

Что отпугивает бизнес от использования ИИ и как научиться ему доверять

Искусственный интеллект (ИИ) уже не рассматривается как второстепенный проект или эксперимент, отметили около 1000 руководителей американских компаний, опрошенных в ходе исследования PwC 2019 AI Predictions. Сегодня у них вызывают беспокойство риски, которые могут отрицательно сказаться на результатах инвестирования в ИИ.

20%

респондентов ответили, что их компании будут развивать ИИ-проекты в 2019 году

Угрозы завтрашнего дня ...

В течение следующих пяти лет руководителей компаний будут беспокоить следующие угрозы:

43% Угрозы, связанные с защитой данных

В октябре 2018 г. зафиксировано 1027 фактов утечки данных, из-за которых рискам подверглись 57 667 911 электронных документов.¹

41% Новые киберугрозы

В 2016 году последствия действий вредоносных программ стоили экономике США по разным оценкам от 57 до 109 млрд. долл. США.²

34% Юридические и репутационные риски

В 2018 48% респондентов заявили о том, что они доверяют коммерческим организациям США, что на 10% ниже показателя предыдущего года.³

33% Слишком сложная для понимания и контроля область

200% увеличение финансирования Программы интерпретируемого ИИ (DARPA XAI) за период 2017-2019 гг.⁴

31% Дефицит специалистов в области ИИ

На 32% по сравнению с прошлым годом выросло количество вакансий для специалистов в области ИИ.⁵

31% Отставание США в области инноваций в сфере ИИ

В Китае в 6 раз больше патентов на технологии глубокого обучения, чем в США.⁶

1. Центр помощи жертвам хищения персональных данных и повышения осведомленности в этой области, Отчеты о результатах расследования случаев утечки данных, 31 октября 2018 г.
2. Совет экспертов в области экономики, Последствия действия вредоносных программ для экономики США с точки зрения затрат, февраль 2018.
3. Исследование Edelman Trust Barometer, 2018 г.
4. Министерство обороны США, Проект бюджета на 2019 финансовый год.
5. Indeed Hiring Lab, Спрос на специалистов в области ИИ растет, март 2018 г.
6. CB Insights, Тенденции в области ИИ, которые будут наблюдаться в 2018 г.

Источник: PwC 2019 AI Predictions
База: 1001 респондент
Вопрос: Какие из следующих сценариев, касающихся развития ИИ, будут представлять реальную угрозу бизнесу в следующие 5 лет?

Самые серьезные угрозы, связанные с ИИ, по отраслям



Потребительские товары

Угрозы, связанные с защитой данных

45%



ТЭК, добывающая промышленность

Дефицит специалистов в области ИИ

41%



Финансовые услуги

Угрозы, связанные с защитой данных

49%



Здравоохранение

Угрозы, связанные с защитой данных

51%



Промышленные товары

Слишком сложная для понимания и контроля область

39%



Высокие технологии, СМИ, телекоммуникации

Новые киберугрозы

43%

Источник: "Прогнозы развития технологии искусственного интеллекта на 2019 год" (PwC 2019 AI Predictions)
База: 1001 респондент (потребительские товары - 132; ТЭК, добывающая промышленность - 46; финансовые услуги - 187; здравоохранение - 110; промышленные товары - 208; высокие технологии, СМИ, телекоммуникации - 208; другие отрасли - 110).
Вопрос: Какие из следующих сценариев, касающихся развития ИИ, будут представлять реальную угрозу бизнесу в следующие 5 лет?

...призывают действовать сегодня

Обеспечение доверия к системам ИИ - terra incognita для руководителей, но оно возглавляет список их текущих задач. Руководители принимают меры для ответственного применения ИИ, включая применение самого ИИ для борьбы с киберугрозами.

37%

руководителей отмечают, что обеспечение доверия к системам ИИ – это их первейшая задача

| | Всего | Потребительские товары | ТЭК, добывающая промышленность | Финансовые услуги | Здравоохранение | Промышленные товары | Высокие технологии, СМИ, телекоммуникации |
|--|-------|------------------------|--------------------------------|-------------------|-----------------|---------------------|---|
| Усиление безопасности ИИ за счет валидации, мониторинга, верификации | 64% | 70% | 72% | 60% | 58% | 63% | 70% |
| Создание прозрачных, объяснимых, доказуемых моделей ИИ | 61% | 58% | 67% | 64% | 56% | 60% | 63% |
| Создание этичных, понятных, легальных систем ИИ | 55% | 52% | 57% | 53% | 56% | 53% | 58% |
| Улучшение корпоративного управления за счет операционных моделей и процессов на базе ИИ | 52% | 55% | 63% | 54% | 36% | 51% | 60% |
| Тестирование на погрешность в данных и моделях, субъективность при выборе алгоритмов человеком | 47% | 50% | 43% | 48% | 48% | 48% | 50% |
| Использование ИИ для управления рисками, борьбы с киберугрозами и мошенничеством | 46% | 47% | 41% | 52% | 55% | 34% | 49% |

Источник: "Прогнозы развития технологии искусственного интеллекта на 2019 год" (PwC 2019 AI Predictions)
База: 1001 респондент (потребительские товары - 132; ТЭК, добывающая промышленность - 46; финансовые услуги - 187; здравоохранение - 110; промышленные товары - 208; высокие технологии, СМИ, телекоммуникации - 208; другие отрасли - 110).
Вопрос: Какие шаги предпримет ваша организация в 2019 году, чтобы разработать и внедрить системы ИИ, соответствующие принципам доверия, справедливости и стабильности? Какие задачи, связанные с использованием ИИ будут наиболее важными для вашей организации в 2019 году?

Конечная цель: ответственное применение ИИ

Чтобы укрепить доверие к ИИ, проработайте следующие пять областей:



Достоверность

Учитывается ли влияние субъективности при использовании ИИ? Минимизировано ли ее влияние на данные и модели ИИ?



Интерпретируемость

Можно ли объяснить, каким образом модель ИИ приняла решение? Гарантирована ли правильность этих решений?



Надежность и безопасность

Можно ли положиться на работу систем ИИ? Уязвимы ли системы ИИ перед атаками?



Корпоративное управление

Кто отвечает за системы ИИ? Внедрены ли надлежащие процедуры контроля?



Системная этика

Соответствуют ли системы ИИ нормативно-правовым требованиям? Какое влияние ИИ окажет на сотрудников?