

• СОВМЕСТНОЕ ОТРАСЛЕВОЕ ИССЛЕДОВАНИЕ

Тренды ИТ-рынка в контексте ИИ- безопасности

Защита ИИ в компаниях-разработчиках ПО

Сентябрь 2026

ОБРАЩЕНИЕ РУКОВОДИТЕЛЕЙ



Ренат Лашин

Исполнительный директор
АРПП «Отечественный софт»

Искусственный интеллект перестал быть экспериментом и вышел из стадии пилотов. ИИ стал органичной частью производственных процессов создания ПО. Мы провели это исследование, чтобы оценить уровень зрелости безопасности ИИ-решений.

Наша задача как ассоциации помочь разработчикам в построении доверенных ИИ-технологий и предоставить площадку для выработки практик создания безопасного ПО.



Юрий Сергеев

Генеральный директор
AppSec Solutions

Безопасность ИИ сегодня — ключевое условие защищённого контура разработки ПО. Рынок внедряет ИИ быстро и при этом осознанно принимает непокрытый риск: технология уже встроена в бизнес-процессы многих разработчиков ПО.

Уверен, что это исследование поможет читателю обратить внимание на вопросы защиты ИИ-систем в своих организациях и подготовить план действий для обеспечения кибербезопасности искусственного интеллекта.

Что именно измерялось

Исследование зрелости процессов ИИ было проведено среди компаний-разработчиков ПО — участников АРПП «Отечественный софт».

КАКИЕ КЛАССЫ ИИ ОЦЕНИВАЛИСЬ

показатель внедрения

Оценка строилась по следующим классам ИИ-систем

- 1 Большие языковые модели
- 2 Локальные языковые модели
- 3 ИИ-ассистенты кода
- 4 ИИ-агенты и мульти-агентные системы
- 5 RAG — генерация с опорой на базу знаний
- 6 Классические ML-модели

ВОСЕМЬ БАЗОВЫХ КОНТРОЛЕЙ

показатель защиты

Контроль засчитывается только при ответе «да». «Планируем» и «в проработке» не учитываются — показатель отражает практику, а не намерения.

- 1 Инвентаризация используемых ИИ-решений
- 2 Явный владелец политик безопасности ИИ
- 3 Политика взаимодействия ИИ с внешними источниками
- 4 Перечень заимствованных компонентов ИИ
- 5 Программа обучения безопасности ИИ
- 6 Безопасное управление данными обучения
- 7 Оценка угроз для ИИ-решений
- 8 Утверждённая стратегия безопасности ИИ

ПЕРИМЕТР ОПРОСА: СЕМЬ ДОМЕНОВ БЕЗОПАСНОСТИ ИИ

Безопасность LLM-приложений

Шлюз безопасности ИИ

Защита данных обучения

Безопасность ИИ-кода

Теневой ИИ

Безопасность ИИ-агентов

Управление и регуляторика

ИИ внедрён повсеместно. Контур защиты только создается

ВНЕДРЕНИЕ

100%

компаний используют ИИ. Вариант **«не используем»** не выбрал ни один респондент.

ЗАЩИТА

23%

базовых контролей безопасности ИИ внедрено в среднем. У **каждой третьей** компании — ни одного.

СТРАТЕГИЯ

19%

утвердили стратегию безопасности ИИ. Ещё **56%** отвечают «планируем».

СЛЕПАЯ ЗОНА

69%

говорят, что **атак не было**, и при этом **угрозы не оценивали**. Отсутствие инцидентов здесь означает отсутствие видимости.

БАРЬЕР №1

70%

называют главным барьером **нехватку ИБ-экспертизы в ИИ**. «Нет подходящих решений» — лишь 9%.

54 компании-разработчика ПО, 67% — создают собственные ИИ-решения

Ядро выборки — средние ИТ-компании с собственной разработкой: процессы ИБ у них уже формализованы, а выделенной функции безопасности ИИ ещё нет.

ОБЪЁМ ВЫБОРКИ

54

компаний-разработчика ПО.

УРОВЕНЬ РЕСПОНДЕНТОВ

65%

руководители технического блока: CTO/CIO, CISO, Product Owner, AppSec-лид.

СОЗДАЮТ ИИ-РЕШЕНИЯ

67%

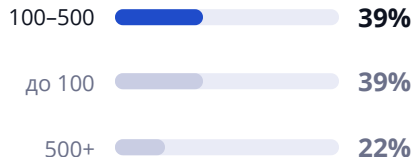
отвечают за безопасность ИИ не только внутри, но и как поставщики продукта.

ГОРИЗОНТ ВОПРОСОВ

12-24

месяца — планы по безопасности ИИ.

РАЗМЕР КОМПАНИИ, СОТРУДНИКОВ



Число разработчиков: до 50 — 46%, от 50 до 200 — 35%, свыше 200 — 19%.

РОЛЬ РЕСПОНДЕНТА

CTO / CIO	33%
Product Owner / R&D	22%
Разработчик / тех. эксперт	7%
AppSec / DevSecOps	6%
CISO и служба ИБ	4%
CEO, COO, CBDO и иные	28%

СФЕРА ДЕЯТЕЛЬНОСТИ

Бизнес-приложения и корпоративное ПО	39%
Инженерное и отраслевое ПО	20%
ИИ, данные и сервисы	13%
Информационная безопасность	9%
Системное и инфраструктурное ПО	9%
Коммуникации и телеком	6%

РАЗДЕЛ I

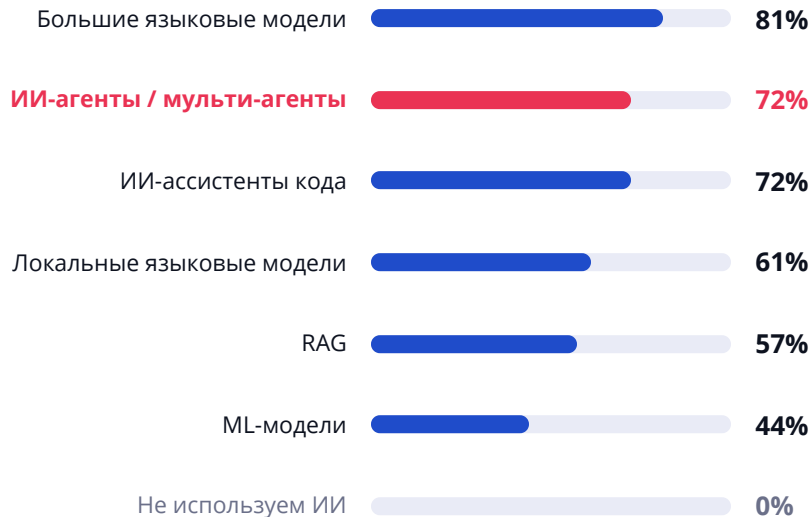
Внедрение ИИ: быстрее, чем принято считать

ИИ используют все компании выборки, и не только для текста: в стеке уже работают автономные агенты.

ИИ-агенты — второй по распространённости класс ИИ

Мультиагентные системы идут вровень с ассистентами кода и обгоняют локальные модели и RAG, что меняет профиль риска

КАКИЕ КЛАССЫ ИИ УЖЕ ИСПОЛЗУЮТСЯ · ДОЛЯ КОМПАНИЙ, N=54



● класс с автономным поведением и полномочиями

СКОЛЬКО КЛАССОВ ИСПОЛЗУЮТ ОДНОВРЕМЕННО

3,9 из 6

в среднем на компанию. Больше половины — **56%** — используют четыре класса и более.

ТЕНЕВОЙ ИИ

100%

подтверждают, что сотрудники пользуются **внешними ИИ-сервисами**: 59% — «частично», 41% — «массово».

ЧТО ЭТО ЗНАЧИТ

Ни одна компания не отрицает ни использования ИИ, ни внешних сервисов у сотрудников, что говорит о формировании нового направления для кибербезопасности - защита от теневого ИИ.

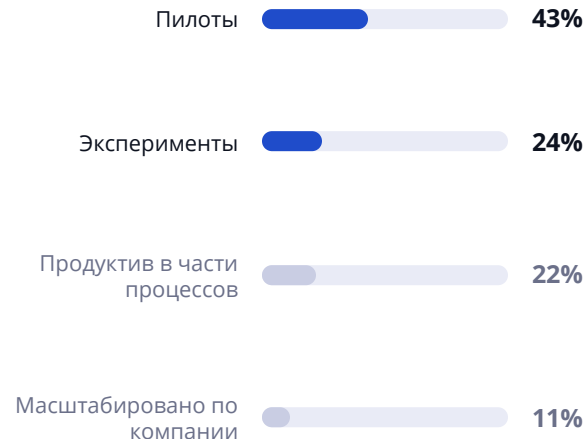
ИИ вошёл в производственный контур, но формально остался в пилотах

ГДЕ ПРИМЕНЯЕТСЯ ИИ · ДОЛЯ КОМПАНИЙ



В среднем **3,7 из 6 сценариев** на компанию. Красным — сценарий, напрямую влияющий на код продукта.

ЗАЯВЛЕННАЯ ЗРЕЛОСТЬ ВНЕДРЕНИЯ ИИ



Агенты дошли до продуктива быстрее, чем контроль

Почти четверть компаний держит ИИ-агентов в продуктивной среде. Затраты по токенам контролирует меньше половины из них.

ТЕСТИРУЮТ АГЕНТОВ

52%

компаний — на стадии тестирования ИИ-агентов.

В ПРОДУКТИВНОЙ СРЕДЕ

22%

уже эксплуатируют агентов в продуктиве.

КОНТРОЛЬ ТОКЕНОМИКИ

42%

компаний с агентами в продуктиве контролируют затраты по токенам.

ПОЧЕМУ ЭТО ВАЖНО

Агент — это не чат. У него есть полномочия, доступ к инструментам и возможность действовать без человека в цикле. Ошибка агента исполняется, а не показывается на экране.

Контроль токенов — это телеметрия агента, а не статья расходов. Расход показывает, сколько вызовов сделал агент и как менялось его поведение. Без этого нет ни базовой линии, ни способа заметить аномалию.

РАЗРЫВ КОНТРОЛЯ · ДОЛЯ КОМПАНИЙ

Агенты используются (тест или продуктив)  **74%**

Политика взаимодействия с внешними инструментами  **26%**

Контроль затрат агентов по токенам  **9%**

Оценка угроз ИИ-решений проведена  **9%**

● внедрение технологии ● контроль над технологией

74% против 9%. Технологию внедряют в восемь раз чаще, чем оценивают её угрозы.

РАЗДЕЛ II

Главный разрыв: внедрение против защиты

Разрыв измеряется двумя показателями: насколько широко в компаниях внедрён ИИ и насколько выстроена его защита по восьми базовым контролям.

Чем ближе контроль к практике, тем реже он внедрён

Инвентаризация ИИ-решений есть почти у половины компаний. Оценка угроз — контроль, который требует методологии и специалистов, — внедрена у 9%.

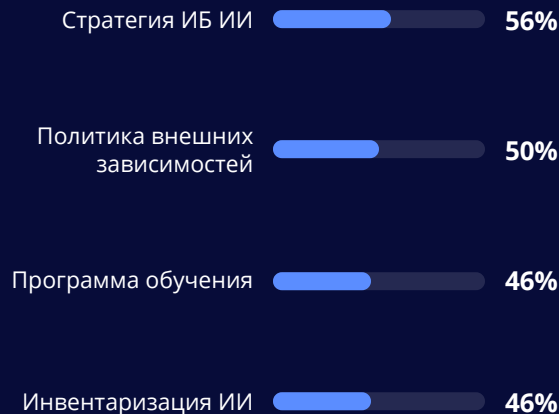
ВОСЕМЬ БАЗОВЫХ КОНТРОЛЕЙ · ДОЛЯ КОМПАНИЙ, ГДЕ КОНТРОЛЬ ВНЕДРЁН



Порог «внедрено» — только ответ «да». Ответы «планируем» и «в проработке» не засчитываются.

«ПЛАНИРУЕМ» КАК НОРМА

Доля компаний в состоянии «планируем / в проработке»:



Внедрение — 65% шкалы. Защита — 23%

Каждый показатель — доля выполненного от максимума: сколько из шести классов ИИ компания использует и сколько из восьми базовых контролей внедрила. Разрыв почти трёхкратный.

Насколько широко внедрён ИИ

в среднем 3,9 из 6 классов технологий

65%



Насколько выстроена защита ИИ

в среднем 1,9 из 8 базовых контролей

23%



ЧТО ПОКАЗЫВАЕТ РАЗРЫВ

Защита **не растёт вместе с внедрением**. Компании с четырьмя и более классами ИИ внедрились лишь немногим больше контролей, чем те, кто использует один-два класса. Чем больше ИИ в стеке, тем шире незакрытая поверхность атаки.

РАСПРЕДЕЛЕНИЕ КОМПАНИЙ ПО ЧИСЛУ ВНЕДРЁННЫХ КОНТРОЛЕЙ



72% компаний имеют не более двух контролей из восьми.

ИТ-разработчики уже фиксируют атак на ИИ

Столкнувшиеся с атаками называют промпт-инъекции в чат-ботов и модификацию клиентских приложений. При этом 91% компаний не проводили оценку угроз своих ИИ-решений — отсутствие инцидентов здесь говорит об отсутствии видимости, а не атак.

СТОЛКНУЛИСЬ С АТАКАМИ НА ИИ

4%

ответили «да». 74% — «нет», 22% — «не владею информацией».

НЕТ НИ АТАК, НИ ОЦЕНКИ УГРОЗ

69%

компаний одновременно заявляют, что атак не было и что угрозы они не оценивали.

ПОЧЕМУ ЭТО ОПАСНЕЕ ПОДТВЕРЖДЁННОГО ИНЦИДЕНТА

Ключевые атаки на ИИ — **инъекция промпта, утечка системного промпта, извлечение данных через ответы модели, отравление данных обучения** — не оставляют следов в привычной телеметрии. Они выглядят как валидный запрос с валидным ответом.

Без оценки угроз и фильтрации на шлюзе безопасности ИИ компания не может отличить нормальную работу модели от успешной атаки. Ответ «инцидентов не было» в этих условиях **ничего не измеряет**.

ЛОЖНОЕ ЧУВСТВО БЕЗОПАСНОСТИ

Считают ИИ-код безопаснее
людского (4–5)  **11%**

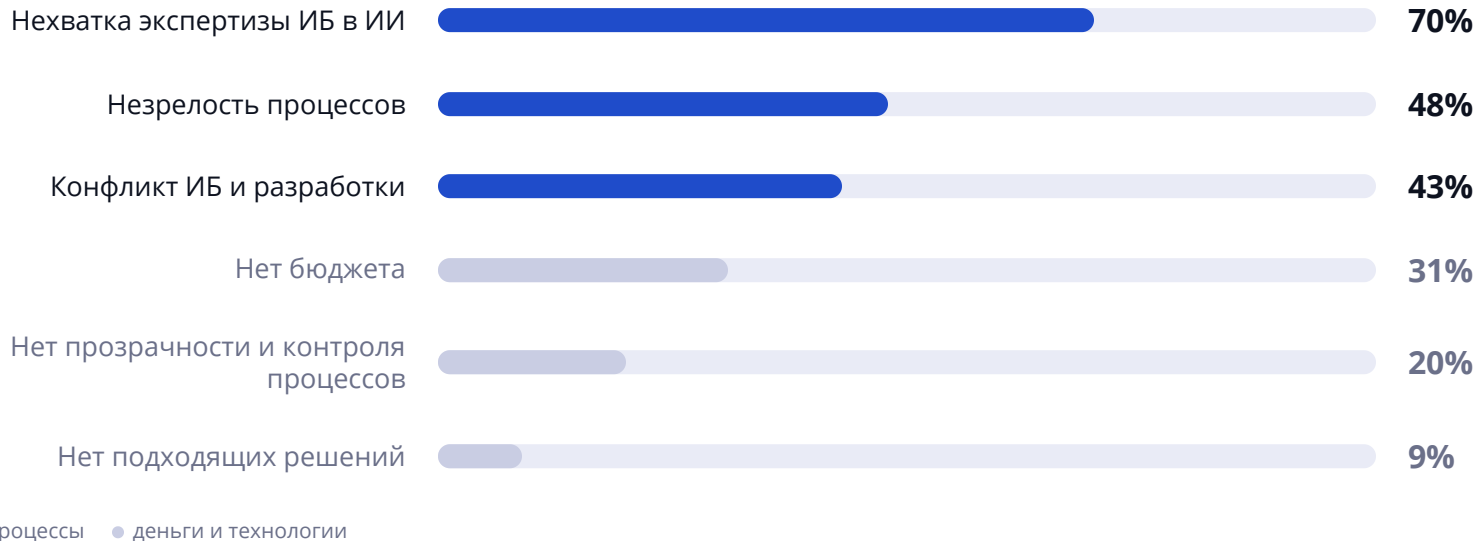
Не считают (1–2)  **44%**

Применяют ИИ в разработке кода  **81%**

Запрос рынка на квалифицированных ИИ-экспертов

Нехватка ИБ-экспертизы в ИИ — барьер №1, с почти восьмикратным отрывом от «нет подходящих решений». Спрос смещён от лицензий к компетенциям и процессам.

НАИБОЛЕЕ КРИТИЧНЫЕ БАРЬЕРЫ БЕЗОПАСНОГО ВНЕДРЕНИЯ ИИ · ДОЛЯ КОМПАНИЙ



Владелец безопасности ИИ даёт ×4,2 к зрелости контролей

ДОЛЯ ВНЕДРЁННЫХ БАЗОВЫХ КОНТРОЛЕЙ (ИЗ 7) — В СРЕДНЕМ ПО СЕГМЕНТУ

Выделенная роль или комитет · 24% выборки **48%**



CISO / служба ИБ · 11% выборки **24%**



Ответственность у СТО / CIO · 19% выборки **14%**



Размыто, нет ответственного · 46% выборки **10%**



46% выборки — в худшем сегменте. Размытая ответственность за безопасность ИИ остаётся самым частым ответом на весь опрос.

СЕГМЕНТ «НЕТ ОТВЕТСТВЕННОГО»: ЧТО ТАМ С КОНТРОЛЯМИ

КОНТРОЛЬ	ВНЕДРЁН
Оценка угроз ИИ	4%
Политика внешних зависимостей	4%
Программа обучения	4%
Стратегия безопасности ИИ	8%
Безопасное управление данными обучения	8%
Перечень заимствованных компонентов ИИ	12%
Инвентаризация ИИ-решений	28%

Создание коллегиального центра по ИИ помогает в развитии зрелости безопасных ИИ-систем

CISO / СЛУЖБА ИБ

24%

базовых контролей — вдвое меньше. ИБ видит риск, но не управляет решениями о внедрении ИИ.

СТО / CIO

14%

базовых контролей. Владелец внедрения ИИ и владелец его безопасности в одном лице — конфликт интересов.

КАК ЭТО ЧИТАТЬ

Безопасность ИИ — не подраздел ИБ. Она требует решений о данных, о закупке моделей, о правах агентов и о допустимом использовании — это полномочия за пределами службы ИБ.

СТО как владелец — худший из «назначенных» вариантов. Тот, кто отвечает за скорость внедрения ИИ, не может одновременно быть его тормозом. Один из респондентов формулирует запрос прямо: «баланс возможностей использования ИИ и ограничений ИБ».

ВТОРОЙ РАЗРЕЗ: ЗРЕЛОСТЬ ВНЕДРЕНИЯ ПРОТИВ ЗАЩИТЫ



Защита появляется только на этапе масштабирования. Компании, у которых ИИ уже в продуктивных процессах, но не масштабирован (21% контролей), защищены практически так же, как те, кто ещё в пилотах (22%). Переход из пилота в продуктив сам по себе контролей не добавляет.

Меньше всего контролей — у компаний на 100–500 человек

Зависимость защищённости от размера U-образная: у малых и крупных компаний контролей больше, чем у средних. При этом средние — самая массовая группа выборки, поэтому именно на них приходится основная часть незакрытого риска.

ДОЛЯ ВНЕДРЁННЫХ БАЗОВЫХ КОНТРОЛЕЙ (ИЗ 7) — ПО РАЗМЕРУ КОМПАНИИ

500+ человек · 22% выборки **33%**



до 100 человек · 39% выборки **20%**



100–500 человек · 39% выборки **16%**



Разница между крупными и средними — **×2,1**. Это разрез по одному признаку: размер не объясняет разрыв сам по себе, но показывает, где он сосредоточен.

ВОЗМОЖНОЕ ОБЪЯСНЕНИЕ

Малые компании держат ИИ в одних руках: контур небольшой, решения принимает основатель, теневой ИИ виден без инструментов.

Крупные компании имеют выделенную ИБ и формальные процедуры допуска технологий.

Средние уже потеряли обозримость малых, но ещё не выстроили процессы крупных. ИИ внедряют десятки команд, а владельца безопасности ИИ ещё нет.

РАЗДЕЛ III

Что данные означают для отдельной компании и для отрасли в целом

Как обеспечить безопасность ИИ

Порядок задан данными: сначала организационные решения с кратным эффектом, затем видимость, затем контроли и регуляторный трек.

01

30 дней

Собрать комитет по безопасности ИИ

CISO, СТО, юрист и владелец продукта с правом останавливать внедрение. Коллегиальная форма даёт 48% внедрённых контролей против 24% у CISO в одиночку — единственный шаг с кратной отдачей в данных.

02

30–60 дней

Инвентаризировать ИИ и теневой ИИ

Утверждённый перечень ИИ-решений и целей использования. Закрывает разрыв между 100% теневого ИИ и 43% инвентаризации. Технически — через шлюз безопасности ИИ как точку наблюдения.

03

60 дней

Провести оценку угроз ИИ-решений

Модель угроз по OWASP Top 10 for LLM: инъекция промпта, утечка системного промпта, небезопасный вывод, отравление данных, полномочия агентов. Сейчас есть у 9% — самый дефицитный контроль.

04

60–90 дней

Поставить контроль на границе с моделью

Политика взаимодействия ИИ с внешними источниками и инструментами (сейчас 26%) плюс фильтрация запросов и ответов, контроль персональных данных и секретов на лету, лимиты токенов для агентов.

05

90 дней

Запустить обучение по безопасности ИИ

Закрывает барьер №1. Программа есть у 19% компаний, при том что 82% из назвавших экспертизу главным барьером обучение не ведут.

06

90 дней

Запланировать внедрение требований ФСТЭК

Не оценивать, а действовать: текущее состояние понятно. Утвердить план внедрения мер по приказу № 117 и методике от 12.04.2026 — со сроками и ответственными — и начать с перечня заимствованных компонентов ИИ (модели, веса, датасеты, внешние API).

РАЗДЕЛ IV

Голос рынка

Что говорят участники ИТ-отрасли



Артем Галонский

Генеральный директор Postgres Professional

ГОЛОС РЫНКА · 1 ИЗ 5

КАКИЕ ТРЕНДЫ В ОБЛАСТИ БЕЗОПАСНОСТИ ИИ БУДУТ ОПРЕДЕЛЯТЬ ИТ-РЫНОК В БЛИЖАЙШИЕ ДВА ГОДА?

В ближайшие два года безопасность ИИ будет развиваться как часть общей архитектуры управления данными и доступом. По мере перехода от экспериментов к промышленному использованию ИИ ключевыми становятся вопросы: какие данные доступны модели, учитывает ли она права конкретного пользователя, можно ли проверить источник ответа. А также можно ли ограничить действия ИИ-агента и всегда иметь функционал возврата агента в предыдущее состояние до выполнения последней операции.

Один из главных трендов — защита RAG-сценариев и корпоративных ассистентов, работающих с внутренними знаниями и операционными системами. Подключение языковой модели к данным не должно расширять права сотрудника: помощник обязан учитывать роли, ограничения на уровне строк и столбцов, а также требования к маскированию персональных и финансовых данных.

Не менее важен контроль ИИ-агентов, которые могут не только отвечать на вопросы, но и выполнять действия в корпоративных системах. Здесь необходимы разграничение полномочий, аудит, подтверждение критичных операций и возможность быстро отозвать доступ.

Отдельное направление — защита качества и целостности данных. ИИ способен ускорять принятие решений, но так же быстро масштабирует ошибку, если она присутствует в исходных данных или корпоративной базе знаний.

Поэтому будут востребованы контроль происхождения данных, мониторинг аномалий и проверка изменений в критичных наборах.

КАКИЕ БИЗНЕС-ПРОЦЕССЫ И ОРГАНИЗАЦИИ ВЫИГРЫВАЮТ БОЛЬШЕ ВСЕГО СЕЙЧАС?

Наибольший эффект ИИ получают компании с большим объемом повторяющихся операций и высокой стоимостью ошибки: банки, страховые организации, ритейлеры, маркетплейсы, логистические и телеком-компании, промышленные холдинги. Помимо работы с обращениями, документами, поиском по внутренним знаниям и антифродом, одним из наиболее прикладных сценариев становится AI DBA. ИИ помогает администраторам быстрее разбираться с медленными запросами, блокировками, нетипичной нагрузкой и причинами инцидентов, а также готовить рекомендации по настройке СУБД. В критичных OLTP-системах при этом он должен работать как помощник: решение о внесении изменений в продуктивную среду остается за специалистом. При этом ИИ дает быстрый эффект не только крупным компаниям. Малый бизнес и стартапы могут без масштабной перестройки процессов применять его в ежедневной работе: автоматизировать подготовку описания товаров и изображений, ответы клиентам, типовые документы и коммерческие предложения. Там, где результат легко проверить и скорректировать, небольшие команды часто внедряют ИИ быстрее крупных организаций.

ЧТО ВПЕЧАТЛЯЕТ ЛИЧНО ВАС БОЛЬШЕ ВСЕГО ПРИ РАБОТЕ С ИИ?

Больше всего в работе с ИИ впечатляет его способность снижать порог входа в сложные технологические системы. Пользователь может сформулировать задачу на естественном языке, а ИИ помогает превратить ее в запрос к данным, сценарий проверки, черновик документа или последовательность технических действий.

Для меня, как и для многих опытных руководителей и менеджеров с инженерным бэкграундом или опытом в разработке, ИИ дает возможность быстрее возвращаться к самостоятельному созданию продуктов: проверять идеи, собирать прототипы и делать небольшие рабочие инструменты без длительного погружения в код и необходимости сразу формировать отдельную команду. Особенно ценна эта возможность там, где она сочетается с дисциплиной: точной моделью данных, корректно настроенными правами доступа, проверяемыми источниками и обязательной валидацией результата.

Для корпоративного применения это, пожалуй, главный принцип: ИИ не отменяет требований к надежности, безопасности и качеству данных. Напротив, чем глубже он интегрирован в бизнес-процессы, тем важнее становятся зрелость архитектуры данных, управляемость доступа и прозрачность принимаемых решений.



Павел Борченко

Управляющий директор ООО «Робин»

КАКИЕ ТРЕНДЫ В ОБЛАСТИ БЕЗОПАСНОСТИ ИИ БУДУТ ОПРЕДЕЛЯТЬ ИТ-РЫНОК В БЛИЖАЙШИЕ ДВА ГОДА?

Для внутренних сервисов на текущий момент приоритетны анонимизация передаваемых данных и подключение к действующим ролевым моделям. Для внешних сервисов — фокус на гардрейлы и любые инъекции через агентов. Но на два года вперед с ИИ-технологиями загадывать сложно: всё меняется каждые несколько месяцев.

ЧТО ВПЕЧАТЛЯЕТ ЛИЧНО ВАС БОЛЬШЕ ВСЕГО ПРИ РАБОТЕ С ИИ?

Больше всего меня впечатляет, насколько быстро люди привыкли к новой технологии, даже особо не разбираясь, как она работает. Люди часто доверяют информации, выданной ИИ-агентами, даже не проверяя источники. Отправляют рабочую информацию в облачные ИИ, не задумываясь о конфиденциальности этой информации. Генерируют отчеты и документы и отправляют их, не читая. ИИ поменял многие аспекты нашей жизни быстрее, чем мы успели к ним подготовиться, и теперь мы пытаемся догнать прогресс и поменять действующие процессы.

КАКИЕ БИЗНЕС-ПРОЦЕССЫ И ОРГАНИЗАЦИИ ВЫИГРЫВАЮТ БОЛЬШЕ ВСЕГО СЕЙЧАС?

Мы видим, что сегодня выигрывают те компании, которые подходят к задаче внедрения ИИ точно, а не пытаются внедрить ИИ массово по всем процессам сразу. Основную выгоду ИИ сейчас даёт в извлечении неструктурированной информации и в недетерминированных процессах. Например, при обработке обращений или сборе информации из постоянно меняющихся источников. Раньше эти задачи пытались делать на правилах и алгоритмах, но это имело высокую стоимость при реализации и поддержке. ИИ поменял подход к таким задачам.

При этом некоторые организации пытаются автоматизировать всё ИИ-агентами, даже там, где классическая автоматизация и роботизация дали бы лучший эффект и обошлись дешевле. Поэтому мы часто начинаем разговор с клиентами не с того, как и куда мы будем внедрять ИИ, а смотрим на процессы в организации и предлагаем подходящие инструменты под каждый процесс. И на практике чаще всего рутинные задачи, от которых хочет избавиться клиент, не требуют ИИ или требуют его лишь на нескольких небольших шагах.



Алексей Захаров

Директор по технологическому консалтингу Axiom JDC

КАКИЕ ТРЕНДЫ В ОБЛАСТИ БЕЗОПАСНОСТИ ИИ БУДУТ ОПРЕДЕЛЯТЬ ИТ-РЫНОК В БЛИЖАЙШИЕ ДВА ГОДА?

В ближайшие два года главными трендами в области безопасности ИИ станет рост рынка систем обеспечивающих безопасность разработки ПО, что связано с появлением новых угроз атак на цепочки поставок, вредоносный маскированный код не заметный сканерам, также смещение фокуса с защиты отдельных элементов ПО на безопасность всего стека разработки с применением ИИ-систем, включая создание ИИ-агентов для контроля за безопасностью в разработке. Так, все больше эксплойтов создается с помощью ИИ и соответственно защита тоже должна строится на системах с использованием ИИ, иначе не выдержать конкуренцию технологий. Усилится регуляторное давление, а обязанности CISO расширятся до стратегического участия в управлении ИИ-рисками в составе модели угроз организации, при этом в центрах безопасности (SOC) до 80% инцидентов будут обрабатываться с помощью ИИ-агентов в режиме человеко-машинного взаимодействия, а разработка будет использовать ИИ еще в процессе сборки и проверки ПО. Иными словами, ИИ-безопасность превратится из технической опции в обязательный фундамент корпоративной цифровой стратегии.

КАКИЕ БИЗНЕС-ПРОЦЕССЫ И ОРГАНИЗАЦИИ ВЫИГРЫВАЮТ БОЛЬШЕ ВСЕГО СЕЙЧАС?

Наибольшую выгоду сегодня получают компании, которые целенаправленно внедряют ИИ в свои ключевые процессы разработки ПО, операционные процессы, а также сам сектор компаний работающих в сфере кибербезопасности, выступающий в роли «авангарда» в эпоху ИИ.

ЧТО ВПЕЧАТЛЯЕТ ЛИЧНО ВАС БОЛЬШЕ ВСЕГО ПРИ РАБОТЕ С ИИ?

Скорость, точность, качество и возможность адаптации ИИ под любые задачи. Существенное сокращение трудозатрат до 10 раз экономия времени на рутинные операции. За человеком остается принятие результата и правильная постановка задачи, наряду с конфигурацией много-агентных ИИ архитектур.



Владимир Андреев

Президент Docsvision

КАКИЕ ТРЕНДЫ В ОБЛАСТИ БЕЗОПАСНОСТИ ИИ БУДУТ ОПРЕДЕЛЯТЬ ИТ-РЫНОК В БЛИЖАЙШИЕ ДВА ГОДА?

- 1 Вопросы организации работы с доверенными моделями в рамках концепции национальных и суверенных моделей ИИ
- 2 Вопросы разграничения доступа к персональным данным и другой чувствительной информации, хранящейся в корпоративных ИС при их использовании ИИ
- 3 Отражение новых видов атак, с использованием ИИ

Это приведет к коммерциализации сегмента AI Security и появлению нового класса продуктов.

КАКИЕ БИЗНЕС-ПРОЦЕССЫ И ОРГАНИЗАЦИИ ВЫИГРЫВАЮТ БОЛЬШЕ ВСЕГО СЕЙЧАС?

- Все процессы обработки документов — IDP (Intellectual Document Processing), нормоконтроль, поиск расхождений в документах, анализ полноты документации, комплаенс контроль и пр.
- Клиентский сервис и поддержка
- Разработка ПО
- Задачи оценки рисков и оптимизации

ЧТО ВПЕЧАТЛЯЕТ ЛИЧНО ВАС БОЛЬШЕ ВСЕГО ПРИ РАБОТЕ С ИИ?

Повышение производительности при разработке ПО, интерактивные возможности ИИ при разработки сложных документов и моделей ПО



Алексей Смирнов

Председатель совета директоров «Базальт СПО»

КАКИЕ ТРЕНДЫ В ОБЛАСТИ БЕЗОПАСНОСТИ ИИ БУДУТ ОПРЕДЕЛЯТЬ ИТ-РЫНОК В БЛИЖАЙШИЕ ДВА ГОДА?

- 1 Выработка мер контроля ИИ для предотвращения несанкционированных действий.
- 2 Определение лиц, несущих ответственность за действия ИИ (кто займет эту роль - разработчик, владелец или пользователь).
- 3 Разработка инструментов автоматического анализа моделей ИИ.

КАКИЕ БИЗНЕС-ПРОЦЕССЫ И ОРГАНИЗАЦИИ ВЫИГРЫВАЮТ БОЛЬШЕ ВСЕГО СЕЙЧАС?

- Тестирование ПО и поиск уязвимостей.
- Генерация программного кода.
- Ассистенты для колл-центров, расшифровка и протоколирование совещаний.
- Поиск и обработка информации, аналитические справки.
- Биржевая торговля.

ЧТО ВПЕЧАТЛЯЕТ ЛИЧНО ВАС БОЛЬШЕ ВСЕГО ПРИ РАБОТЕ С ИИ?

Начало перехода от эмуляции действий специалиста к анализу данных и принятию решений на базе сложных семантик.



Тренды ИТ-рынка в контексте ИИ- безопасности

Совместное отраслевое исследование АРПП «Отечественный софт» и AppSec Solutions

Сентябрь 2026