

EFFECTIVE MANAGEMENT OF BIG DATA: A COMPARATIVE ANALYSIS OF PLATFORMS AND TECHNOLOGIES FOR INFORMATION PROCESSING

V.V. Verniahovskaya

*Master of economics, Deputy Dean
of the faculty of engineering and
Economics at BSUIR*

O.M. Raptunovich

*Senior Lecturer at the
Department of Economic
Informatics BSUIR, master*

V.A. Usova

*Student of BSUIR, Faculty of
Engineering and Economics,
specialty Information Systems and
Technologies*

Abstract. The article examines the effective use of big data and analyzes platforms and technologies for data analysis. Various tools and methods are used for data analysis, storage, and processing. Attention is paid to the platforms Hadoop, Apache Spark and others, as well as machine learning technologies that affect the performance and scalability of data processing.

Keywords: big data, Hadoop, Apache Spark, machine learning, MapReduce, NoSQL databases, data analysis, Kafka, Flink.

УДК 004.896

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ



Е. Н. Бычек

*Студентка кафедры инженерной психологии и
эргономики Белорусского государственного
университета информатики и
радиоэлектроники
bychekeliza@gmail.com*



Н. В. Щербина

*Старший преподаватель кафедры инженерной
психологии и эргономики Белорусского
государственного университета информатики
и радиоэлектроник, магистр технических наук
shcherbina@bsuir.by*

Е. Н. Бычек

Обучается на третьем курсе Белорусского государственного университета информатики и радиоэлектроники. Область научных интересов связана с информационными системами и технологиями в обеспечении промышленной безопасности».

Н. В. Щербина

Окончила Белорусский национальный технический университет. Область научных интересов связана с исследованием проблем саморегуляции функционального состояния человека, аспектов деятельности человека-оператора в системах контроля и управления, промышленной безопасностью, организацией учебного и научно-исследовательского процессов в техническом университете.

Аннотация: Проанализирована роль технологий искусственного интеллекта (ИИ) в трансформации систем промышленной безопасности на основе актуальных отраслевых источников. Рассмотрены ключевые направления применения ИИ: от предиктивной аналитики и компьютерного зрения до интеллектуальных средств индивидуальной защиты. Особое внимание уделено сдвигу от реактивных к проактивным стратегиям предотвращения инцидентов. В работе также систематизированы основные этические и организационные вызовы, связанные с внедрением ИИ, включая вопросы доверия, прозрачности и приватности.

Ключевые слова: промышленная безопасность, искусственный интеллект, компьютерное зрение, интеллектуальные носимые устройства, предиктивная аналитика, этика, безопасность труда, мониторинг, отказ оборудования.

Введение. Концепция Индустрии 4.0, или Четвертой промышленной революции, центрирована вокруг данных, аналитики и взаимосвязанных систем. Ее ядро составляет способность не просто собирать информацию, но и использовать ее для прогнозирования и решения проблем до их возникновения, что имеет прямое отношение к сфере промышленной безопасности. Внедрение искусственного интеллекта знаменует переход от традиционных, зачастую реактивных методов обеспечения безопасности (чек-листы, периодические проверки) к проактивной, предсказывающей модели. Как отмечают эксперты, ИИ способен анализировать массивы данных с беспрецедентной скоростью, обнаруживая паттерны, невидимые человеческому глазу, что позволяет прогнозировать риски и предотвращать инциденты. Актуальность этой трансформации подчеркивается глобальной статистикой: по данным Международной организации труда, ежегодно происходит около 317 миллионов несчастных случаев на производстве [1].

Основная часть. Практическое применение искусственного интеллекта в промышленной безопасности реализуется через несколько взаимодополняющих технологических направлений:

1 *Предиктивная аналитика и мониторинг оборудования.* Одно из наиболее значимых применений ИИ – прогнозирование отказов оборудования, которое основывается на обработке и анализе больших объемов данных. Алгоритмы машинного обучения анализируют исторические и текущие данные с датчиков IoT для отслеживания ключевых показателей (вибрация, температура, давление и др.), выявляют незначительные отклонения от нормальных закономерностей, и как следствие, прогнозируют потенциальные отказы до их возникновения, что позволяет находить долгосрочные решения. Такой подход позволяет перейти от планово-предупредительного обслуживания к обслуживанию по фактическому состоянию, минимизируя незапланированные простои и снижая риски аварий, связанных с внезапным выходом техники из строя. На рисунке 1 показаны преимущества ИИ в предоставлении отказов оборудования. Данный подход формирует методологическую основу Индустрии 4.0, в рамках которой данные служат инструментом для упреждающего выявления и нивелирования потенциальных проблем [2].



Рисунок 1. Преимущества ИИ в предотвращении отказов оборудования

2 *Компьютерное зрение для анализа поведения и условий труда.* Системы на основе компьютерного зрения используют камеры и сенсоры для непрерывного автоматического мониторинга производственной среды в реальном времени. Они способны распознавать потенциальные опасности, такие как: отсутствие предписанного средства индивидуальной защиты (СИЗ), несанкционированное нахождение в опасной зоне, небезопасное обращение с оборудованием или появление таких рисков, как разливы жидкостей. Данные системы предоставляют инструмент для постоянного аудита соблюдения протоколов безопасности, выступая в роли «дополнительной пары глаз», которая не устает и не отвлекается.

На рисунке 2 показаны преимущества компьютерного зрения для анализа поведения и условий труда на промышленных объектах [3-5].

3 *Интеллектуальные носимые устройства и биометрический мониторинг.* Интеллектуальные носимые устройства и системы биометрического мониторинга стали неотъемлемой частью концепции Индустрии 4.0, превращая традиционные СИЗ в активные цифровые инструменты.

Современные СИЗ эволюционируют в сторону интеграции с ИИ.

Умные каски, жилеты и браслеты, оснащенные датчиками, отслеживают не только окружающую среду (наличие газов, экстремальные температуры и т.п.), но и физиологическое состояние работника (уровень усталости, тепловой стресс, частоту сердечных сокращений и т.п.).

В случае выявления опасных отклонений устройство может подать предупреждение самому работнику и/или диспетчеру.

Кроме того, разрабатываются AI-экзоскелеты, которые снижают физическую нагрузку на оператора, предотвращая травмы опорно-двигательного аппарата при работе с тяжестями [1].

Преимущества компьютерного зрения для анализа поведения и условий труда на промышленных объектах



Рисунок 2. Преимущества компьютерного зрения

На рисунке 3 показаны преимущества интеллектуальных носимых устройств и биометрического мониторинга [6-8].

4 *Автоматизация опасных задач и инспекций*. ИИ и робототехника берут на себя выполнение задач в средах с недопустимо высоким риском для человека.

Это включает использование автономных дронов для инспекции труднодоступных или опасных объектов (например, высотных конструкций, нефтехимических резервуаров) и развертывание роботов для работ с токсичными веществами или в зонах возможных обрушений.

Таким образом, минимизируется непосредственная экспозиция персонала к угрозам.

Преимущества интеллектуальных носимых устройств и биометрического мониторинга

Повышение безопасности и снижение травматизма	Контроль доступа и дисциплины
<ul style="list-style-type: none">• контроль жизненных показателей (позволяет выявлять отклонения показателей от нормы до того, как они приведут к ошибкам или несчастным случаям)• снижение травматизма• экзоскелеты и поддержка (усиливают физические возможности человека, снижают нагрузку на суставы, предотвращают травмы опорно-двигательного аппарата)	<ul style="list-style-type: none">• биометрические СКУД (использование уникальных физиологических характеристик для доступа в чистые зоны или управления опасным оборудованием исключает возможность передачи пропусков другим лицам и повышает общую дисциплину)• контроль условий среды (носимые датчики могут фиксировать уровни радиации, концентрацию газов или уровень шума непосредственно вокруг конкретного работника, обеспечивая более точную защиту, чем стационарные системы)
Рост продуктивности и эффективности	Оперативная реакция на инциденты
<ul style="list-style-type: none">• AR-индустрия (умные очки (AR) выводят пошаговые подсказки и чертежи прямо перед глазами рабочего, освобождая руки и исключая необходимость сверяться с бумажными документами)• умные перчатки (позволяют сканировать штрих-коды жестами и фиксировать перемещение инвентаря в цифровой системе без использования терминалов сбора данных)• предиктивная аналитика (ИИ анализирует биометрические данные персонала для выявления скрытых признаков заболеваний, например, хронического стресса, что позволяет вовремя корректировать график работы)	<ul style="list-style-type: none">• детекция падений и неподвижности (акселерометры и гироскопы мгновенно передают сигнал тревоги диспетчеру, если работник упал или долгое время не подает признаков активности)• геопозиционирование и SOS-сигналы (в случае аварии система точно указывает местонахождение пострадавшего, что критически важно для работы в шахтах, на крупных складах или удаленных объектах)

Рисунок 3. Преимущества интеллектуальных носимых устройств и биометрического мониторинга

На рисунке 4 показаны преимущества использования автоматизации опасных задач и инспекций на производственных объектах [9-11].

Американское общество инженеров по безопасности (ASSP) в своей позиции обозначило четыре фундаментальных принципа ответственного использования ИИ в безопасности, которые служат ориентиром для организаций [4]:

1 *Доверие*: ИИ должен усиливать навыки и способности специалистов по безопасности, а не заменять человеческое суждение и принятие решений. Окончательный контроль и контекстуальная оценка рисков должны оставаться за человеком.

2 *Прозрачность*: Работники, менеджеры и руководители должны быть информированы о возможностях и ограничениях, используемых ИИ-технологий. Открытость в отношении того, как системы работают и какие данные обрабатывают, формирует культуру доверия и подотчетности.

3 Справедливость: Необходимо гарантировать, что ИИ-технологии не усугубляют существующие и не создают новые формы дискриминации в области охраны труда и промышленной безопасности. Алгоритмы должны быть свободны от предвзятостей, которые могут негативно сказаться на определенных группах работников.

Преимущества использования автоматизации опасных задач и инспекций на производственных объектах

Безопасность и здоровье работников <ul style="list-style-type: none">• исключение работника из опасных зон (роботы и дроны заменяют людей при работе в замкнутых пространствах, на высоте, в условиях экстремальных температур, радиации и т.п.)• снижение физической и когнитивной нагрузки (автоматизация рутинных и стрессовых задач, позволяет снизить уровень стресса у работников и минимизировать риск ошибок из-за усталости)• мгновенное реагирование (системы мониторинга на базе ИИ в реальном времени анализируют данные с датчиков и камер, предсказывая аварийные ситуации и автоматически блокируя работу оборудования при угрозе)	Повышение эффективности инспекций <ul style="list-style-type: none">• скорость и частота (роботизированные системы проводят комплексные проверки объектов быстрее человека, что позволяет проводить инспекции чаще, не останавливая производственный цикл)• доступ к труднодоступным местам (использование дронов и малогабаритных роботов позволяет обследовать трубопроводы, резервуары и опоры ЛЭП без необходимости возведения строительных лесов или использования промышленных альпинистов)• точность данных (автоматизированные системы, оснащенные сенсорами высокого разрешения, обнаруживают дефекты, например, микротрещины, утечки газа, перегрев, которые невидимы для человеческого глаза)
Экономические и операционные преимущества <ul style="list-style-type: none">• переход к предиктивному обслуживанию (постоянный автоматизированный мониторинг позволяет внедрять стратегии обслуживания «по состоянию», что снижает количество внеплановых простоев)• цифровизация отчетности (результаты инспекций мгновенно оцифровываются и интегрируются в системы управления жизненным циклом физических активов и в систему планирования предприятия в целом активами, обеспечивая прозрачность данных для всех подразделений)• оптимизация штата (автоматизация высвобождает квалифицированный персонал для более сложных аналитических и управленческих задач, повышая общую производительность труда)	Соответствие нормативным требованиям <ul style="list-style-type: none">• автоматизированный соответствие (с 1 января 2023 года Республика Беларусь перешла на интегрированную автоматизированную систему контрольной (надзорной) деятельности, что упростило взаимодействия с надзорными органами)• объективность контроля (использование автоматизации исключает субъективность и возможность сокрытия нарушений, что критически важно для соблюдения требований промышленной безопасности)

Рисунок 4. Преимущества использования автоматизации опасных задач и инспекций на производственных объектах

4 Конфиденциальность: Организации обязаны внедрять надежные меры защиты для предотвращения несанкционированного доступа, неправомерного использования или эксплуатации конфиденциальной информации, собираемой ИИ-системами. Защита персональных данных работников является критически важной.

Несмотря на ряд преимуществ использования ИИ в промышленной безопасности, практическое внедрение ИИ-технологий в производственный процесс затруднено из-за ряда финансовых (высокие инвестиции), технических (сложность интеграции), социальных (сопротивление работников) проблем, проблем кибербезопасности, а также этических аспектов (справедливость и непредвзятость, прозрачность и объяснимость, ответственность, приватность и безопасность данных).

Заключение. Искусственный интеллект утвердился в качестве трансформационного инструмента в области промышленной безопасности, предлагая переход от исторически сложившейся реактивной модели к проактивной, основанной на данных. Технологии предиктивной аналитики, компьютерного зрения и интеллектуальных носимых устройств демонстрируют значительный потенциал для предотвращения аварий, снижения травматизма и оптимизации производственных процессов. Однако, как и любая мощная технология, ИИ требует ответственного и взвешенного подхода к внедрению. Ключом к успешной интеграции

является не слепая автоматизация, а создание симбиотической системы, где ИИ выступает в роли мощного аналитического инструмента, расширяющего возможности специалистов по безопасности, а не заменяющего их профессиональное суждение. Соблюдение принципов доверия, прозрачности, справедливости и конфиденциальности, сформулированных профессиональным сообществом, является обязательным условием для построения эффективных, этических и принимаемых работниками систем безопасности будущего. Таким образом, будущее промышленной безопасности лежит не в противопоставлении человека и машины, а в их разумной интеграции, где технология служит для защиты самого ценного ресурса – человеческой жизни и здоровья. Внедрение ИИ-систем потребует психологического сопровождения в производственном секторе, которое может быть представлено следующими направлениями:

1) технологическая тревога: психологическая подготовка работников, объясняющая, что ИИ – это инструмент, а не замена работника, а также профилактика цифрового отчуждения для предотвращения чувства контроля над процессом, когда работник перестает понимать, почему система приняла то или иное решение;

2) поддержка в условиях проактивной модели: помочь в адаптации к работе в условиях неопределенности и доверия ИИ-системам, а также помочь в оптимизации режимов труда работника во избежание потери концентрации внимания;

3) этический и психологический мониторинг: помочь психолога в реальном времени либо через обучение ИИ-систем принятию решения о критических показателях жизнедеятельности работника, а также этическая безопасность персональных данных;

4) цифровое доверие: недопущение гипердоверия и преодоления недоверия.

Список литературы

[1] How AI is transforming workplace safety for engineers [Электронный ресурс]. – Режим доступа : <https://www.eit.edu.au/ai-is-transforming-workplace-safety-for-engineers/>. – Дата доступа: 16.01.2026.

[2] Industry 4.0 is all about analytics and industrial data [Электронный ресурс]. – Режим доступа : <https://www.wizata.com/knowledge-base/industry-4.0-is-all-about-analytics-and-industrial-data>. – Дата доступа: 18.01.2026.

[3] The disrupt Labs [Электронный ресурс]. – Режим доступа : <https://thedisruptlabs.com/what-is-computer-vision-ai/>. – Дата доступа: 20.01.2026.

[4] Defining the Role of AI in Safety [Электронный ресурс]. – Режим доступа : <https://www.assp.org/news-and-articles/defining-the-role-of-ai-in-safety>. – Дата доступа: 18.01.2026.

[5] Zest Minds Making Technology Work for you [Электронный ресурс]. – Режим доступа : <https://www.zestminds.com/blog/real-world-applications-computer-vision/#:~:text=When%20combined%20with%20IoT%20data,and%20clinician%20support%2C%20not%20replacement>. – Дата доступа: 20.01.2026.

[6] Ajprotech [Электронный ресурс]. – Режим доступа : <https://ajprotech.com/blog/internet-of-things/top-wearables-of-2026-trends-in-health-and-fitness.html#:~:text=AI%2DDriven%20Sensor%20Fusion%20and,security%20by%20minimizing%20cloud%20dependency>. – Дата доступа: 20.01.2026.

[7] Cerexio [Электронный ресурс]. – Режим доступа : <https://cerexio.com/blog/benefits-of-employing-wearable-technology-in-manufacturing-cerexio-singapore#:~:text=It%20is%20evident%20that%20wearable,production%20lines%20and%20reduces%20mistakes>. – Дата доступа: 20.01.2026.

[8] Министерство по чрезвычайным ситуациям Республики Беларусь [Электронный ресурс]. – Режим доступа : <https://niipb.mchs.gov.by/novosti/504370/>. – Дата доступа: 20.01.2026.

[9] Yamato [Электронный ресурс]. – Режим доступа : <https://www.yamatoscale.co.uk/automation-in-manufacturing-the-impact-on-safety-and-efficiency/#:~:text=Outside%20of%20safety%20concerns%2C%20there,results%20in%20a%20shorter%20timeframe>. – Дата доступа: 21.01.2026.

[10] Field Eagle [Электронный ресурс]. – Режим доступа : <https://www.fieldeagle.com/blog/top-technology-trends-watch-industrial-inspections-2026/#:~:text=Align%20safety%20and%20environmental%20goals,December%202029%2C%202025>. – Дата доступа: 21.01.2026.

[11] Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа : <https://pravo.by/novosti/novosti-pravo-by/2022/december/72610/>. – Дата доступа: 20.01.2026.

Авторский вклад

Авторы внесли равнозначный вклад.

USE OF ARTIFICIAL INTELLIGENCE IN INDUSTRIAL SAFETY

E. N. Bychek

*Student of the Department of Engineering
Psychology and Ergonomics, BSUIR*

N. V. SHCHerbina

*Senior Lecturer, Department of Engineering
Psychology and Ergonomics, BSUIR, Master of
Technical Sciences*

Abstract. The article analyzes the role of artificial intelligence (AI) technologies in the transformation of industrial safety systems based on current industry sources. Key areas of AI application are considered: from predictive analytics and computer vision to intelligent personal protective equipment. Special attention is paid to the shift from reactive to proactive incident prevention strategies. The work also systematizes the main ethical and organizational challenges associated with the implementation of AI, including issues of trust, transparency, and privacy.

Keywords: industrial safety, artificial intelligence, computer vision, intelligent wearables, predictive analytics, ethics, occupational safety, monitoring, equipment failure.