kaspersky

ИИ для кибербезопасности: опыт, проверенный временем

Эффективные решения
без пустых обещаний

kaspersky.ru

Введение

Искусственный интеллект, в частности машинное обучение, использовался «за кадром» для решения разнообразных задач задолго до появления ChatGPT. Современные компании рассматривают ИИ как инструмент для повышения прибыльности — и игнорировать такую перспективу было бы недальновидно.

И это особенно очевидно в кибербезопасности — отрасли, которую можно по праву считать естественным спутником ИИ. На рынок выводится все больше продуктов на базе ИИ «нового поколения», и появление каждого сопровождается громкими маркетинговыми заявлениями. Вендоры уверены, что их продукты (даже самые тривиальные) будут пользоваться исключительно высоким спросом. И небезосновательно: 94% компаний считают, что без интеллектуальных защитных решений уже не обойтись[1]. Но способны ли данные вендоры на деле выполнить заявленное? И действительно ли их продукты способны укрепить безопасность? Из этой брошюры вы узнаете о нескольких ключевых ИИ-технологиях, которые мы разработали за последние 20 лет, и уникальных знаниях, которые позволяют нам создавать действительно нужные бизнесу продукты. Надеемся, эти данные пригодятся вам, чтобы спокойно и обдуманно подойти к вопросу приобретения защитного решения.

Искусственный интеллект (ИИ) вступает в период стремительного развития, постепенно становясь неотъемлемой частью нашей реальности. И хотя технологический прорыв происходит на наших глазах, сама идея ИИ давно присутствует в культурном пространстве. Книги и кинематограф — от «Матрицы» до «Мира Дикого Запада» — на протяжении десятилетий формировали наше восприятие этой технологии. Она завораживает и порой даже пугает, не оставляя равнодушным никого.

Но одно дело — фантастика, и совсем другое — реальность. В повседневной жизни, а особенно в бизнесе, мы сталкиваемся с не менее впечатляющими сценариями применения ИИ.

ИИ в кибербезопасности: мифы и реальность

Во второй половине прошлого десятилетия ИИ активно позиционировался как единственный подход, который способен справиться с новыми и продвинутыми киберугрозами. Но это верно лишь отчасти — не стоит ожидать от него невозможного. На самом деле ИИ развивается постепенно, и мы находимся только в начале этого пути. Важно помнить и о другой стороне медали: **эту же технологию используют и злоумышленники,** которые осваивают ее значительно быстрее, часто игнорируя законы и нормы морали.

Пока ИИ не оказал большого влияния на методы и тактики атакующих, но тем не менее мы видим, что он заметно повышает эффективность атак: упрощая планирование, он позволяет проводить их чаще — и для этого не нужны глубокие познания в программировании.

Но стремительный рост киберпреступности — лишь одна из причин, по которым вендоры столь активно внедряют новую технологию в свои продукты. Вторая причина кроется в недостатке специалистов по ИБ и стремлении компаний найти решения, способные хотя бы частично закрыть пробелы в безопасности. В условиях кадрового голода, когда опытных специалистов не хватает, а услуги доступных экспертов обходятся крайне дорого, такое решение выглядит вполне закономерным.

> Хорошая новость состоит в том, что мы используем ИИ для обнаружения вредоносного ПО. Плохая новость — в том, что преступники тоже используют его в своих целях[2].
>
> **Евгений Касперский**
>
> Основатель и генеральный директор «Лаборатории Касперского»

[1] Kaspersky. (2024). Cyber defense & AI: Are you ready to protect your organization? Kaspersky

[2] И. Рубио, Е. Касперский: 'The good news is that we use AI to detect malware. The bad news is that criminals also use it'. El Pais (англ.), 2024 г.

Решения, которые позиционируются как универсальные, на самом деле таковыми **не являются** и вряд ли принесут бизнесу ощутимую пользу в части соблюдения требований, обеспечения непрерывности процессов и выполнения других важных задач.

У 48% компаний на поиски нового сотрудника уходит более полугода, а в 46% компаний новички, впервые занявшие должность специалиста по ИБ, смогли сформировать уверенные профессиональные навыки, только проработав на новом месте год или больше[3].

Таким образом, даже те компании, которые предлагают самые высокие зарплаты, не могут нанять опытных технических специалистов. Что же в таком случае остается делать компаниям с более скромным бюджетом? Конечно же, искать альтернативу, доступную здесь и сейчас.

Но к выбору решений на базе ИИ следует подходить осторожно. И не только потому, что не все заявленные возможности соответствуют реальности: злоумышленники тоже осваивают ИИ, и некачественное или небезопасное решение может создать ложное чувство защищённости или новые уязвимости. Несмотря на заметный прогресс, мы еще не знакомы со всем потенциалом этой технологии, который может раскрыться как на стороне защиты, так и на стороне нападения.

Однако ведущие вендоры действительно уже давно используют ИИ в своих решениях. Вот какие задачи они решают:

Автоматический сбор артефактов и метаданных с последующей обработкой для создания эффективных моделей ИИ и машинного обучения, предназначенных для выявления угроз, подготовки аналитических данных о них и ответных мер

Объяснение сути и уровня опасности угроз и уязвимостей с рекомендациями по дальнейшим действиям

Уменьшение влияния человеческого фактора на безопасность и снижение нагрузки на аналитиков

Сочетание профессионализма экспертов и защитных технологий на основе ИИ откроет для бизнеса гораздо больше преимуществ, чем революционные продукты, которые опираются исключительно на вычислительные методы.

Качественные защитные решения позволяют компаниям не только отражать атаки, с которыми они раньше не сталкивались, но и снижать усталость сотрудников, повышая их продуктивность, а также быстрее реагировать на инциденты.

Для создания полностью автоматизированного центра мониторинга и реагирования (SOC) машинам нужно научиться переосмысливать ситуации, оперируя абстрактными понятиями. ИИ еще только развивает свои творческие возможности и способность к критическому мышлению, поэтому **ключевую роль в интерпретации данных по-прежнему играет человек,** даже если рутинную часть работы выполняет машина.

[3] The portrait of modern information security professional». «Kaspersky blog daily», 2024 г.

Обнаружение нового вредоносного ПО

Ежедневно мы с помощью ИИ анализируем и классифицируем **более 500 000** вредоносных образцов, опираясь на обширные данные о новейших угрозах из реальной среды. Эта непрерывная работа позволяет эффективно защищать ваш бизнес и оставаться на шаг впереди киберугроз.

в 24%

всех мировых атак был зафиксирован фишинг (2024 г.)[4]

ИИ в кибербезопасности: наш опыт — ваши возможности

Вот уже два десятилетия мы интегрируем ИИ-компоненты — в частности, машинное обучение — в наши продукты, непрерывно повышая уровень защиты пользователей. Обширные знания и богатый опыт применения ИИ-технологий в кибербезопасности в сочетании с уникальными наборами данных, эффективными методами и передовыми платформами для обучения моделей позволяют нам создавать продукты для решения сложных бизнес-задач.

Например, ИИ-аналитик в Kaspersky Managed Detection and Response (MDR) автоматически отсеивает ложные срабатывания и обеспечивает быстрое реагирование, снижая нагрузку на экспертов SOC и предотвращая выгорание. А решение для прогнозной аналитики Kaspersky Machine Learning for Anomaly Detection (MLAD) анализирует телеметрию и распознает ранние признаки возможного отказа оборудования, сбоев процессов, человеческих ошибок или кибератак, сокращая периоды простоя на промышленных предприятиях.

Ниже рассмотрены другие возможности наших решений, которые усиливают безопасность компаний по всему миру.

Быстрое расследование инцидентов

В 2025 году наши ИИ-технологии обработали **более 95 000 оповещений** в сервисе Kaspersky Managed Detection and Response — они проверили инциденты и отреагировали на них, не требуя вмешательства специалистов, что наглядно демонстрирует эффективность интеллектуальной автоматизации.

Надежная защита от распространенных угроз

На сегодняшний день наши антифишинговые технологии, в том числе на базе ML, заблокировали **более 67 миллионов** фишинговых атак, защитив наших клиентов от одной из самых распространенных угроз.

Оперативный анализ текущего ландшафта угроз

Благодаря автоматической генерации записей об обнаруженных событиях безопасности на основе деревьев решений мы обнаруживаем **десятки тысяч новых вредоносных программ ежедневно.** Мгновенный анализ угроз позволяет нам оставаться на шаг впереди киберпреступников — а значит, и вам тоже.

Приведем конкретный пример. ИИ существенно сокращает время обнаружения атак типа DLL Hijacking, когда легитимное приложение, под влиянием действий злоумышленников, загружает вредоносную динамическую библиотеку. Хакеры внедряют в систему уязвимое легитимное ПО вместе с вредоносной DLL. При запуске ПО не проверяет легитимность библиотеки и загружает ее просто по имени, что приводит к выполнению вредоносного кода в контексте легитимного приложения.

Эта техника крайне сложна для обнаружения традиционными методами. Наш ИИ выявляет такие атаки, анализируя параметры запуска и работы программ, распознавая случаи, когда легитимное ПО взаимодействует с вредоносной библиотекой. Благодаря этому эффективность обнаружения значительно возрастает, а решения компании заметно опережают традиционные подходы.

[4] Аналитический отчет Managed Detection and Response, 2024 г.

Почему мы это делаем?

Потому что кибербезопасность — это командная игра. Знания, остающиеся за закрытыми дверями, не помогают формировать цифровую среду. А наша цель — сделать ее надежной и безопасной для бизнеса.

Активное использование автоматизации и ИИ для предотвращения угроз снижает расходы компаний в среднем на $2,2 млн.[5]

Надежная защита мобильных устройств

В 2024 году наша облачная ИИ-технология Cloud ML for Android остановила более 6 миллионов атак на пользователей наших мобильных продуктов. Анализируя набор уникальных атрибутов, она способна обнаруживать даже прежде неизвестные вредоносные приложения для Android в режиме реального времени. Таким образом, пользователи мобильных устройств могут быть уверены: как бы быстро ни развивались угрозы, мы всегда готовы им противостоять.

Более 100 патентов по всему миру

За годы работы мы накопили серьезную технологическую базу: сегодня в нашем портфеле более ста патентов по всему миру. Большая их часть связана с методами обнаружения угроз — от выявления вредоносных программ на основе анализа поведенческих журналов до определения вредоносных серверов по телеметрическим данным. Однако наше портфолио значительно шире. Мы также создаем технологии, которые помогают улучшать качество данных для обучения моделей, находить аномалии в инфраструктуре и даже выявлять подозрительные контакты на детских устройствах в рамках родительского контроля.

Для нас патенты — это не просто формальный показатель, а практические инструменты, которые ежедневно работают на защиту клиентов. При этом мы убеждены, что знания должны приносить пользу шире, чем рамки одного продукта. Поэтому делимся исследованиями с профессиональным сообществом: представляем их на конференциях по машинному обучению и информационной безопасности, публикуем на профильных площадках. В открытом доступе можно найти даже работы, посвященные анализу безопасности наших собственных алгоритмов.

Ответственное использование ИИ: задаем стандарты

Безопасность ИИ — общее преимущество

Безопасность разработки и применения ИИ-технологий для нас — не формальность, а часть долгосрочной стратегии. Алгоритмы, которые мы создаем, должны быть надежными, устойчивыми и действительно соответствовать тем задачам, для которых они предназначены. При этом они работают не только на нас, но и на наших клиентов — а значит, от их качества напрямую зависит устойчивость и безопасность бизнеса. Именно поэтому процесс обучения моделей выстроен в соответствии со строгими требованиями безопасности: они защищены от внешнего вмешательства, а результаты их работы невозможно искусственно исказить.

Такой подход помогает нам соответствовать ожиданиям рынка в части прозрачности, этики и нормативного регулирования. В результате наши решения уверенно применяются в компаниях из отраслей с повышенными требованиями к безопасности — там, где доверие и контроль имеют принципиальное значение.

[5] IBM. (2024). Cost of a Data Brach Report 2024. IBM.

Мы обладаем большим опытом практических исследований в следующих областях:

Использование передовых технологий, например больших языковых моделей, для обнаружения угроз в системных журналах и фишинговых ссылках

Безопасность генеративного ИИ, включая защиту приватности

Использование наших технологий в центрах мониторинга и реагирования

Использование ИИ злоумышленниками

Атаки на LLM-системы

Мы понимаем, что доверие нельзя завоевать одними словами. Поэтому регулярно делимся тем, как устроены наши внутренние процессы: рассказываем о подходах к обучению моделей и о том, как оцениваем их эффективность.

Для нас доверие — это не просто слово, а главный ориентир в том, что мы делаем каждый день.

Наша ключевая задача — сделать искусственный интеллект безопасным для всех

Шесть принципов этичного использования ИИ

Мы хотим, чтобы наши ИИ-технологии были безопасными уже с начала их разработки, поэтому сформулировали шесть принципов этичного использования ИИ в кибербезопасности, представив их на форуме ООН по управлению интернетом в 2023 году[6]. Мы считаем, что наша отрасль должна служить примером и задавать стандарты этичного и безопасного использования ИИ для защиты не только бизнеса, но и каждого человека.

Мы стремимся предвидеть возможные сценарии бездумного или неправильного использования ИИ и максимально предотвращать их, чтобы защитить пользователей и бизнес от потенциального вреда.

По мере того как роль ИИ в борьбе с киберугрозами продолжает расти, уверенность в безопасности его разработки становится фундаментом доверия к интеллектуальным решениям.

Наши принципы:

1. Конфиденциальность
2. Кибербезопасность как цель
3. Человеческий контроль
4. Прозрачность
5. Безопасность
6. Открытость к диалогу

[6] «Kaspersky призывает к этичному использованию ИИ в кибербезопасности» , «Kaspersky blog daily», 2023 г

«Лаборатория Касперского» подписала пакт Европейской комиссии об искусственном интеллекте,взяв на себя обязательство соответствовать требованиям будущего закона об ИИ (AI Act), который вступил в силу в 2026 году.[7]

Лидеры в обеспечении безопасности ИИ

На форуме ООН по управлению интернетом в 2024 году мы представили руководство по безопасной разработке и развертыванию ИИ-систем[8], которое поможет организациям избежать сопутствующих рисков, — в частности, в нем изложены требования безопасности, которые следует учитывать при внедрении интеллектуальных решений. Руководство содержит подробные практические советы, помогающие устранить технические недочеты и снизить операционные риски.

Они охватывают следующие направления кибербезопасности:

- Обучение и развитие культуры кибербезопасности
- Моделирование угроз и оценка рисков
- Цепочка поставок и безопасность данных
- Безопасность инфраструктуры (облака)
- Регулярное обновление и обслуживание систем безопасности
- Защита от атак, направленных на технологии ML
- Тестирование и валидация
- Соответствие международным стандартам

Центр экспертизы

В центре экспертизы Kaspersky AI Technology Research[9] специалисты по обработке данных, инженеры машинного обучения, эксперты по киберугрозам и инфраструктурным решениям совместно решают сложные задачи на стыке кибербезопасности и искусственного интеллекта. Это включает не только разработку прикладных технологий, но и исследования безопасности ИИ-алгоритмов. Выбирая наши решения, вы пользуетесь знаниями и опытом команды экспертов.

Заключение

Впечатляющие на первый взгляд функции могут не иметь практической ценности, если не учитывать, что ИИ действительно способен решать конкретные задачи в области кибербезопасности. Дефицит квалифицированных специалистов на рынке усугубляет ситуацию: у многих компаний нет собственной экспертизы, и это затрудняет оценку того, насколько предложение вендора ИИ действительно подкреплено опытом.

Однако именно экспертные знания лежат и будут лежать в основе надежных защитных решений. На протяжении двух десятилетий мы применяем ИИ для защиты клиентов, обеспечивая сохранность их финансов, данных, репутации и стабильность рабочих процессов. Практический эффект наших технологий подтверждается ежедневно: мы выявляем более 500 000 вредоносных образцов и автоматически закрываем десятки тысяч предупреждений в рамках сервиса MDR. Эффективность наших решений подтверждена многолетними независимыми тестами[10] и успешными реализациями проектов.Мы продолжаем развивать инновации в области ИИ. Так, недавно мы усилили возможности искусственного интеллекта в нашей системе управления информацией и событиями безопасности (SIEM)[11], что повышает скорость и точность обнаружения, анализа и реагирования на новые угрозы.

Подробнее о направлениях нашей экспертизы и о том, как они помогают клиентам, можно узнать на странице, посвященной Центру исследований технологий ИИ и другим экспертным центрам компании.[12]

[7] Wheeler, K. (2025, January). How Kaspersky leads AI security standards with EU AI Pact. Cyber Magazine.
[8] IGF. (2024). IGF 2024 WS #31 Cybersecurity in AI: balancing innovation and risks. IGF.
[9] «Центр экспертизы Kaspersky AI Technology Research: кто мы и чем занимаемся». «Kaspersky blog daily», 2024 г.
[10] «Показатель ТОП 3». «Лаборатория Касперского», 2024 г.
[11] Extended AI capabilities and resource visualization: great new features provided by Kaspersky SIEM. Kaspersky, 2025 г.
[12] Центры экспертизы «Лаборатории Касперского», 2024 г.

Почему нам доверяют

Решения «Лаборатории Касперского» регулярно побеждают в тестах ведущих исследовательских и аналитических компаний и не раз были признаны самыми эффективными в отрасли решениями для обнаружения угроз, расследования инцидентов и принятия ответных мер.

О «Лаборатории Касперского»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности и защиты конфиденциальности данных с 1997 года.

Наши технологии обеспечивают защиту самых важных аспектов бизнеса более 200 тысяч корпоративных клиентов.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты рабочих мест, а также ряд специализированных решений и сервисов для борьбы с комплексными и постоянно эволюционирующими киберугрозами, в том числе кибериммунные системы.

Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, которые обеспечивают безопасность бизнеса, критически важных инфраструктур, государственных учреждений и рядовых пользователей, защищая более миллиарда устройств от новейших угроз и целевых атак.

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее