2. Хутская, Н. Г. Циклы паросиловых установок : учеб.-метод. пособие по дисциплине «Термодинамика» для студентов специальности «Энергоэффективные технологии и энергетический менеджмент» / Н. Г. Хутская, Г. И. Пальченок, А. В. Новик. – Минск : БНТУ, 2022 – 56 с.
3. International Energy Agency. Key World Energy Statistics – URL: http://www.iea.org/publications/freepublications/publication/KeyWorld2014 (дата обращения: 05.10.2025).

PRIVACY RISKS IN THE AGE OF ARTIFICIAL INTELLIGENCE: CHALLENGES AND SAFEGUARDS

O. A. S. M. AL-Ameri[1], M. F. S. H. Al-Kamali[2]

[1]Belarusian State University of Informatics and Radioelectronics, Minsk

[2] Sukhoi State Technical University of Gomel, Republic of Belarus

This study explores the privacy risks associated with artificial intelligence (AI) amidst rapid technological advancements. It highlights concerns related to data collection, consent, and unauthorized use, emphasizing the challenges these pose for individual privacy. The study also discusses the need for robust regulatory frameworks to safeguard personal information in the age of AI, ensuring that innovation does not infringe on privacy rights.

Keywords: privacy risks, artificial intelligence, data Protection, consent, regulatory frameworks, surveillance.

РИСКИ КОНФИДЕНЦИАЛЬНОСТИ В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОБЛЕМЫ И МЕРЫ ПРЕДОСТОРОЖНОСТИ

О. А. С. М. Аль-Амери[1], М. Ф. С. Х. Аль-Камали[2]

[1]Белорусский государственный университет информатики и радиоэлектроники, г. Минск

[2]Гомельский государственный технический университет имени П. О. Сухого, Республика Беларусь

Рассмотрены риски нарушения конфиденциальности, связанные с искусственным интеллектом (ИИ) в условиях стремительного развития технологий, а также проблемы, связанные со сбором данных, согласием и несанкционированным использованием. Подчеркнуты проблемы, которые они создают для конфиденциальности личности. В исследовании также обсуждена необходимость создания надежной нормативно-правовой базы для защиты персональных данных в эпоху ИИ, гарантирующей, что инновации не нарушают права на неприкосновенность частной жизни.

Ключевые слова: риски нарушения конфиденциальности, искусственный интеллект, защита данных, согласие, нормативно-правовая база, наблюдение.

As technology advances, it brings with it a host of risks, particularly concerning privacy. Tools that enhance data collection and analysis simultaneously increase the chances of misuse of personal and sensitive information. This privacy risk is particularly pronounced in the era of artificial intelligence (AI), where vast amounts of sensitive data are collected to build and refining AI and machine learning systems. While policymakers are striving to address these privacy concerns through regulations, they inadvertently create compliance challenges for organizations utilizing AI in decision-making processes. Despite these concerns, companies continue to implement AI models to enhance productivity and deliver value [1, 2].

This study delves into the privacy risks associated with AI and examines the safeguards that impact society and commerce today. AI privacy involves protecting personal or sensitive information collected, used, shared, or stored by AI systems. This

concept is closely related to data privacy, which asserts that individuals should control their personal data – determining how organizations collect, store, and utilize it. Although the notion of data privacy predates AI, societal attitudes toward it have evolved alongside technological advancements.

A decade ago, individuals primarily considered data privacy in the context of online shopping, often expressing indifference about companies tracking their purchases. However, as AI systems have begun to collect data more broadly, privacy concerns have escalated, particularly regarding civil rights implications. Key privacy risks tied to AI include: the collection of sensitive data, obtaining data without consent, unauthorized use of data, unchecked surveillance, bias, unauthorized data transfers, and potential data leaks.

One reason AI poses a greater risk to data privacy compared to previous technological developments is the sheer volume of information it processes. AI systems routinely handle terabytes or petabytes of data, which often include sensitive information such as healthcare data, personal social media content, and financial records. With more sensitive data being collected and stored than ever before, the likelihood of breaches or unauthorized disclosures increases significantly.

Controversies often arise when data is collected to develop AI systems without individuals' explicit consent. Users of various platforms now expect greater transparency and autonomy regarding their data. For instance, LinkedIn faced backlash when users discovered they had been automatically opted in to allow their data to be used for training generative AI models.

Even when data is collected with consent, privacy risks remain if the data is repurposed beyond the initially disclosed uses. For example, a patient in California discovered that images taken for a medical procedure were used in an AI training dataset without her consent. Such scenarios highlight the pervasive nature of privacy concerns in AI.

Surveillance practices – such as the use of security cameras in public spaces or tracking cookies on personal devices – existed long before AI emerged, but AI could exacerbate these issues. AI models are often employed to analyze surveillance data, and the results can sometimes reflect bias, leading to harmful outcomes, such as wrongful arrests linked to AI-driven law enforcement decisions.

AI models also store vast amounts of sensitive data, making them attractive targets for malicious actors. Unauthorized data transfers can occur through various means, including point-injection attacks where attackers disguise harmful inputs as legitimate requests, tricking AI systems into revealing sensitive information. For instance, an attacker could manipulate a virtual assistant powered by a large language model to request private documents.

Data leaks, which involve accidental exposure of sensitive information, are another significant concern. For example, OpenAI’s ChatGPT, a prominent large language model, inadvertently exposed some users’ chat log addresses. Smaller proprietary AI models also face similar risks; a healthcare company's in-house AI diagnostic tool could unintentionally leak customer data to others using the same network.

Policymakers have sought to protect individual privacy from technological advances since at least the 1970s. However, the rapid expansion of commercial data collection and AI deployment has intensified the urgency for comprehensive data privacy laws. Notable regulations include the EU’s General Data Protection Regulation (GDPR), the EU Artificial Intelligence Act, U.S. privacy regulations, and China’s interim measures for managing generative AI services.

While AI presents remarkable opportunities for innovation, it also raises significant privacy concerns that must be addressed through effective governance and regulatory frameworks. As the landscape of data privacy continues to evolve, the implementation of

stringent safeguards will be crucial for ensuring that technological advancements do not come at the expense of individual privacy rights.

Reference

1. Al-Billeh, T., Hmaidan, R., Al-Hammouri, A., and Al Makhmari, M. (2024). The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards. Jurnal Media Hukum, 2024, no. 31 (2), pp. 333–350.
2. S. Shahriar, S. Allana, S. M. Hazratifard and R. Dara, "A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle," in IEEE Access, vol. 11, pp. 61829–61854, 2023. Doi 10.1109/ACCESS.2023.3287195

DIGITAL TRANSFORMATION IN YEMEN'S HEALTHCARE SECTOR: ENHANCING DATA PROTECTION AND RESILIENCE

J. A. A. Blalah[1], M. F. S. H. Al-Kamali[2]

[1]Scientific Organization for Research and Innovation, Yemen

[2]Sukhoi State Technical University of Gomel, Republic of Belarus

This works examines technology-based strategies for enhancing data protection and digital resilience in Yemen's healthcare sector amidst ongoing challenges. It emphasizes the importance of secure systems to improve healthcare access and patient trust.

Keywords: data protection, digital resilience, healthcare transformation, Yemen, telemedicine.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В СЕКТОРЕ ЗДРАВООХРАНЕНИЯ ЙЕМЕНА: ПОВЫШЕНИЕ ЗАЩИТЫ ДАННЫХ И УСТОЙЧИВОСТИ

Дж. А. А. Блала[1], М. Ф. С. Х. Аль-Камали[2]

[1]Научная организация исследований и инноваций, Йемен

[2]Гомельский государственный технический университет имени П. О. Сухого, Республика Беларусь

Рассмотрены технологические стратегии повышения защиты данных и цифровой устойчивости в секторе здравоохранения Йемена в условиях сохраняющихся трудностей. Подчеркивается важность безопасных систем для улучшения доступа к медицинской помощи и повышения доверия пациентов.

Ключевые слова: защита данных, цифровая устойчивость, трансформация здравоохранения, Йемен, телемедицина.

As Yemen navigates a complex landscape shaped by ongoing conflict and economic hardships, the digital transformation of its healthcare system has become increasingly essential. The integration of technology in healthcare offers significant opportunities to improve access to medical services and enhance patient outcomes. However, this transition raises critical concerns regarding data protection and privacy. Ensuring the security of sensitive health information is vital for maintaining patient trust and fostering effective healthcare delivery in Yemen. This work explores technology-based strategies aimed at enhancing digital resilience in the Yemeni healthcare sector, with a particular focus on data protection measures that can mitigate risks associated with digital health systems.

The healthcare system in Yemen faces numerous challenges, including limited resources, a fragmented infrastructure, and ongoing conflicts that complicate service