AI-POWERED INTELLIGENT CENTERS: OPTIMIZING INFORMATION INFRASTRUCTURE OF UNIVERSITIES AMID WAR

Abstract. The core objective of this article is to investigate how AI-powered intelligent centers can optimize the information infrastructure of universities amid wartime challenges, particularly focusing on Ukrainian institutions facing unprecedented disruptions. The scientific problem addressed is the need for robust and adaptive information systems that sustain educational activities, ensure data security, and provide real-time support to students and staff. The research aims to provide a roadmap for universities to maintain and improve their operations and educational outcomes despite the ongoing conflict.

The research reveals that AI-powered intelligent centers significantly enhance educational experiences, operational efficiency, and institutional resilience. Key features identified include data integration, predictive analytics, virtual assistants, adaptive learning, administrative automation, AI-driven cybersecurity, intelligent tutoring systems, research support, resource management, and personalized communication. These features collectively address critical needs within the university ecosystem, enabling better decision-making, resource optimization, and personalized education.

The findings offer valuable insights for policymakers and educational institutions. Investments in high-performance servers, machine learning models, AI chatbot software, adaptive learning platforms, RPA tools, AI-driven cybersecurity solutions, and intelligent tutoring software are essential. Additionally, developing disaster recovery plans, enhancing cybersecurity measures, securing international grants, and providing mental health support services are crucial for navigating wartime challenges.
This study distinguishes itself by addressing the unique context of war-torn regions, emphasizing the transformative potential of AI in maintaining and advancing educational infrastructure. It contributes significantly to understanding contemporary security challenges and offers practical solutions for enhancing the resilience and efficiency of universities amid conflict.

**Keywords:** artificial intelligence, higher education in wartime, information infrastructure, intelligent center, university.

Харченко Олександр Анатолійович кандидат технічних наук, доцент, декан факультету інформаційних технологій, Державний торговельно-економічний університет, вул. Кіото, 19, м. Київ, 02156, тел.: (066) 951-00-83, https://orcid.org/0000-0002-9255-9287

Савон Олексій Євгенійович аспірант кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, вул. Кіото, 19, м. Київ, 02156, тел.: (044) 531-49-57, https://orcid.org/0009-0006-4905-8969

ІНТЕЛЕКТУАЛЬНІ ЦЕНТРИ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ: ОПТИМИЗАЦІЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УНІВЕРСИТЕТЕВ У УМОВАХ ВІЙНИ

Анотація. Основною метою статті є визначення, яким чином інтелектуальні центри на основі штучного інтелекту можуть оптимізувати інформаційну інфраструктуру університетів в умовах викликів воєнного часу, зокрема, на основі аналізу українських закладів вищої освіти, які стикаються з безпрецедентними викликами освітній діяльності. Наукова проблема, окреслена в статті, полягає в необхідності створення надійних та адаптивних інформаційних систем, які підтримують освітню діяльність, забезпечують безпеку даних і надають підтримку студентам, науково-педагогічним працівникам і співробітникам у режимі реального часу. Дослідження має на меті надати дорогу карту для закладів вищої освіти, щоб підтримувати та покращувати їхню діяльність та освітні результати, незважаючи на війну, що триває.

У статті показано, що інтелектуальні центри на основі штучного інтелекту значно покращують освітній досвід, операційну ефективність та інституційну стійкість. До ключових особливостей таких центрів належать інтеграція даних, предиктивна аналітика, віртуальні асистенти, адаптивне навчання, автоматизація адміністрування, кібербезпека на основі ШІ, інтелектуальні системи навчання, підтримка досліджень, управління ресурсами та персоналізована комунікація. Ці функції в сукупності задовольняють критичні потреби університетської екосистеми, забезпечуючи краще прийняття рішень, оптимізацію ресурсів та персоналізовану освіту.
Результаты доследження надають цінну інформацію для політиків та закладів вищої освіти. Інвестиції у високопродуктивні сервери, моделі машинного навчання, програмне забезпечення для чат-ботів зі штучним інтелектом, адаптивні навчальні платформи, інструменти RPA, рішення для кібербезпеки на основі штучного інтелекту та інтерактивальні навчальні програмне забезпечення є вкрай необхідними. Крім того, розробка планів післяаварійного відновлення, посилення заходів кібербезпеки, отримання міжнародних грантів та надання послуг з підтримки психічного здоров’я науково-педагогічних працівників, співробітників і студентів мають вирішальне значення для подолання викликів воєнного часу.

Це дослідження вирізняється тим, що розглядає унікальний контекст регіонів, охоплених війною, підкреслюючи трансформаційний потенціал штучного інтелекту в підтримку та розвитку освітньої інфраструктури. Воно робить значний внесок у розуміння сучасних викликів безпеці та пропонує практичні рішення для підвищення стійкості та ефективності закладів вищої освіти в умовах збройного конфлікту високої інтенсивності.

Ключові слова: штучний інтелект, вища освіта під час війни, інформаційна інфраструктура, інтелектуальний центр, університет.

Statement of the problem. The optimization of information infrastructure in universities amid war is an urgent challenge, particularly for Ukrainian institutions facing unprecedented disruptions. Wartime conditions amplify the importance of robust and adaptive information systems that can sustain educational activities, ensure data security, and provide real-time support to students and staff. The integration of AI-powered intelligent centers offers transformative solutions, yet it demands significant investment in technology, skilled personnel, and data resources. By exploring these innovations, the article connects directly to essential scientific and practical tasks, aiming to provide a roadmap for universities to maintain and improve their operations and educational outcomes despite the ongoing conflict.

Analysis of recent studies and publications. The optimization of university information infrastructure and the implementation of artificial intelligence (AI) in education are widely discussed in academic literature. Li emphasizes the importance of efficiently allocating teaching resources in universities, proposing an enhanced adaptive genetic algorithm integrated with BP network training. This algorithm addresses slow evolution and poor population diversity by introducing new parameters for crossover and mutation probabilities, along with using momentum and adaptive learning rate strategies to optimize BP network performance. AI deployment within wireless networks facilitates efficient data collection, processing, and transmission, optimizing university resources, a method validated for reliability and effectiveness by extensive experiments [1]. However, Li’s work does not address the security and resilience of AI and wireless networks against cyber threats,
crucial in war scenarios, nor does it discuss scalability and flexibility, essential in rapidly changing war conditions.

Greshta, Shylo, Korolkov, Kulykovskyi, and Kapliienko explore the challenges faced by higher education institutions in war zones, specifically Ukraine, focusing on the National University “Zaporizhzhia Polytechnic”. Their study highlights efforts to maintain digital educational services through relocating staff to safer regions, securing power supplies with battery systems and diesel generators, and using backup internet channels and satellite communication via Starlink. Organizational adjustments, new software, and innovative communication tools, supported by the Ministry of Education and Science of Ukraine, are deemed crucial. Their experience offers valuable insights for other institutions in similar scenarios [2, pp. 85-86]. However, the study overlooks the unique capabilities of AI in managing and securing digital infrastructure, such as predictive maintenance, automated resource allocation, and intelligent threat detection.

Wang, Du, and Wu discuss the direct impact of a university’s information services platform on its management. With vast data resources and complex management needs, creating a comprehensive and efficient platform is a research focus where AI advancements hold significant promise for smart campus applications. Their exploration into developing a secure university information services platform using AI, specifically intelligent dormitory allocation and face recognition, utilizes the beetle antennae search algorithm to enhance the K-means algorithm for better clustering, and an improved VAE-GAN model with a CNN-based algorithm boosts security. Simulation results validate these improvements in efficiency and security [3]. However, the discussion lacks a broader perspective on optimizing overall information infrastructure using AI and does not address practical challenges in implementing these technologies in a war-torn environment.

Lin, Huang, Zhang, and Chang examine the influence of administrative mechanisms on university operations, integrating AI and corporate governance. They propose solutions for issues such as unclear role definitions and insufficient departmental cooperation, aiming to enhance interdepartmental communication and cooperation for better services and higher management efficiency [4]. However, their focus on administrative reform and general management efficiency lacks direct relevance to the technical aspects of AI-powered intelligent centers and their role in information infrastructure optimization.

Drach, Petroye, Borodiyenko, Reheilo, Bazeliuk, Bazeliuk, and Slobodianiuk delve into the theoretical foundations and practical applications of AI in higher education, reviewing policies from global organizations like UNESCO, the European Union, and the OECD on effective AI use. They systematize ethical principles for AI integration, including human-centered values, transparency, accountability, sustainability, confidentiality, safety, and inclusiveness. A SWOT analysis identifies strengths, weaknesses, opportunities, and risks associated with AI
in higher education, with practical recommendations established based on a 2023 national survey on Open Science involving over 1,500 respondents [5, p. 76]. Nonetheless, their broad discussion on ethical principles lacks practical insights on applying these principles in universities operating in war zones.

López-Chila, Llerena-Izquierdo, Sumba-Nacipucha, and Cueva-Estrada conduct a bibliometric study reviewing AI in higher education to guide future research. Their analysis of 870 articles from the Scopus database between 2017 and 2023 shows a significant rise in AI studies, particularly in computer science and social sciences, with leading publications from China and the U.S. [6]. Despite this, the text lacks concrete examples or strategies for implementing AI in conflict-affected universities.

Wildman, Diallo, Hodulik, Page, Tolk, and Gondal introduce The Artificial University (TAU), an open-source simulation model of a university using a contact network based on public data. This study evaluates various interventions and testing protocols for a simulated university with 6,500 individuals, highlighting the importance of rapid test results and targeted testing [7]. However, it diverges from discussing how AI can enhance university information systems' resilience, efficiency, and security, crucial for AI-powered intelligent centers.

Chepkii, Skachkov, Yefymchykov, Nabok, Honcharuk, and Yelchaninov focus on modernizing IT infrastructure in military professional training using cloud computing and virtualization technology. They propose a complex cloud IT-infrastructure model with hardware for cloud services at the physical level and software at the abstract level, recommending access to VMs through a secure shell [8, p. 199]. Although detailed, this focus limits relevance to broader university settings, particularly those affected by war. The text does not explore how proposed cloud infrastructure and virtualization can ensure resilience and security of university information systems in war-torn regions.

Despite providing insights into various aspects of optimizing university information infrastructure and implementing AI in education, there is a lack of research on the peculiarities of establishing AI-powered intelligent centers at universities during the war.

The purpose of the article is to investigate how AI-powered intelligent centers can optimize the information infrastructure of universities amidst wartime challenges by enhancing educational experiences, operational efficiency, and institutional resilience.

Outline of the main material. The integration of AI-powered intelligent centers into the information infrastructure of universities presents a transformative opportunity to enhance educational experiences and institutional efficiency. Each feature, from data integration to personalized communication, brings unique benefits that address specific needs within the university ecosystem. However, the successful implementation of these features at Ukrainian universities requires significant investment in technology, skilled personnel, and data resources (Table 1).
### Table 1. Key features of AI-powered intelligent centers in university information infrastructure

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Required resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data integration</td>
<td>Centralizes and integrates data from various sources for comprehensive analysis.</td>
<td>High-performance servers, data integration software, data scientists.</td>
</tr>
<tr>
<td>Predictive analytics</td>
<td>Uses machine learning to predict student outcomes and optimize resources.</td>
<td>Machine learning models, historical data, analytics software.</td>
</tr>
<tr>
<td>Virtual assistants</td>
<td>AI-powered chatbots to provide 24/7 support to students and staff.</td>
<td>AI chatbot software, training data, natural language processing (NLP) specialists.</td>
</tr>
<tr>
<td>Administrative automation</td>
<td>Automates routine administrative tasks to improve efficiency.</td>
<td>Robotic process automation (RPA) tools, administrative data, IT support.</td>
</tr>
<tr>
<td>Cybersecurity enhancement</td>
<td>Utilizes AI to detect and mitigate cyber threats in real-time.</td>
<td>AI-driven cybersecurity solutions, cybersecurity experts, threat intelligence data.</td>
</tr>
<tr>
<td>Intelligent tutoring systems</td>
<td>Provides personalized tutoring using AI to address individual learning needs.</td>
<td>Intelligent tutoring software, student data, AI tutors.</td>
</tr>
<tr>
<td>Research support</td>
<td>AI tools to aid in research by analyzing large datasets and identifying trends.</td>
<td>Data analysis tools, research data, domain experts.</td>
</tr>
<tr>
<td>Resource management</td>
<td>Optimizes the use of campus resources such as classrooms and equipment.</td>
<td>Resource management software, IoT devices, data analysts.</td>
</tr>
<tr>
<td>Personalized communication</td>
<td>Tailors communication to individual students’ needs and preferences.</td>
<td>CRM systems, AI algorithms, communication data.</td>
</tr>
</tbody>
</table>

*Source: elaborated by the authors*

Data integration is the backbone of any AI-powered intelligent center. It involves collecting and centralizing data from multiple sources such as student records, administrative systems, and learning management systems. The essence of this feature lies in its ability to provide a comprehensive view of all university operations, enabling better decision-making and strategic planning. To establish this feature at Ukrainian universities, high-performance servers are required to handle...
the large volumes of data. Additionally, data integration software and skilled data scientists are essential to ensure that the data is accurately collected, processed, and analyzed.

Predictive analytics leverages machine learning algorithms to analyze historical data and predict future outcomes. In a university setting, this can be used to forecast student performance, identify at-risk students, and optimize resource allocation. The essence of this feature is its ability to transform data into actionable insights, which can significantly enhance student success rates and institutional efficiency. Implementing predictive analytics at Ukrainian universities necessitates the availability of machine learning models and historical data, as well as analytics software to process the data. Skilled data analysts and machine learning specialists are also crucial to develop and maintain these predictive models.

AI-powered virtual assistants or chatbots provide 24/7 support to students and staff, addressing common queries and offering guidance on administrative processes. The essence of this feature is its ability to enhance accessibility and convenience, reducing the workload on administrative staff and providing timely assistance to users. Establishing virtual assistants at Ukrainian universities requires AI chatbot software and extensive training data to ensure the chatbots can handle a wide range of queries. Natural language processing (NLP) specialists are also needed to refine the chatbot’s ability to understand and respond to user inputs accurately.

Adaptive learning platforms tailor the educational experience to each student's unique needs, preferences, and performance levels. This personalized approach helps in addressing learning gaps and promoting better academic outcomes. The essence of adaptive learning lies in its ability to create a more engaging and effective learning environment. To implement adaptive learning at Ukrainian universities, it is necessary to have access to adaptive learning platforms, detailed student performance data, and instructional designers who can develop personalized learning content.

Administrative automation involves using AI to streamline routine administrative tasks such as scheduling, grading, and record-keeping. This feature enhances operational efficiency and frees up staff to focus on more strategic activities. The essence of administrative automation is its potential to reduce errors and improve the overall administrative workflow. To establish this feature at Ukrainian universities, robotic process automation (RPA) tools are required, along with comprehensive administrative data and IT support to integrate and maintain the automation systems.

AI-driven cybersecurity solutions can detect and respond to cyber threats in real-time, providing a robust defense against data breaches and other cyber-attacks. The essence of this feature is its ability to enhance the security of the university's information infrastructure, protecting sensitive data from unauthorized access.
Implementing this feature at Ukrainian universities necessitates AI-powered cybersecurity tools, access to threat intelligence data, and cybersecurity experts who can monitor and manage the security systems effectively.

Intelligent tutoring systems use AI to provide personalized tutoring to students, adapting to their individual learning needs and styles. This feature supports students in achieving their academic goals by offering targeted assistance. The essence of intelligent tutoring systems is their ability to provide customized support that can address specific learning challenges faced by students. Establishing these systems at Ukrainian universities requires intelligent tutoring software, access to student performance data, and AI tutors who can design and deliver personalized tutoring sessions.

AI tools can significantly enhance research capabilities by analyzing large datasets, identifying patterns, and providing insights that might not be apparent through traditional analysis methods. The essence of this feature is its ability to accelerate research processes and uncover new knowledge. To implement AI-driven research support at Ukrainian universities, data analysis tools are required, along with access to extensive research data and collaboration with domain experts who can interpret and apply the findings.

AI can optimize the utilization of campus resources such as classrooms, laboratories, and equipment by predicting demand and scheduling accordingly. The essence of resource management is its ability to maximize efficiency and reduce wastage of resources. Implementing this feature at Ukrainian universities involves using resource management software, Internet of Things (IoT) devices to track resource usage, and data analysts to manage and optimize the resource allocation process.

AI can tailor communication to individual students based on their preferences, behaviors, and needs, ensuring that they receive relevant information and support. The essence of personalized communication is its ability to enhance student engagement and satisfaction. To establish this feature at Ukrainian universities, customer relationship management (CRM) systems integrated with AI algorithms are required, along with access to communication data and skilled personnel to manage and maintain these systems.

Establishing AI-powered intelligent centers in Ukrainian universities during the ongoing war presents significant challenges. However, by identifying and addressing key threats through strategic mitigation measures, universities can navigate these challenges and continue to advance their educational and technological capabilities (Table 2).
### Table 2. Key threats and mitigation strategies for establishing AI-powered universities’ intelligent centers during the war

<table>
<thead>
<tr>
<th>Threats</th>
<th>Essence</th>
<th>Mitigation measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure damage</td>
<td>Physical damage to university buildings and IT infrastructure.</td>
<td>Develop and implement robust disaster recovery plans, establish off-site backups, and utilize cloud services.</td>
</tr>
<tr>
<td>Cyber-attacks</td>
<td>Increased risk of cyber-attacks targeting educational institutions.</td>
<td>Implement advanced cybersecurity measures, conduct regular security audits, and provide cybersecurity training.</td>
</tr>
<tr>
<td>Financial constraints</td>
<td>Limited funding due to war-related economic pressures.</td>
<td>Seek international grants and partnerships, prioritize critical projects, and implement cost-effective solutions.</td>
</tr>
<tr>
<td>Displacement of personnel</td>
<td>Displacement of skilled personnel due to conflict zones.</td>
<td>Develop remote work capabilities, provide support for displaced staff, and invest in local talent development.</td>
</tr>
<tr>
<td>Communication disruptions</td>
<td>Disruptions in communication channels affecting coordination and operations.</td>
<td>Establish multiple communication channels, use satellite communication where necessary, and create contingency plans.</td>
</tr>
<tr>
<td>Data security risks</td>
<td>Increased vulnerability of sensitive data due to instability.</td>
<td>Enhance data encryption, implement strict access controls, and use secure data storage solutions.</td>
</tr>
<tr>
<td>Supply chain issues</td>
<td>Disruptions in the supply chain affecting the availability of necessary equipment.</td>
<td>Establish alternative supply chains, maintain inventory of critical equipment, and collaborate with local suppliers.</td>
</tr>
<tr>
<td>Psychological impact</td>
<td>Stress and trauma affecting the mental health of staff and students.</td>
<td>Provide mental health support services, establish counseling programs, and promote a supportive community environment.</td>
</tr>
<tr>
<td>Political instability</td>
<td>Uncertainty and changes in government policies impacting projects.</td>
<td>Maintain flexibility in project planning, engage with government stakeholders, and stay informed about policy changes.</td>
</tr>
<tr>
<td>Resource Allocation</td>
<td>Diverted resources to immediate war needs, affecting long-term projects.</td>
<td>Advocate for balanced resource allocation, demonstrate the long-term benefits of AI projects, and seek external funding.</td>
</tr>
</tbody>
</table>

*Source: compiled by the authors*

The ongoing war, particularly the Russian aggression against Ukraine, poses a significant threat to the physical infrastructure of educational institutions.
University buildings, data centers, and IT infrastructure are vulnerable to damage from shelling, bombings, and other forms of attack. The essence of this threat lies in the disruption of essential services and the potential loss of critical data and equipment. To mitigate this threat, it is crucial to develop and implement robust disaster recovery plans. These plans should include strategies for quickly restoring services and minimizing downtime in the event of infrastructure damage. Establishing off-site backups of critical data is also essential to ensure data recovery in case of local data center damage. Utilizing cloud services can provide additional resilience, as cloud providers often have geographically distributed data centers that are less vulnerable to localized physical damage.

During times of conflict, the risk of cyber-attacks on educational institutions increases significantly. Adversaries may target universities to disrupt operations, steal sensitive data, or sabotage critical infrastructure. The essence of this threat is the potential for significant operational disruptions and data breaches, which can have long-term consequences for the institution. To mitigate the risk of cyber-attacks, universities must implement advanced cybersecurity measures. This includes using firewalls, intrusion detection systems, and anti-malware solutions to protect against various cyber threats. Regular security audits are necessary to identify and address vulnerabilities in the system. Additionally, providing cybersecurity training to staff and students can help create a culture of security awareness and reduce the risk of human error contributing to security breaches.

The war imposes severe economic pressures, leading to limited funding availability for educational projects. The essence of this threat is the difficulty in securing the necessary financial resources to establish and maintain AI-powered intelligent centers, which require significant investment. To address financial constraints, universities can seek international grants and partnerships. Collaborating with global institutions and organizations can provide access to additional funding and resources. Prioritizing critical projects and implementing cost-effective solutions can also help make the most of limited financial resources. Efficient budgeting and financial planning are essential to ensure that funds are allocated effectively to support key initiatives.

The conflict zones in Ukraine have led to the displacement of skilled personnel, including faculty, researchers, and IT professionals. The essence of this threat is the loss of critical human resources needed to implement and manage AI-powered intelligent centers. To mitigate the impact of personnel displacement, universities should develop remote work capabilities. This includes providing the necessary technology and support for staff to work from safe locations. Offering support for displaced staff, such as housing assistance and relocation services, can help retain valuable personnel. Investing in local talent development is also crucial to build a resilient workforce that can adapt to changing circumstances.
War can lead to disruptions in communication channels, affecting coordination and operational efficiency. The essence of this threat is the potential breakdown in communication, which can hinder project progress and day-to-day operations. To address communication disruptions, universities should establish multiple communication channels to ensure redundancy. This can include using email, instant messaging, and video conferencing platforms. In areas with severe disruptions, satellite communication can provide a reliable alternative. Creating contingency plans for communication breakdowns is also essential to ensure that critical information can still be disseminated effectively.

The instability caused by the war increases the vulnerability of sensitive data. Data breaches and unauthorized access to critical information can have severe consequences for the university and its stakeholders. The essence of this threat is the heightened risk of data loss or theft. Enhancing data encryption is a key measure to protect sensitive information. Implementing strict access controls ensures that only authorized personnel can access critical data. Using secure data storage solutions, such as encrypted cloud storage, can further reduce the risk of data breaches. Regularly updating security protocols and conducting vulnerability assessments are essential to maintaining a secure data environment.

The war can disrupt supply chains, affecting the availability of necessary equipment and materials for establishing AI-powered intelligent centers. The essence of this threat is the potential delays and shortages that can impede project progress. To mitigate supply chain issues, universities should establish alternative supply chains to ensure a steady flow of necessary equipment. Maintaining an inventory of critical equipment can help cushion against temporary disruptions. Collaborating with local suppliers can also provide more reliable access to resources and reduce dependency on international supply chains that may be affected by the conflict.

The stress and trauma associated with the war can significantly impact the mental health of staff and students. The essence of this threat is the potential decline in productivity and well-being, which can affect overall project success. Providing mental health support services is essential to address the psychological impact of the conflict. Establishing counseling programs and promoting a supportive community environment can help staff and students cope with stress and trauma. Encouraging open communication about mental health issues and providing resources for self-care can also contribute to a healthier and more resilient university community.

The uncertainty and changes in government policies during the war can impact the execution of projects. The essence of this threat is the potential for sudden regulatory changes that can disrupt project plans and funding. To navigate political instability, universities should maintain flexibility in project planning. This includes being prepared to adapt to changing regulations and requirements. Engaging with government stakeholders and building strong relationships can also help advocate for the continuity of critical projects. Staying informed about policy changes and anticipating potential impacts can aid in proactive planning and decision-making.
During the war, resources are often diverted to immediate needs, affecting long-term projects. The essence of this threat is the competition for limited resources, which can delay or halt the establishment of AI-powered intelligent centers. Advocating for balanced resource allocation is crucial to ensure that long-term projects receive the necessary support. Demonstrating the long-term benefits of AI projects, such as improved educational outcomes and operational efficiency, can help secure funding and resources. Seeking external funding from international organizations and private donors can also provide additional support for critical initiatives.

**Conclusions.** The integration of AI-powered intelligent centers into the information infrastructure of universities amidst war presents a profound opportunity to revolutionize educational experiences and operational efficiency. Key findings from the study highlight the transformative potential of features such as data integration, predictive analytics, virtual assistants, adaptive learning, administrative automation, AI-driven cybersecurity, intelligent tutoring systems, research support, resource management, and personalized communication. These technologies collectively address critical needs within university ecosystems, enhancing decision-making, resource optimization, and personalized education.

For policymakers, the practical implications are significant. Investment in high-performance servers, machine learning models, AI chatbot software, adaptive learning platforms, RPA tools, AI-driven cybersecurity solutions, intelligent tutoring software, data analysis tools, resource management software, and CRM systems integrated with AI algorithms is essential. Policymakers must also focus on developing robust disaster recovery plans, enhancing cybersecurity measures, securing international grants and partnerships, and providing mental health support services to navigate the challenges posed by war.

Further research should explore the long-term impact of AI integration on educational outcomes and institutional resilience during conflict. Studies should investigate the effectiveness of AI-driven interventions in diverse university settings, the scalability of these solutions, and the potential for cross-border collaboration in AI development. Additionally, research on the ethical implications of AI in education, the role of AI in promoting equitable access to learning resources, and the development of adaptive policies to support AI integration in volatile environments is crucial. The ongoing relevance of these findings underscores the need for continued innovation and strategic investment in AI technologies to future-proof educational institutions against emerging challenges.

**References:**


Література:


