открытый фреймворк, разработанный для оценки способности различных LLM генерировать безопасный код и устранять уязвимости, способствуя выбору наиболее эффективных моделей для безопасной разработки.

# 6. Заказчики

Внедрение больших языковых моделей (LLM) в сферу кибербезопасности привлекает внимание различных организаций, стремящихся усилить защиту своих данных и систем. Рассмотрим профили заказчиков, их потребности и примеры успешного применения LLM в кибербезопасности.

Заказчики технологии LLM в кибербезопасности

Типичные профили заказчиков

1. Крупные компании: корпорации с обширной IT-инфраструктурой и значительными объемами данных, для которых критически важна защита от киберугроз.
2. Государственные учреждения: организации, обрабатывающие конфиденциальную информацию и обеспечивающие национальную безопасность.
3. Компании, работающие с критически важными данными: финансовые институты, медицинские организации и другие предприятия, для которых утечка данных может привести к серьезным последствиям.

Ожидания и потребности заказчиков

* Защита от утечек данных: предотвращение несанкционированного доступа и распространения конфиденциальной информации.
* Предотвращение угроз: раннее обнаружение и нейтрализация кибератак, включая эксплуатацию уязвимостей и фишинговые атаки.
* Снижение затрат на управление инцидентами безопасности: автоматизация процессов обнаружения и реагирования на инциденты для уменьшения нагрузки на команды безопасности.

Примеры внедрения LLM для кибербезопасности

1. Positive Technologies: компания разработала LLM для анализа смарт-контрактов на языке Solidity, что позволяет эффективно выявлять уязвимости и повышать безопасность блокчейн-приложений.
2. MaxPatrol SIEM: в этом решении используются LLM для генерации описаний запускаемых процессов, что помогает аналитикам безопасности быстрее идентифицировать потенциальные угрозы.
3. Symantec: компания применяет LLM для проактивного мониторинга и защиты от атак, сгенерированных с использованием искусственного интеллекта, обеспечивая надежную защиту от новых угроз.

# 7. Выводы

Большие языковые модели (LLM) оказывают значительное влияние на развитие кибербезопасности, предоставляя новые возможности для автоматизации процессов анализа угроз, обнаружения уязвимостей и предотвращения атак. Их применение позволяет значительно повысить эффективность защиты данных, сократить время реагирования на инциденты и снизить нагрузку на специалистов.

Однако, несмотря на преимущества, использование LLM сопряжено с вызовами, такими как высокая потребность в вычислительных ресурсах, сложности интерпретации результатов и риски злоупотребления моделями злоумышленниками. Для успешного внедрения важно обеспечивать постоянное обновление данных для обучения моделей, разрабатывать механизмы защиты и учитывать ограничения в ресурсах.

Развитие LLM продолжит трансформировать ландшафт кибербезопасности, особенно с учетом роста популярности облачных решений, IoT и национальных стратегий в области ИИ. Своевременная интеграция технологий и преодоление связанных рисков сделают LLM ключевым элементом защиты в современных информационных системах.

Источники:

[Brown, T. B. et al. (2020). “Language Models are Few-Shot Learners.” *NeurIPS 2020.*](https://arxiv.org/abs/2005.14165)

[Devlin, J. et al. (2018). “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.” *NAACL-HLT 2019.*](https://arxiv.org/abs/1810.04805)

[Лаборатория Касперского. Статья «Искусственный интеллект и машинное обучение в кибербезопасности»:](https://www.kaspersky.ru/blog/ai-in-cybersecurity-myths/25369/)

[Институт системного программирования РАН (ИСИ РАН). Материалы по обработке естественного языка (NLP):](http://www.ispras.ru/ru/labs/labs_nlp/)  
  
[Securelist. Публикации о методах противодействия киберугрозам с использованием ИИ и машинного обучения:](https://securelist.ru/tag/mashinnoe-obuchenie/)

[HanXiang Xu et al. "Large Language Models for Cyber Security: A Systematic Literature Review." arXiv, 2024.](https://arxiv.org/abs/2405.04760)

[Mohamed Amine Ferrag et al. "Generative AI and Large Language Models for Cyber Security: All Insights You Need." arXiv, 2024.](https://arxiv.org/abs/2405.12750)

[Farzad Nourmohammadzadeh Motlagh et al. "Large Language Models in Cybersecurity: State-of-the-Art." arXiv, 2024.](https://arxiv.org/abs/2402.00891)

[Positive Technologies. "Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть первая."](https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pervaya/)

[Secuteck. "Анализ и прогнозирование уязвимостей с помощью искусственного интеллекта и больших языковых моделей."](https://www.secuteck.ru/articles/analiz-i-prognozirovanie-uyazvimostej-s-pomoshchyu-iskusstvennogo-intellekta-i-bolshih-yazykovyh-modelej)

[Как искусственный интеллект используется в анализе больших данных?](https://bindata.ru/article/4063)

[Применение искусственного интеллекта в анализе данных: обзор текущего состояния и будущих направлений](https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-v-analize-dannyh-obzor-tekuschego-sostoyaniya-i-buduschih-napravleniy)

[Борьба с мошенничеством и кибератаками на основе данных](https://aismarthub.ru/articles/view/iskusstvennyy-intellekt-i-big-data-kak-analizirovat-ogromnye-obyemy-informatsii)

[Как искусственный интеллект используется в анализе больших данных?](https://bindata.ru/article/4063)

[Применение искусственного интеллекта в анализе данных: обзор текущего состояния и будущих направлений](https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-v-analize-dannyh-obzor-tekuschego-sostoyaniya-i-buduschih-napravleniy)

[Anomaly detection optimization using big data and deep learning to reduce false-positive](https://arxiv.org/abs/2209.13965)

[Борьба с мошенничеством и кибератаками на основе данных](https://aismarthub.ru/articles/view/iskusstvennyy-intellekt-i-big-data-kak-analizirovat-ogromnye-obyemy-informatsii)

[Большие языковые модели и кибербезопасность](https://www.itweek.ru/ai/article/detail.php?ID=227909)

[«Лаборатория Касперского»: как ИИ продолжит влиять на кибербезопасность в 2024 году](https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-kak-ii-prodolzhit-vliyat-na-kiberbezopasnost-v-2024-godu)

[Применение технологий искусственного интеллекта в сфере кибербезопасности](https://scienceforum.ru/2021/article/2018025215)

[Анализ и прогнозирование уязвимостей с помощью искусственного интеллекта и больших языковых моделей](https://www.secuteck.ru/articles/analiz-i-prognozirovanie-uyazvimostej-s-pomoshchyu-iskusstvennogo-intellekta-i-bolshih-yazykovyh-modelej)

[Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть первая](https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pervaya/)

[Прогноз развития рынка кибербезопасности в Российской Федерации на 2024–2028 годы](https://www.csr.ru/ru/news/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2024-2028-gody/)

[Уязвимости и угрозы безопасности, с которыми сталкиваются большие языковые модели](https://www.unite.ai/ru/%D1%83%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B8-%D0%B8-%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D1%8B-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8%2C-%D1%81-%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%BC%D0%B8-%D1%81%D1%82%D0%B0%D0%BB%D0%BA%D0%B8%D0%B2%D0%B0%D1%8E%D1%82%D1%81%D1%8F-%D0%B1%D0%BE%D0%BB%D1%8C%D1%88%D0%B8%D0%B5-%D1%8F%D0%B7%D1%8B%D0%BA%D0%BE%D0%B2%D1%8B%D0%B5-%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D0%B8/)

[Большие языковые модели в кибербезопасности: современное состояние](https://newsletter.radensa.ru/wp-content/uploads/2024/02/2402.00891.de_.ru_.pdf)

[AI на фронтире кибервойны. Как LLM меняют ИБ-ландшафт](https://habr.com/ru/companies/bastion/articles/856180/)

[Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть первая](https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pervaya/)

[Обеспечение информационной безопасности в крупных компаниях — ключевые стратегии](https://sber.pro/digital/publication/tsifrovaya-bronya-osnovnie-strategii-informatsionnoi-bezopasnosti-dlya-krupnogo-biznesa/)

[AI на фронтире кибервойны. Как LLM меняют ИБ-ландшафт](https://habr.com/ru/companies/bastion/articles/856180/)

[LLM в кибербезопасности: на пути к AI-ассистенту](https://ptresearch.media/articles/llm-v-kiberbezopasnosti-na-puti-k-ai-assistentu)

[Как мы обучали LLM для поиска уязвимостей в смарт-контрактах Solidity](https://habr.com/ru/companies/pt/articles/860476/)

[LLMSecCode: инновационный фреймворк для оценки безопасных возможностей кодирования LLMs](https://saile.ru/%D1%84%D1%80%D0%B5%D0%B9%D0%BC%D0%B2%D0%BE%D1%80%D0%BA-%D0%B4%D0%BB%D1%8F-%D0%BE%D1%86%D0%B5%D0%BD%D0%BA%D0%B8-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%BA%D0%BE/)

[Как отечественные разработчики отвечают на вызовы кибербезопасности](https://www.rbc.ru/technology_and_media/28/11/2024/674450b39a794747b8cb31fd)

[Positive Technologies на Habr](https://habr.com/ru/companies/pt/articles/860476/?utm_source=chatgpt.com)

[MaxPatrol SIEM - PT Research](https://ptresearch.media/articles/llm-v-kiberbezopasnosti-na-puti-k-ai-assistentu?utm_source=chatgpt.com)

[Symante](https://oberig-it.com/ru/stati/obzor-sredstv-zashhity-symantec-proaktivno-otslezhivaet-i-zashhishhaet-ot-llm-atak/?utm_source=chatgpt.com)

[c и LLM-защита - Oberig IT](https://oberig-it.com/ru/stati/obzor-sredstv-zashhity-symantec-proaktivno-otslezhivaet-i-zashhishhaet-ot-llm-atak/?utm_source=chatgpt.com)