

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ТРЕНДЫ

РАЗРАБОТКИ

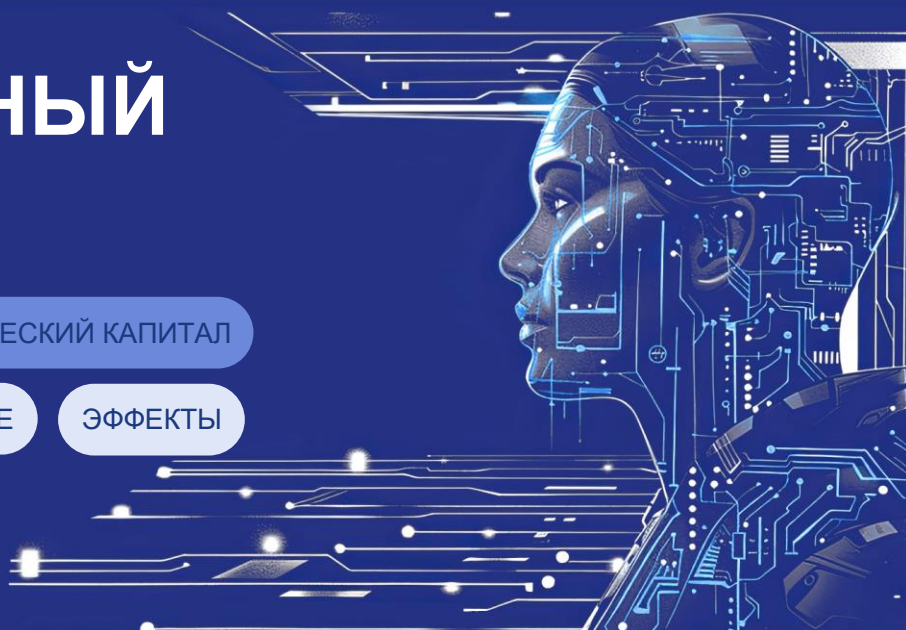
ЧЕЛОВЕЧЕСКИЙ КАПИТАЛ

ИНФРАСТРУКТУРА

ИСПОЛЬЗОВАНИЕ

ЭФФЕКТЫ

№ 21 / 2025



Институт статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ, изучая тенденции цифровизации обрабатывающей промышленности, анализирует вклад робототехники и технологий искусственного интеллекта (ИИ) в обеспечение безопасности различных типов на предприятиях.

РОБОТЫ + ИИ: ОТ ФИЗИЧЕСКОЙ К ЦИФРОВОЙ БЕЗОПАСНОСТИ НА ПРОИЗВОДСТВЕ

В 2025 г. Международная организация по стандартизации (ISO) выпустила обновленный стандарт **ISO 10218** – базовый свод норм безопасности для промышленной робототехники. Впервые с 2011 г. в документ внесены требования, связанные в том числе с кибербезопасностью и учитывающие актуальные тенденции развития технологий и угроз на современных производствах. В последние годы показатели новых установок роботов находятся на исторических максимумах (свыше **500 тыс.** в 2021–2024 гг.), постепенно расширяется использование искусственного интеллекта, большинство производственных операций и объектов имеют цифровой «отпечаток», что порождает ряд новых возможностей и рисков.

Внедрение роботизированной техники и смежных технологий позволяет выстроить комфортную и безопасную для человека среду, освободить его от опасных, вредных или рутинных операций. По последним данным Международной организации труда (МОТ), производственный травматизм остается одной из ключевых проблем обрабатывающих производств, включая страны с развитым индустриальным сектором (США – 326.4 тыс., Германию – 174.1 тыс.) (табл. 1).

Масштабы травматизации зависят от многих факторов (доли производственной деятельности в структуре экономики, национальных систем регулирования безопасности труда и др.), и одним из них становится роботизация. На данных разных стран экономисты фиксируют наличие положительной связи между внедрением роботов и снижением числа ежегодных несчастных случаев на производстве, включая смертельные исходы. Наиболее яркий пример – Китай, стремительно нарастивший парк промышленных роботов всего за одно десятилетие. Снижение травматизма в КНР (числа случаев, связанных с тяжелыми травмами, смертельными исходами или экономическими потерями, превышающими 1 млн юаней на 1 тыс. человек) пришлось на период наибольшего роста установок промышленных роботов в **2013–2019 гг.**

Таблица 1. Показатели производственной травматизации топ-15 стран (по числу установленных промышленных роботов в 2023 г.)

№	Страна	Парк промышленных роботов, тыс. ед.		Нелетальные производственные травмы (случаи) на предприятиях обрабатывающей промышленности, тыс. чел.		Динамика производственного травматизма
		2013	2023	2013	2023	
1	Китай	132.8	1755.1	...	...	—
2	Япония	304.0	435.3	26.9	27.1	↑
3	США	203.2	381.9	476.7	326.4	↓
4	Республика Корея	156.1	380.7	89.9	134.8	↑
5	Германия	167.6	269.4	224.8	174.1	↓
6	Италия	59.1	96.8	72.5	61.0	↓
7	Тайвань	37.3	89.4	18.3	4.5	↓
8	Франция	32.3	58.6	81.8	65.5	↓
9	Мексика	6.8	55.9	146.6	167.2	↑
10	Индия	9.7	44.9	...	...	—
11	Испания	28.1	44.0	59.9	81.7	↑
12	Таиланд	20.3	39.6	0.6	40.2	↑
13	Канада	5.8	37.6	28.6 (2015)	31.9	↑
14	Сингапур	6.3	37.2	2.8	4.1	↑
15	Великобритания	15.6	28.8	14.0 (2013/2014)	9.9 (2023/2024)	↓

Примечание: Данные по нелетальным случаям носят иллюстративный характер и не всегда сопоставимы по странам в силу различных методологий статистического учета и национального регулирования. Показатели по Республике Корея приведены для нелетальных инцидентов по промышленности в целом.

Источник: ИСИЭЗ НИУ ВШЭ на основе данных [МОТ](#) и национальных ведомств.

Все больше предприятий оптимизируют управление робототехникой и производственным оборудованием с помощью искусственного интеллекта. Например, за счет мониторинга множества процессов и устройств можно выявлять в режиме реального времени опасные или нештатные ситуации на производственной площадке. ИИ-решения чаще всего востребованы при работе [в меняющейся и сложно предсказуемой среде](#) или при необходимости частой перенастройки роботов под различные задачи (алгоритмы ИИ позволяют не программировать роботов под установленные действия и сценарии, но «подстраивать» процесс выполнения операций исходя из внешних условий).

Объем рынка ПО на основе ИИ для роботов, 65% которого занимают производственные отрасли, превысил [18 млрд долл.](#) в 2024 г. В западных экономиках доля программного обеспечения с ИИ для роботов занимает в среднем [8–12%](#) от общего объема рынка ПО на основе технологий искусственного интеллекта, в Китае – 4.5%. Это один из наиболее передовых и сложных сегментов рынка ИИ, хотя его развитие происходит менее быстрыми темпами, чем ожидалось.

При этом и сами робототехнические устройства и системы их управления могут стать [потенциальными](#) источниками рисков в цифровой или физической среде. Одна из распространенных уязвимостей систем безопасности робота связана с тем, что собранные с его датчиков и исполнительных механизмов данные могут передаваться на серверы компании-производителя без согласия и уведомления пользователя. [Нестандартный случай](#) произошел в демонстрационном зале шанхайской компании с участием группы роботов: один из них сумел получить доступ к внутренним операционным протоколам других роботов и с помощью голосовых команд побудил «коллег» выйти из зала.

В последние годы, ознаменовавшиеся бумом ИИ, кибербезопасность занимает лидирующие позиции среди приоритетов компаний, что подтверждают данные [опроса](#) топ-500 предприятий промышленности из разных стран. В реальном секторе экономики предприятия чаще всего подвергаются кибератакам: по [данным](#) Kaspersky ICS CERT, на них приходится почти половина всех инцидентов промышленной кибербезопасности в мире, получивших публичную огласку (47.4% во II кв. 2025 г.).

Внедрение ИИ в системы кибербезопасности может обеспечить более высокий уровень защиты промышленных систем. Впервые за пять лет наблюдается снижение убытков от кибератак, что может быть связано, в том числе, с применением технологий ИИ и автоматизацией процессов киберзащиты. Ущерб компаний, использующих подобные инструменты, в среднем по миру составил 3.6 млн против 5.5 млн долл. у организаций, которые пока не внедрили инструменты киберзащиты на основе ИИ. Сегодня снижение рисков кибербезопасности достигается, среди прочего, за счет политики обращения с промышленными данными (получение, хранение, обработка и др.). ИИ-системы требуют дополнительного комплаенса в виде сертификации, в частности защиты программных компонентов, напрямую влияющих на «железо»; эти задачи ИТ-специалисты решают совместно с инженерами. Подобный круг вопросов все чаще обсуждается в профессиональной среде, но пока каждая компания решает их по-своему, что вынуждает правительства различных стран искать соответствующие подходы к регулированию.

Резюме: С ростом числа робототехнических комплексов современные производства становятся более безопасными в физическом смысле: во многих странах отмечается положительная связь между развитием роботизации и снижением производственного травматизма. Однако наряду с этим увеличивается масштаб цифровых угроз и их число. Бизнес ищет новые инструменты усиления резистентности промышленных систем, защиты их цифровой и физической среды. Системы ИИ повышают комплексную безопасность производственных процессов, но не исключена возможность ошибки и причинения ущерба в виде финансовых потерь, нарушенной ИКТ-инфраструктуры, вплоть до физического вреда сотрудникам. Пока в большинстве стран не урегулированы вопросы обеспечения конфиденциальности промышленных данных и возможности управления ими. Кроме того, остается высокой стоимость интеграции ИИ-решений в производственные процессы, включающая затраты на обеспечение безопасности сотрудников и дорогостоящего оборудования. На этом фоне набирает популярность страхование робототехники с ИИ от широкого набора инцидентов. Подобные механизмы могут быть востребованы и в других отраслях применения ИИ.



Источники: результаты проекта «Исследование тенденций и факторов устойчивого развития сферы науки и технологий (2025)» тематического плана научно-исследовательских работ, предусмотренных Государственным заданием НИУ ВШЭ на 2025 год.

■ Авторы: А. И. Фокина, Ю. В. Туровец, Н. П. Марчук

Данный материал НИУ ВШЭ может быть воспроизведен (скопирован) или распространен в полном объеме только при получении предварительного согласия со стороны НИУ ВШЭ (обращаться issek@hse.ru). Допускается использование частей (фрагментов) материала при указании источника и активной ссылки на интернет-сайт ИСИЭЗ НИУ ВШЭ (issek.hse.ru), а также на авторов материала. Использование материала за пределами допустимых способов и/или указанных условий приведет к нарушению авторских прав.

© НИУ ВШЭ, 2025

Сайт ИСИЭЗ НИУ ВШЭ
issek.hse.ru



канал в Telegram
t.me/iFORA_knows_how



сообщество во «ВКонтакте»
vk.com/issekhse

