kaspersky

Кибербезопасность для всех: новая эра защиты на базе ИИ

Как «Лаборатория Касперского»
делает защиту доступной для всех

kaspersky.ru

Сегодня, когда речь заходит об ИБ, **искусственный интеллект** играет двойственную роль, так как пользуется спросом и у защитников, и у злоумышленников. Последние используют его для создания более масштабных и быстрых атак. Но те же технологии позволяют компаниям усиливать защиту, автоматизировать процессы компенсировать нехватку кадров.

Важно отметить, что задача не в том, чтобы заменить экспертов, а в том, чтобы сделать высокий уровень защиты доступным еще большему числу организаций.

Именно эту концепцию «Лаборатория Касперского» реализует в своих ИИ-разработках.

> Если ИБ-специалисты хорошо делают свою работу, она будет состоять в основном из рутины – проверки журналов, учетных записей и правил, обеспечения нормативного соответствия, а также множества других несложных, но критически важных задач. Их выполнение в ручном режиме быстро приводит к выгоранию, и в результате у аналитика возникает желание сменить работу или даже профессию. Поэтому мы применяем ИИ, чтобы сократить число таких рутинных задач и снизить нагрузку на специалистов – это одна из наших целей
>
> **Илья Маркелов**
>
> руководитель направления развития единой корпоративной платформы «Лаборатории Касперского»

Ситуацию усугубляет выгорание специалистов, на которых возложено решение бесчисленных задач безопасности

Кибербезопасность на границе прошлого и будущего

Киберугрозы развиваются стремительно. Их масштаб и сложность растут с каждым годом, и даже подготовленным организациям все труднее противостоять атакам. Экспертная киберзащита больше не конкурентное преимущество — это базовое условие устойчивости бизнеса.

Однако обеспечить такой уровень защиты могут не все. Одна из причин — дефицит кадров. Опытных и квалифицированных специалистов не хватает, и даже крупным компаниям с внушительным бюджетом не всегда удается сформировать мощную ИБ-команду.

Еще до того, как ИБ (информационная безопасность) стала важнейшей функцией бизнеса, когда киберугрозы существовали, но не были столь распространенными, достаточно было пары экспертов, способных управлять базовыми антивирусами и межсетевыми экранами. Но после разрушительных атак последнего десятилетия (таких как NotPetya, WannaCry и SUNBURST) стало очевидно: базовой защиты уже недостаточно.

Кадровый голод в сфере кибербезопасности

Дефицит специалистов по информационной безопасности — глобальная проблема. Более 40% экспертов в этой области признаются, что команды в их организации «немного» или «значительно» недоукомплектованы. А половина опрошенных отмечают, что теоретические знания, полученные ими в учебном заведении, оказались бесполезными, когда дело дошло до выполнения реальных задач. Менее половины получили практический опыт во время обучения в колледже или вузе[1].

И дело не только в нехватке квалифицированных специалистов, но и в высокой стоимости их услуг – многие компании просто не могут позволить себе нанять экспертов по кибербезопасности, **а значит, и организовать собственный центр мониторинга и реагирования (SOC), который бы обеспечивал круглосуточную защиту.** С этой проблемой сталкиваются даже компании с внушительным бюджетом: 48% руководителей ИБ-отделов отмечают, что на поиски нового сотрудника уходит более полугода[1].

К сожалению, даже самые современные решения не могут защитить организацию от всех угроз — они становятся по-настоящему эффективными только в руках профессионалов, потому компания, в которой не хватает квалифицированных аналитиков, остается по-прежнему уязвимой к кибератакам.

Раньше компании могли отслеживать угрозы и реагировать на них в ручном режиме, но эти процессы становятся все менее эффективными: современные угрозы слишком сложны, а специалистов недостаточно, чтобы справиться с ними вручную. Инциденты, которые можно было обнаружить на ранних этапах, остаются незамеченными. В результате компании по всему миру несут серьезные финансовые убытки.

[1] The Portrait of Modern Information Security Professional. Kaspersky Daily, 2024 г.

Защита корпоративного уровня — для всех

«Лаборатория Касперского» работает над технологиями искусственного интеллекта уже более 20 лет, используя глобальные базы аналитических данных об угрозах и огромные объемы телеметрии для обучения моделей машинного обучения. Эти технологии выделяют наиболее критичные события среди потока оповещений, позволяя нашим клиентам сосредоточиться на действительно серьезных инцидентах.

В частности, решения «Лаборатории Касперского» регулярно обращаются к матрице MITRE ATT&CK, которая содержит обширные сведения о тактиках, техниках и методах злоумышленников, и формулируют рекомендации по реагированию, опираясь на приведенные в ней описания, а не только на базу знаний компании.

Илья Маркелов

руководитель направления развития единой корпоративной платформы «Лаборатории Касперского»

SIEM-система «Лаборатории Касперского» — еще один прекрасный пример реализации ИИ-технологий. Для того чтобы скрыть свое присутствие в системе, операторы вредоносного ПО шифруют свои команды, и в результате оператор видит в журнале событий зашифрованную строку, совершенно бессмысленную на вид. Наш ИИ-модуль расшифровывает такие команды и объясняет, что произойдет в результате выполнения сценария, на понятном пользователю языке.

Раньше операторам, обрабатывающим подобные события, приходилось сначала выполнять рутинную операцию — декодировать зашифрованную строку с помощью специального конвертера, например Base64. А затем начинался самый сложный и кропотливый процесс, который требовал специальных знаний: оператор определял природу вредоносного кода, расшифровывал его, чтобы прочесть команду, представленную, например, в виде сценария PowerShell с многочисленными параметрами, и изучал документацию PowerShell, чтобы понять, что произойдет при выполнении этого сценария.

С нашим ИИ в этом больше нет необходимости. Все, что нужно сделать администратору, чтобы узнать потенциальный результат выполнения сценария и уровень опасности угрозы, — это нажать на кнопку, чтобы наш модуль выдал ему нужную информацию.

Как и почему «Лаборатория Касперского» делает защиту корпоративного уровня доступной для всех

Компания работает с искусственным интеллектом уже долгие годы: собирает данные, экспериментирует и внедряет новые технологии в свои решения. Но эта работа теряет смысл, если ее плоды недоступны для широкой аудитории. Мы уверены, что любая организация, будь то технологический стартап, крупная больница или цифровой банк, имеет право на безопасность мирового уровня, и чем надежнее защищены отдельные организации, тем безопаснее мир в целом.

Малый и средний бизнес

Небольшим и средним компаниям зачастую не хватает ресурсов для содержания полноценной ИБ-команды. Решения «Лаборатории Касперского» на базе ИИ могут помочь таким предприятиям без вмешательства специалиста автоматически обнаруживать угрозы, включая вредоносное ПО, программы-вымогатели и фишинг. То есть они могут существенно повысить свою безопасность без найма дополнительных сотрудников.

Комментарий Ильи Маркелова:

«Наши ИИ-решения позволяют сотрудникам с даже небольшим опытом решать сложные задачи кибербезопасности. Для работы с генеративным ИИ не нужны специальные навыки: система дает подробные объяснения и советы на понятном пользователю языке — куда смотреть, что делать и что произойдет в результате выполнения той или иной команды. Она предоставляет пользователю контекст и дополнительные сведения, поэтому компания может доверить выполнение задач безопасности даже менее квалифицированным специалистам».

При этом «Лаборатория Касперского» уверена, что каждая организация вправе самостоятельно решать, как защитить себя от угроз. Но несмотря на высокий уровень автоматизации, окончательное решение всегда принимает оператор.

Доверие, прозрачность и результат

«Лаборатория Касперского» хочет, чтобы искусственный интеллект в сфере кибербезопасности приносил пользу всем. Однако без доверия к используемым решениям это невозможно. Обеспечивая безопасность разработки и применения ИИ-технологий, компания создает надежные продукты, которым можно доверить защиту бизнеса. Обучение ИИ-моделей соответствует строгим стандартам безопасности — они защищены от вредоносных манипуляций.

Крупный бизнес

В отличие от небольших компаний, у большинства крупных предприятий есть собственные команды опытных ИБ-специалистов. И искусственный интеллект «Лаборатории Касперского» призван усилить эти команды, а не заменить их.

Илья поясняет:

«Наше решение существенно снижает нагрузку на команду, одновременно повышая ее продуктивность за счет автоматизации, а работать с ним смогут даже не самые опытные специалисты. Искусственный интеллект не заменяет аналитиков — он позволяет им сосредоточиться на критических задачах, освобождая их от повседневной рутины.»

Крупные компании все чаще сталкиваются с трудностями в управлении IT-инфраструктурой — чем сложнее становятся корпоративные системы, тем более изощренно их атакуют злоумышленники. «Лаборатория Касперского» предлагает ИИ-технологии и средства автоматизации, которые повышают эффективность управления инфраструктурой без необходимости развертывания дополнительных решений и, следовательно, финансовых вложений.

Такой подход полностью отвечает ожиданиям аудитории в части этики, прозрачности и нормативного соответствия и делает ИИ-решения «Лаборатории Касперского» подходящим для организаций из строго регулируемых отраслей. Время от времени компания демонстрирует принципы своей внутренней работы, что еще больше укрепляет доверие.

Тем временем в Центре Kaspersky AI Technology Research специалисты по обработке данных, инженеры систем машинного обучения, эксперты по угрозам и развертыванию инфраструктур решают непростые задачи, возникающие на стыке кибербезопасности и искусственного интеллекта. Среди этих задач — не только разработка прикладных технологий, но и исследование безопасности ИИ-алгоритмов.

Передовые решения «Лаборатории Касперского» на основе искусственного интеллекта также отличает высокая производительность. Так, в 2025 году ИИ-технологии в сервисе Kaspersky Managed Detection and Response обработали более 95 000 оповещений[2].

Вновь слово Илье Маркелову:

«Все наши технологии регулярно проходят независимые тестирования. Решения «Лаборатории Касперского» принимают участие в многочисленных исследованиях эффективности обнаружения и реагирования и неизменно опережают конкурентов в части точности и скорости реагирования. При этом наградами отмечена вся наша линейка продуктов, а не только интеллектуальные решения.»

> Наши ИИ-модели постоянно обучаются, а эксперты анализируют результаты обучения и при необходимости корректируют их. Наш искусственный интеллект всегда предоставляет пользователям обоснование своих решений. Например, он не просто помечает безопасное событие зеленым цветом, но и объясняет, почему оно считается безопасным. Если ИИ не может принять однозначного решения, он обязательно сообщит об этом пользователю и предоставит право выбора ему.
>
> **Илья Маркелов**
>
> руководитель направления развития единой корпоративной платформы «Лаборатории Касперского»

[2] Kaspersky Security Services, Global Report «Anatomy of a Cyber World», «Лаборатория Касперского», 2026 г.

Заключение

ИИ становится необходимым инструментом кибербезопасности. Без него уже практически невозможно противостоять злоумышленникам и защищать компании с ограниченными кадровыми ресурсами. Решения «Лаборатории Касперского» на базе ИИ делают передовую защиту доступной любой компании.

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

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

#kaspersky
#активируйбудущее