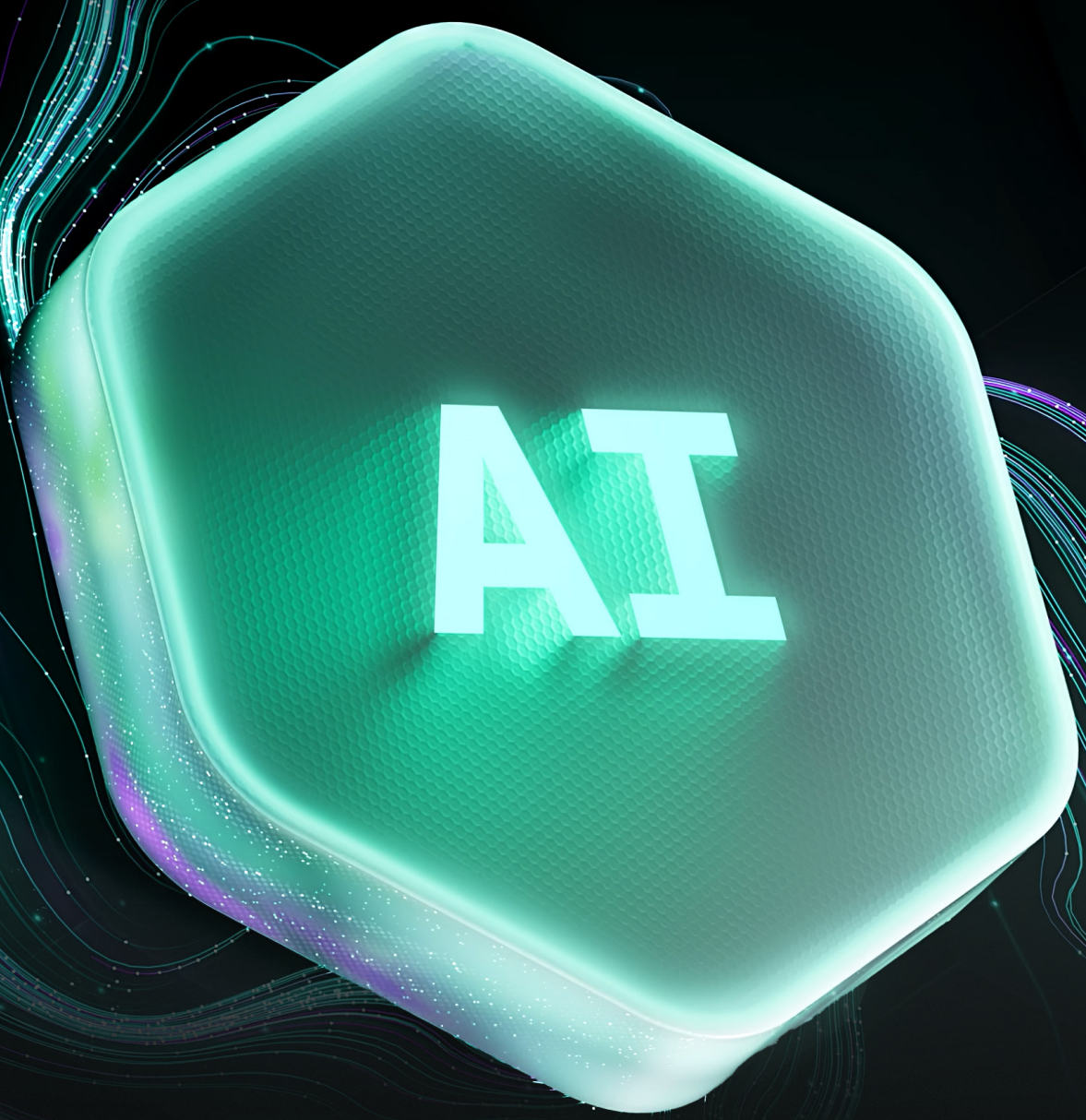




AI

Как ИИ делает решения Kaspersky еще эффективнее

Наш путь в области ИИ начался еще в 2005 году. Задолго до нынешнего всплеска интереса к технологиям искусственного интеллекта мы уже использовали машинное обучение для решения ключевых задач кибербезопасности. Сегодня этот опыт обеспечивает нам значительное конкурентное преимущество в детектировании угроз.

ИИ — это инструмент. Наша экспертиза — то, что делает его эффективным

Вокруг темы искусственного интеллекта сегодня существует значительный информационный шум. Каждый поставщик обещает решение проблем безопасности с помощью ИИ как по волшебству.

Подход Kaspersky отличается. Мы рассматриваем ИИ не как универсальное решение всех проблем, а как мощный практический инструмент, который должен создаваться на основе достоверных данных и глубокой человеческой экспертизы.



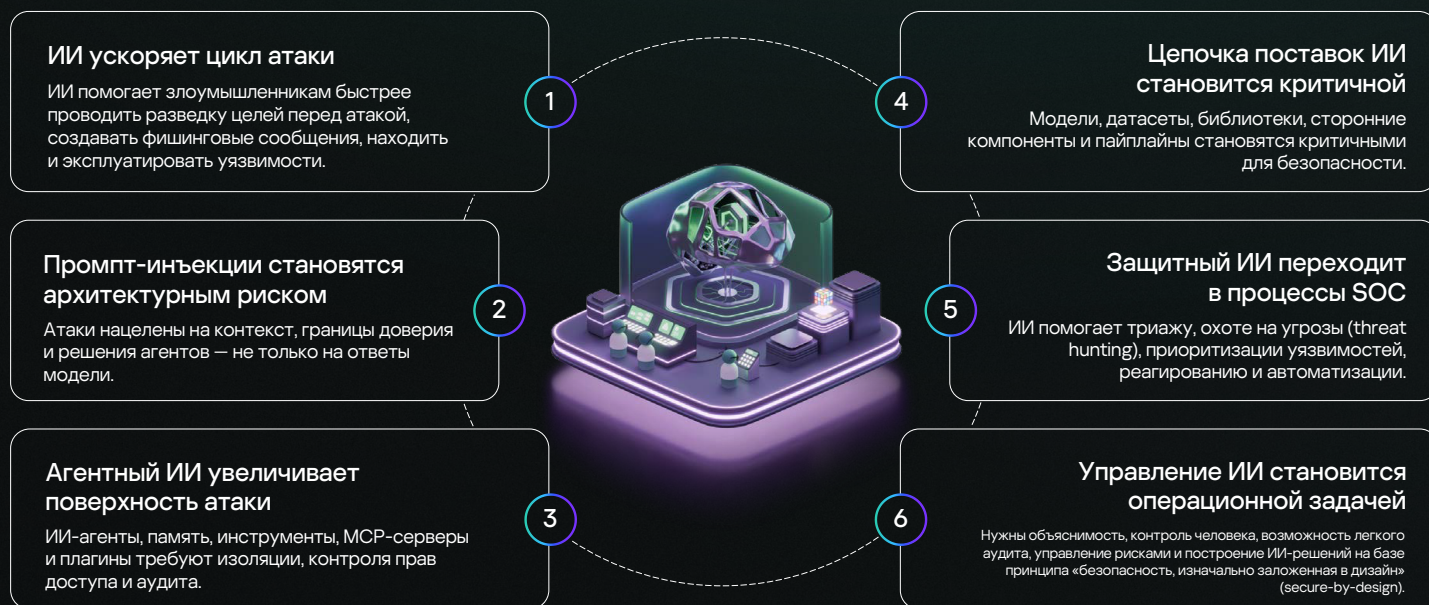
Искусственный интеллект становится частью практически каждого уровня цифровой среды —

от пользовательских приложений и программной разработки до инфраструктуры и операций обеспечения кибербезопасности.

ИИ меняет не только инструменты защиты. Он меняет саму стратегию кибербезопасности.

Влияние ИИ на кибербезопасность уже не сводится к отдельному классу «угроз для ИИ». Он ускоряет привычные атаки, создает новые точки входа в ИИ-системах и цепочках их поставок — и в то же время дает защитникам новые возможности для обнаружения, анализа и реагирования.

ИИ-тренды, меняющие ландшафт кибербезопасности



Новая реальность требует решать две задачи одновременно:

Использовать возможности ИИ для повышения эффективности защиты — и обеспечивать безопасность самих ИИ-систем, данных и процессов вокруг них. Именно поэтому стратегия Kaspersky развивается в двух взаимодополняющих направлениях:

- Кибербезопасность, усиленная ИИ
- Безопасность систем, использующих ИИ



Наша стратегия в области ИИ: два ключевых направления

Мы строим наши исследования и разработки мирового уровня в области искусственного интеллекта вокруг двух важнейших задач.

ИИ — в нашей ДНК

- Собственный Центр исследования технологий искусственного интеллекта Kaspersky (AI Technology Research Center)
- **Более 20 лет** инноваций в области ИИ
- Мы изучаем угрозы, связанные с ИИ, столько же времени, сколько используем **ИИ для защиты**



Мониторинг ландшафта угроз, связанных с ИИ

Почти 30-летний опыт исследования киберугроз позволяет нам отделять реальные риски от информационного шума и эффективно противодействовать угрозам:

- Отслеживать мошенников, использующих ажиотаж вокруг ИИ
- Анализировать, как киберпреступники применяют ИИ для ускорения и масштабирования своих атак
- Прогнозировать развитие угроз, связанных с ИИ, чтобы создавать более эффективную защиту
- Защищать собственные системы от угроз, использующих ИИ или нацеленных на наши ИИ-алгоритмы



Кибербезопасность, усиленная ИИ

Мы используем искусственный интеллект для защиты организаций от полного спектра угроз — от массового вредоносного ПО до сложных атак нового поколения, также использующих возможности ИИ.



Безопасность систем, использующих ИИ

Внедрение ИИ в организациях дает много преимуществ — но одновременно увеличивает поверхность атаки, и создает новые вызовы для безопасности.

Kaspersky AI CERT развивает способы обеспечения безопасности ИИ-систем — от больших языковых моделей (LLM) до промышленных решений — перед лицом таких новых угроз, как:

- состязательные атаки, включающие промпт-инъекции (prompt injections)
- отравление данных (data poisoning)
- кража моделей (model theft)
- компрометация цепочки поставок (supply chain compromise)

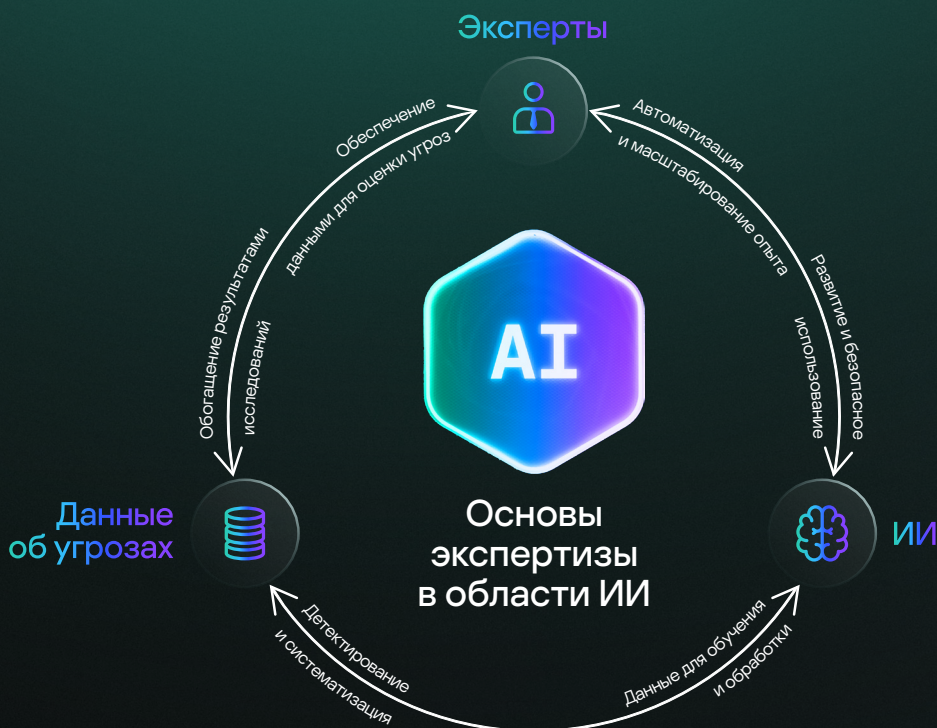
Также отслеживание потоков данных Kaspersky Open Source Threat Data Feeds позволяет заранее знать о небезопасных или скомпрометированных open-source-компонентах ИИ-решений и не использовать их в инфраструктуре организации.



Подтвержденная экспертиза в области ИИ:

- **Технологическая база:**
Kaspersky — держатель более **130 патентов** в сфере ИИ
- **Международное признание:**
участие в инициативе EU AI Pact
- **Практический вклад:**
разработка AI Secure Development Guidelines — рекомендаций по безопасной разработке ИИ-систем
- **Доказанная эффективность:**
ИИ-механизмы обнаружения угроз помогают продуктам Kaspersky стабильно показывать высокие результаты год за годом

Основа нашего подхода: данные, экспертиза и ИИ



Эффективность искусственного интеллекта напрямую зависит от качества данных и экспертизы специалистов, стоящих за ним.

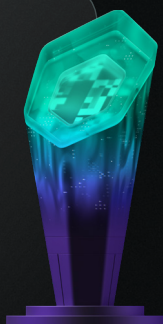
Kaspersky Security Network (KSN) непрерывно обрабатывает обезличенную глобальную угрозную телеметрию, которая постоянно обогащается результатами работы экспертов по исследованию угроз и специалистов по реагированию на инциденты.

Этот безостановочно работающий цикл позволяет нашим ИИ-моделям оставаться устойчивыми, точными и актуальными перед лицом новых угроз.

TOP 3

Максимум независимых тестов. Максимум подтвержденной защиты.*

[Подробнее](#)



* Эффективность решений Kaspersky уже много лет подтверждается высокими результатами независимых тестирований и сравнительными оценками.

ИИ в действии: усиление защиты и оптимизация процессов в центрах обеспечения кибербезопасности (SecOps)



Более 500 000 новых
угроз ежедневно

Kaspersky обнаруживает
вредоносные объекты

1 ИИ для обнаружения угроз — незаметный, но критически важный элемент защиты

Многоуровневый стек технологий искусственного интеллекта встроен в каждое наше решение для защиты IT- и OT-инфраструктуры. Значительная его часть работает незаметно для пользователя, блокируя вредоносное ПО, программы-вымогатели, фишинг и другие используемые в кибератаках инструменты еще до того, как они смогут навредить бизнесу.

Наш подход сочетает модели искусственного интеллекта и машинного обучения, обученные на статических, поведенческих и статистических признаках, работающие как в облаке, так и локально в инфраструктуре заказчика.

Это обеспечивает максимально эффективное обнаружение новых угроз без опоры исключительно на облачные сервисы.



Kaspersky
Corporate
CyberSecurity



Выявление
угроз
с помощью ИИ



Kaspersky
OT CyberSecurity

2 ИИ-автоматизация операций обеспечения кибербезопасности

На рынке ощущается острая нехватка специалистов по кибербезопасности. Аналитики SOC не успевают обрабатывать непрерывный поток оповещений. Наш набор ИИ-технологий для SecOps — это мощные инструменты, с которыми аналитики могут быстрее обнаруживать угрозы, эффективнее проводить расследования и результативно реагировать на инциденты.

2.1 Автоматизированное выявление аномалий с помощью ИИ

Обнаружение подмены DLL-библиотек

Использует глобальную анонимизированную телеметрию загрузки DLL для формирования базового профиля нормальной активности, а затем выявляет аномалии и уведомляет аналитиков.

Обнаружение компрометации учетной записи

Изучает нормальное поведение учетной записи в течение базового периода для обнаружения аномалий.

ИИ-приоритизация алертов

Моделирует нормальную активность хостов, выявляет нетипичные цепочки событий, которые могут свидетельствовать о компрометации, и автоматически расставляет приоритеты, помогая аналитикам сократить объем информационного шума и сосредоточиться на наиболее важных угрозах.

Роль ИИ в работе управляемого обнаружения и реагирования (MDR)

Технология «ИИ-автоаналитик» (AI Auto-Analyst) автоматически отсеивает малозначимые оповещения, позволяя аналитикам работать эффективнее и сокращая среднее время реагирования на инциденты (MTTR). Согласно статистике сервиса Kaspersky MDR, данная технология снижает нагрузку на экспертов SOC «Лаборатории Касперского» **на 25%**.



Kaspersky
Symphony
XDR



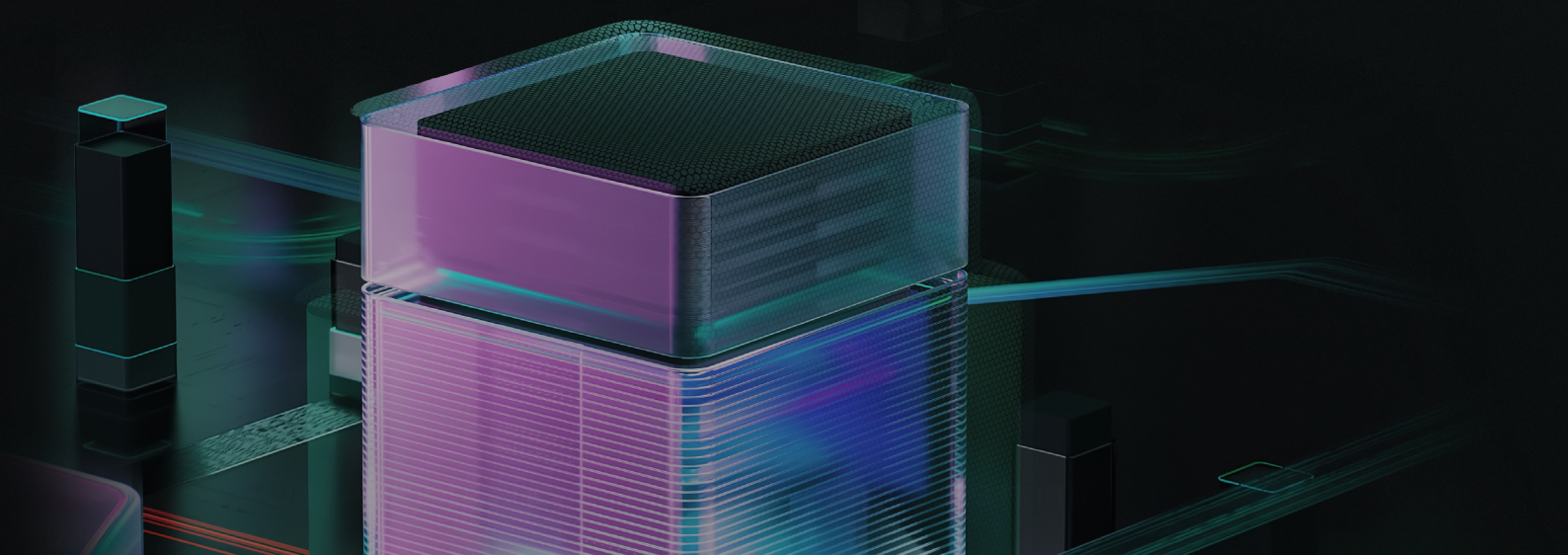
Kaspersky
Unified Monitoring
and Analysis Platform



Kaspersky
Managed Detection
and Response



Kaspersky
Managed Detection
and Response



2.2 Помощь GenAI в проведении операций по обеспечению безопасности

KIRA: ваш GenAI-помощник для SecOps

Kaspersky Investigation and Response Assistant (KIRA) — это семейство инструментов на базе генеративного ИИ (GenAI), предназначенных для обеспечения безопасности. KIRA может подключаться к любой внешней или локальной большой языковой модели (LLM), совместимой с OpenAI. В качестве альтернативы доступно готовое решение на базе отечественной большой языковой модели.

Резюме содержания алерта или инцидента

Дает описание всей цепочки атаки на понятном языке одним нажатием.

Разъяснение содержимого командной строки

Расшифровывает сложные и специально запутанные командные строки, позволяя за считанные секунды понять, что они делают.

Триаж инцидентов с использованием естественного языка

Позволяет вводить запросы обычном языке, снижая требования к квалификации SOC-аналитиков.

Сводка результатов сканирования образов контейнеров

Предоставляет отчет на основе анализа образа, включающий его назначение, а также потенциальные риски и ошибки конфигурации.

Анализ OSINT-данных об угрозах (TI) с помощью GenAI

ИИ-ассистент может анализировать большие объемы OSINT-данных, а затем преобразовывать их в сжатые и понятные отчеты, помогая специалистам быстрее понимать ситуацию и эффективнее реагировать на инциденты.



Kaspersky
Symphony
XDR



Kaspersky
Unified Monitoring
and Analysis Platform



Kaspersky
Endpoint Detection
and Response
Expert



Kaspersky
Container
Security



Kaspersky
Threat Intelligence
Portal



Кибербезопасность на базе ИИ. Опережая киберугрозы.



[Подробнее](#)

www.kaspersky.ru

© 2026 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

[#kaspersky](#)
[#активируйбудущее](#)