

А. В. Дубровский^{1✉}

Техносферная безопасность и искусственный интеллект в современном образовательном контексте

¹Сибирский государственный университет геосистем и технологий, г. Новосибирск,
Российская Федерация
e-mail: avd5@ssga.ru

Аннотация. В статье рассматривается трансформация сущности техносферной безопасности под влиянием глобальных технологических трендов, в первую очередь – стремительного развития систем искусственного интеллекта. Анализируется двойственная роль искусственного интеллекта как источника новых техносферных рисков и как инструмента для их минимизации. Особое внимание уделяется нормативно-правовым рамкам, регулирующим безопасность образовательной среды в условиях цифровизации. На основе анализа актуальных вызовов предложены направления обновления содержания программы подготовки по направлению «Техносферная безопасность», включая внедрение социотехнического подхода и формирование компетенций в области безопасного применения искусственного интеллекта.

Ключевые слова: образовательный контекст, технологические риски, цифровая образовательная среда, подготовка кадров, нормативно-правовое регулирование

A. V. Dubrovsky^{1✉}

Technosphere Safety and Artificial Intelligence in the Modern Educational Context

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: avd5@ssga.ru

Annotation. The article examines the transformation of the essence of technosphere safety under the influence of global technological trends, primarily the rapid development of artificial intelligence systems. The article analyzes the dual role of artificial intelligence as a source of new technosphere risks and as a tool for minimizing them. Special attention is paid to the regulatory framework governing the safety of the educational environment in the context of digitalization. Based on the analysis of current challenges, the article proposes directions for updating the content of the training program in the field of technosphere safety, including the implementation of a sociotechnical approach and the development of competencies in the safe use of artificial intelligence.

Keywords: educational context, technological risks, digital educational environment, personnel training, and legal regulation

Введение

Современный этап развития характеризуется глубочайшей технологической трансформацией, ядром которой выступает искусственный интеллект (ИИ). Отнесение ИИ и прорывных технологий к числу глобальных рисков номер один на период 2025–2033 годов, согласно докладу ООН, фиксирует новую реальность: техносфера перестала быть просто суммой машин и механизмов, превратившись

в сложную, самообучающуюся киберфизическую среду [1]. Это фундаментально меняет сущность техносферной безопасности (ТСБ).

Если классическое понимание ТСБ фокусировалось на защите человека и природы от опасностей, которые представляют промышленных объектов, то сегодня в образовательном контексте мы сталкиваемся с необходимостью подготовки специалистов, способных обеспечивать безопасность в условиях, когда объект защиты и источник угрозы могут быть «гибридными»: сочетать физические и виртуальные компоненты, обладать элементами автономности и непредсказуемости. Цель данной статьи – проанализировать, как глобальные технологические тренды, связанные с ИИ, трансформируют содержание техносферной безопасности и каким образом система высшего образования должна отвечать на эти вызовы в рамках обновления подходов к подготовке кадров.

Методы и материалы

Теоретико-методологическую основу исследования составили системный анализ и социотехнический подход, позволяющие рассматривать безопасность как результат взаимодействия сложных технологических и социальных систем. В работе использованы методы анализа нормативно-правовой документации (федеральные законы, концепции регулирования ИИ), сравнительного анализа научных и экспертных публикаций, а также метод проблемно-теоретической реконструкции для выявления новых требований к компетенциям выпускников.

Материалами для исследования послужили:

- доклады и отчеты международных организаций [1];
- актуальные исследования экспертных центров в области кибербезопасности и ИИ («Лаборатория Касперского», Институт системного программирования им. В.П. Иванникова РАН) [2];
- аналитические материалы по вопросам безопасности образовательной среды и регулирования ИИ в России и за рубежом [3, 4];
- научные публикации, посвященные проблемам безопасности и социальным аспектам машинного обучения [5–7].

Результаты

Трансформация сущности техносферной безопасности под влиянием ИИ. Внедрение ИИ приводит к конвергенции физических и цифровых угроз, что требует переосмысления самой категории «техносферная безопасность». Академик РАН А. Аветисян на Российском форуме «Микроэлектроника -2025» подчеркнул принципиально новый, комплексный характер угроз, связанных с ИИ: они имеют два неразрывных измерения – традиционную кибербезопасность и социогуманитарное [2]. Это означает, что авария на производстве сегодня может быть спровоцирована не только поломкой станка или ошибкой оператора, но и успешной «промпт-инъекцией» в систему управления, либо «отравлением» (искажением) данных, на которых обучалась предиктивная аналитика.

Таким образом, сущность техносферной безопасности в современном контексте расширяется с защиты от опасностей физического мира к

обеспечению устойчивости и доверия к киберфизическим системам. Безопасность становится синонимом способности системы сохранять заданный режим функционирования в условиях, когда противник (или сбой) может воздействовать не на «железо», а на алгоритмы обработки и данные.

Влияние глобальных технологических трендов на техносферные риски. Анализ источников угроз позволяет выделить ключевые тренды, формирующие новые контуры рисков:

- автономные ИИ-агенты: передача агентам (программам, способным самостоятельно выполнять действия) управления критическими процессами, от мониторинга инфраструктуры до принятия решений (например, совершения покупок, управления транспортом, технологическими процессами и др.) создает риск неконтролируемого поведения (галлюцинации) или эксплуатации уязвимостей агента злоумышленниками.

- сложность верификации: генеративные модели делают практически невозможным различение истинной и синтезированной информации (дипфейки), что подрывает доверие к данным мониторинга и может дезориентировать лиц, принимающих решения в чрезвычайных ситуациях;

- когнитивные риски: использование ИИ для манипуляции поведением, в том числе через «умные» образовательные среды и чат-боты, несет риски для психического здоровья и развития критического мышления у обучающихся.

Нормативно-правовые рамки техносферной безопасности в образовании. Правовое поле в этой сфере находится в стадии активного формирования. Ключевые векторы задаются как общим регулированием ИИ, так и специальными нормами для образования. Разработкой безопасных, этичных и надёжных технологий искусственного интеллекта в России занимается Консорциум исследований безопасности технологий искусственного интеллекта, основанный Институтом системного программирования РАН, АНО «Национальный технологический центр цифровой криптографии» и Академией криптографии Российской Федерации.

Российский контекст характеризуется обновленной Концепцией регулирования ИИ, разработанной в Государственной Думе [3]. Концепция провозглашает человекоцентричный подход. Критически важным для образования является прямой запрет на использование ИИ для «механического решения задач за студентов», что должно стимулировать развитие педагогических методик, а не их замену. В профессиональной сфере активно обсуждаются стандарты безопасной разработки систем машинного обучения. Анализ российских правовых исследований показывает необходимость введения в научный оборот и законодательство четкого определения «безопасность образовательной среды», которое учитывало бы не только информационные, но и психолого-педагогические аспекты взаимодействия с ИИ.

Зарубежный опыт демонстрирует схожие озабоченности. При этом, например, в Австралии искусственный интеллект, включая ChatGPT, разрешено использовать во всех школах с 2024 года [4].

Трансформация образовательных тенденций в подготовке по ТСБ. Сложившийся разрыв между академическими программами и потребностями индустрии в сфере ИИ требует пересмотра учебных планов направления «Техносферная безопасность» в следующих направлениях:

- социотехнический подход в инженерном образовании: курсы по ТСБ должны включать не только технические дисциплины, но и модули по этике ИИ, философии технологий и анализу когнитивных рисков. Примером служат различные конференции и научные семинары, рассматривающие вопросы взаимодействия искусственного интеллекта и общества, рассматривающие машинное обучение с социальными и философскими аспектами;

- формирование компетенций по «доверенному ИИ»: специалист по ТСБ должен понимать уязвимости моделей («отравление» или искажение данных, состязательные атаки – данные, на которых система работает неверно (вообще не работает, работает с низким качеством), и владеть методами обеспечения их надежности на всех этапах жизненного цикла;

- интеграция с кибербезопасностью: Стирание граней между физической и информационной безопасностью требует подготовки «гибридных» специалистов. Знание основ KasperskyOS или методов федеративного обучения становится конкурентным преимуществом [8].

Обсуждение

Полученные результаты позволяют утверждать, что техносферная безопасность переживает парадигмальный сдвиг (фундаментальное изменение в общепринятой модели мышления, научных взглядах и системе ценностей). Искусственный интеллект выступает в трех сущностях: как объект изучения (как сделать ИИ-системы безопасными), как инструмент (как с помощью ИИ повысить уровень безопасности) и как катализатор изменений среды (как ИИ меняет природу угроз).

Наиболее дискуссионным вопросом остается баланс между регуляторикой и инновациями. Запретительные меры, такие как ограничения на использование ИИ в образовании или тотальный запрет распознавания эмоций, могут защитить от рисков, но одновременно лишают студентов и преподавателей возможности освоить критически важные технологии.

«Следующие 10–15 лет станут временем «колоссальной технологической трансформации» и развития искусственного интеллекта, заявил президент Владимир Путин на заседании Госсовета. По его мнению, внедрение ИИ является более прорывной технологией, чем освоение космоса» [9].

Представляется, что оптимальной стратегией является не изоляция, а формирование культуры безопасного использования и развитие критического мышления, на что указывают и эксперты «Лаборатории Касперского».

Еще одним важным аспектом является проблема «цифровых островов» и устаревания знаний. Учебные программы по ТСБ должны не просто транслировать текущее знание, но и формировать у студентов способность адаптироваться к технологиям, которых еще не существует. Это требует перехода от модели

«передачи знаний» к модели «развития способности учиться и переучиваться» в быстро меняющейся техносреде.

Заключение

Техносферная безопасность в эпоху искусственного интеллекта трансформируется в междисциплинарную область, лежащую на стыке инженерии, информатики, когнитивной науки и права. Современный образовательный контекст требует от системы подготовки кадров по направлению «Техносферная безопасность» оперативного ответа на вызовы автономности, непрозрачности и двойного назначения ИИ-технологий. Ключевыми векторами этой трансформации должны стать: внедрение социотехнических модулей в учебные планы, формирование компетенций в области анализа и обеспечения безопасности киберфизических систем, а также активное развитие у студентов навыков критического мышления и работы с «доверенными» ИИ-решениями. Дальнейшие исследования в этой области должны быть направлены на разработку конкретных дидактических единиц и методик оценки эффективности новых образовательных моделей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Доклад ООН: внедрение искусственного интеллекта затронет 40 процентов рабочих мест/ Новости ООН [Электронный ресурс] – Режим доступа: <https://news.un.org/ru/story/2025/04/1462941>.
2. Как обеспечить доверенный ИИ в критической информационной инфраструктуре рассказал академик Арутюн Аветисян. РАН [Электронный ресурс] – Режим доступа: <https://new.ras.ru/press-center/kak-obespechit-doverennyi-ii-v-kriticheskoy-informatsionnoy-infrastrukture-rasskazal-akademik-arutyu>.
3. Стогова Е. В Госдуме сформулировали определение искусственного интеллекта. РБК. Технологии и медиа [Электронный ресурс] – Режим доступа: https://www.rbc.ru/technology_and_media/04/09/2025/68b8eec99a79477a1859ed11.
4. В школах Австралии решили разрешить использование ИИ. ИА Красная Весна [Электронный ресурс] – Режим доступа: <https://rossaprimavera.ru/news/c08c1634>.
5. Глухов, А. П. Социально-профессиональные вызовы и методологические аспекты внедрения ИИ в образовательную среду школы / А. П. Глухов, Е. С. Синогина // Вестник Томского государственного педагогического университета. – 2025. – № 5(241). – С. 110-121. – DOI 10.23951/1609-624X-2025-5-110-121.
6. Янукович, М. Ф. Цифровой соавтор: как ИИ меняет природу творчества и смысла / М. Ф. Янукович // Вестник Пермского университета. Философия. Психология. Социология. – 2025. – № 4. – С. 506-515. – DOI 10.17072/2078-7898/2025-4-506-515.
7. Алехина, Е. В. Искусственный интеллект и человеческий разум в перспективе глобализации / Е. В. Алехина, Н. Н. Каргин // Современные философские исследования. – 2025. – № 3. – С. 58-72. – DOI 10.18384/2949-5148-2025-2-58-72.
8. Джат Ю. Что такое федеративное обучение ИИ и в чем его преимущества. Ростелеком [Электронный ресурс] – Режим доступа: <https://blog.rt.ru/b2c/chto-takoe-federativnoe-obuchenie-ii-i-v-chem-ego-preimuschestva.htm>.
9. Путин В. В. назвал искусственный интеллект «более прорывной технологией», чем освоение космоса. Коммерсантъ <https://www.kommersant.ru/doc/8317128>.

© А. В. Дубровский, 2026