МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

МІНІСТЕРСТВО ОСВІТИ ІРАКУ
АЛЬ НУР УНІВЕРСИТЕТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ ПОЛЬЩІ
УНІВЕРСИТЕТ КОМІСІЇ НАРОДНОЇ ОСВІТИ В КРАКОВІ

III Міжнародна науково-практична конференція “Освіта, Право та Публічне управління – новітні тенденції розвитку”

«ELPA–NDT»

27-28 червня 2024 р.
Україна-Ірак-Польща

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
KYIV NATIONAL UNIVERSITY OF CONSTRUCTION AND ARCHITECTURE

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH, IRAQ
ALNOOR UNIVERSITY

MINISTRY OF EDUCATION AND SCIENCE OF POLAND
UNIVERSITY OF THE NATIONAL EDUCATION COMMISSION OF KRAKOW

The III International Scientific and Practical Conference «Education, Law and Public Administration – New Development Trends» (ELPA–NDT)

«ELPA–NDT »

June 27th-28th 2024
Ukraine-Iraq-Poland

РЕДАКЦІЙНА КОЛЕГІЯ:
Хлапонін Д.Ю. – кандидат наук з державного управління
Ворона П.В. – доктор наук з державного управління, професор
Касім Н. Х. – доктор технічних наук, доцент

Конференція проведена за організаційної, інформаційної та технічної підтримки кафедри кібербезпеки та комп'ютерної інженерії КНУБА (завідувач кафедри д.т.н., проф. Хлапонін Ю.І.)

Рекомендовано до видання вченою радою Київського національного університету будівництва і архітектури. Протокол № 22 від 31.05.24 р

Відібрані оргкомітетом доповіді після допрацювання опубліковані в виданні, яке індексується в наукометричній базі Scopus

Зміст

ВСТУПНЕ СЛОВО. INTRODUCTORY WORD 7

Dariia BRUKHAL, Yevheniia SHABALA
CYBER PROPAGANDA AND COUNTERING DISINFORMATION..... 8

Mykola MALENKO, Mykola RUDENKO, Yevheniia SHABALA
BLOCKCHAIN TOKENIZATION FOR MOTIVATION AND REWARD IN EDUCATIONAL PROCESSES, PROSPECTS AND CHALLENGES 12

Юрій ГАРУСТ
ОСОБЛИВОСТІ НОРМАТИВНОЇ РЕГЛАМЕНТАЦІЇ ЗДІЙСНЕННЯ ОБОРОННИХ ЗАКУПІВЕЛЬ ПІД ЧАС ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ В УКРАЇНІ 16

Liza TSYKALO, Yevheniia SHABALA
АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СИСТЕМАХ ДЕРЖАВНОГО УПРАВЛІННЯ ТА ЇХ ВІДПОВІДНОСТІ ЗАКОНОДАВСТВУ ПРО КОНФІДЕНЦІЙНІСТЬ ДАНИХ 19

Анастасія КРАВЧЕНКО
ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОГО ОСВІТНЬОГО СЕРЕДОВИЩА У КОНТЕКСТІ БЕЗПЕРЕРВНОЇ ОСВІТИ..... 24

Вадим САРАПИН, Дмитро ХЛАПОНІН
ПРОБЛЕМНІ ПИТАННЯ ПІДГОТОВКИ ДО ЄДКІ ЗІ СПЕЦІАЛЬНОСТІ 125 «КІБЕРБЕЗПЕКА» У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ..... 28

Олексій ЛУК'ЯНОВ
ІСТОРИЧНІ ДИСЦИПЛІНИ У ПІДГОТОВЦІ БАКАЛАВРІВ ЗІ СПЕЦІАЛЬНОСТІ 281 «ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ 31

Олена БАЛІНА, Ірина БЕЗКЛУБЕНКО, Юрій БУЦЕНКО
МОДЕЛЬ КОНТРОЛЮ НАКОПИЧЕННЯ РЕЙТИНГОВИХ БАЛІВ СТУДЕНТІВ ПРИ ВИВЧЕННІ КУРСУ ВИЩОЇ МАТЕМАТИКИ В ТЕХНІЧНОМУ УНІВЕРСИТЕТІ..... 36

Петро ВОРОНА
РОЛЬ ТА МІСЦЕ ДЕРЖАВНИХ І НЕДЕРЖАВНИХ ОРГАНІВ ТА ОРГАНІЗАЦІЙ ПІД ЧАС ВЕДЕННЯ БОЙОВИХ ДІЙ, ПРОВЕДЕННЯ ОПЕРАЦІЇ 40

Yevhenii STEPANCHENKO, Vadym POLISHCHUK
CYBERSECURITY IN THE CONTEXT OF EDUCATION DIGITALIZATION .. 48

Ростислав ПИСАНИЙ
ІНОВАЦІЙНІ ПІДХОДИ В ЦИФРОВІЙ ОСВІТІ: АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ ТА ПЕРСПЕКТИВИ РОЗВИТКУ 52

Денис ТОКАР, Анастасія ХЛАПОНІНА
ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА 55

Нікіта ДЕМ'ЯНОВ, Олександр ШИМЧУК
ЦИФРОВА ТРАНСФОРМАЦІЯ ТА КІБЕРБЕЗПЕКА В ДЕРЖАВНОМУ УПРАВЛІННІ 58

Лариса ВОРОНА
ОРГАНІЗАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ В ЗАКЛАДАХ ПОЗАШКІЛЬНОЇ ОСВІТИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ 61

Наталія СЕРДЮК
РЕАЛІЗАЦІЯ ПРАВА НА ОСВІТУ В УМОВАХ ВОЄННОГО СТАНУ 63

ВСТУПНЕ СЛОВО. INTRODUCTORY WORD

Петро Ворона
доктор наук з державного управління,
професор, начальник відділення організації
дистанційного навчання навчального
центру Сил ТрО ЗСУ, Україна.

Шановні учасники конференції!

Прийміть найщіріші вітання !

Зичу всім плідної роботи та очікуваних результатів від обміну думками, що мають відбутися на конференції. Ця конференція проходить в умовах російської агресії, тому неможливо обійти її вплив на суспільство і її актуальність.

Ми вже повинні відслідковувати і закарбувати уроки, які отримує Україна у цей час боротьби за збереження держави. Війна виокремила ще більше ті негативи, які мало публічне управління, законодавство та освіта, а також здійснила колосальний вплив на формування української нації та ще більш згуртувала проукраїнські сили. Це змінило українське суспільство, яке є одним з основних підвалин демократичного устрою держави.

Інформаційна війна, як елемент гібридної війни нами не програна. Єдина інформаційна політика сприяє гуртуванню нації. Вказані виклики якраз відповідають напрямкам конференції. Переконаний, що вони будуть обговорюватись на цьому поважному науковому заході.

Щиро переконаний, що Україна переможе, а значить переможе справедливість та демократія у Європі і світі.

The III International Scientific and Practical Conference «Education, Law and PublicAdministration – New Development Trends» (ELPA–NDT)

CYBER PROPAGANDA AND COUNTERING DISINFORMATION

Dariia BRUKHAL (bachelor)[1]
Yevheniia SHABALA (PhD, associate professor)[2]

[1]*Kyiv National University of Contracture and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering, Cyber Security Specialty*
[1]*brukhal_da@knuba.edu.ua*
[2]*Kyiv National University of Contracture and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering*
[2]*shabala.ieie@knuba.edu.ua*

Abstract

У цій статті розглядаються сучасні виклики та стратегії протидії кібер пропаганді. Проводиться аналіз особливостей та структури кіберпропаганди, висвітлює технологічні аспекти та роль освіти у боротьбі з дезінформацією. Визначено правові та політичні підходи до протидії дезінформації, а також наголошено на необхідності комплексного підходу до забезпечення інформаційної безпеки та захисту громадської думки.

Introduction

Digitalization becomes a necessity for governance and ensuring democratic principles over time and in the course of events. First, the COVID-19 pandemic and then the war revealed a problem in digital governance, such as cyber propaganda. Cyber propaganda is the systematic dissemination of false, manipulated or distorted information to influence the opinion or behaviour of a group of people through the Internet and other digital channels [1]. And people who need to force society to change or establish an opinion, using mass digitalization, spread propaganda and disinformation that influences people's minds and makes them easy to control. A vivid example of the harmful effects of cyber propaganda and disinformation is our murderous neighbour, who, by means of influencing the minds of its citizens, created a picture of the noble liberation of brothers from captivity, although he himself is an occupier. Therefore, there is a great need to analyze and research this problem in order to be able to fight and counteract it effectively.

Analysis of cyber propaganda technology

The main purpose of cyber propaganda is to manipulate public opinion and create a favorable environment for achieving specific political, social or other goals. Depending on the specific goal of the propaganda campaign, cyber propaganda methods can be divided into the following.

Manipulation of public opinion, which is carried out by means of the dissemination of fake news, emotional influence, mass retransmission of messages, manipulation of data and statistics, use of psychological techniques, and creation of artificial contexts.

For such an impact, we can highlight some tools: social networks, blogs and websites, forums and comments, video and multimedia content, bots and automated systems. One example of such platforms is the Russian internet agency known as the "Troll Factory" or the "Internet Research Agency" (IRA) [2]. It is notorious for spreading disinformation and propaganda across various social media platforms, including Facebook, Twitter, and Instagram. The IRA employs individuals who create fake accounts and groups to disseminate misleading information, sow discord, and influence public opinion. Similarly, the Chinese government has been accused of deploying the "50 Cent Army," a group of internet users paid to post pro-gover [3].

Undermining trust in institutions often involves such methods of implementation as disinformation campaigns, creation of conspiracy theories, selective leaking of information, exploitation of social media, targeted messaging, propaganda films and documentaries, selective reporting by media outlets. During the 2016 U.S. presidential election, there was a case of Internet trolls working on behalf of a foreign state using Twitter to spread disinformation and undermine trust in the electoral system. They created fake accounts supporting various candidates and spread false news, conspiracy theories and other disinformation that undermined public confidence in the electoral process. This helped to create an atmosphere of distrust among voters and influence their voting preferences.

The polarization of society also occurs through social media, social media algorithms, viral content, mass messaging, and the creation of fake news. One interesting example of social media polarization is the campaign that took place in India during the 2019 presidential election. During this election, various political groups and activists used networks such as Twitter and Facebook to distribute rebuttal content that included memes, videos, and animations with negative images of opponents. These memes were intended to generate laughter and irony, but also sparked political debate and tension between supporters of different candidates.

Other forms of propaganda, such as mobilizing support or opposition and creating psychological pressure, have similar methods of implementation to the above, but the most popular at present is disinformation.

Combating disinformation

Countering disinformation is an extremely important task in today's information environment. In order to effectively combat disinformation, it is necessary to develop comprehensive strategies that cover both technological and human aspects.

1. Analysis of strategies to counter disinformation

The analysis of disinformation counteraction strategies includes research and evaluation of various methods and approaches used to prevent the spread of disinformation and combat it.

The introduction of artificial intelligence algorithms and technologies in the fight against disinformation can have a significant impact on the ability to detect and reduce

the spread of harmful information. Artificial intelligence algorithms can efficiently identify and analyze large amounts of data, which allows for timely detection and response to disinformation. Machine learning can also be used to create models to predict potentially harmful information and respond quickly to its spread. One potential downside could be the possible emergence of algorithms that misclassify information or the introduction of algorithms that could be used to censor or restrict freedom of speech. In addition, algorithms could be subject to manipulation or abuse, which could lead to new forms of disinformation [4]. To improve the effectiveness of AI algorithms and technologies in the fight against disinformation, it is necessary to actively develop algorithms to identify new forms of disinformation and adapt them to the rapidly changing social media and media environment. It is also important to develop ethical standards and control over the use of artificial intelligence to prevent possible negative consequences.

Also, the development of media literacy and critical thinking is a qualitative counteraction to disinformation. Increasing media literacy and critical thinking contributes to the formation of a responsible attitude to information, raising the level of citizens' education and reducing the impact of disinformation. People are able to better recognize manipulations in the media and analyze information with greater caution. To improve the development of media literacy and critical thinking, it is necessary to conduct information campaigns among the population on the importance of a critical attitude to information. It is also important to stimulate the development of critical thinking through engaging in discussions and analyzing real-life situations using scientific and factual sources.

Cooperation with social networks and online platforms involves entering into partnership agreements and developing joint strategies to effectively identify and remove disinformation content and allows for the efficient dissemination of useful information and audience engagement. However, such cooperation can lead to dependence on platform algorithms that can suppress diversity of opinion and information pluralism. To improve this situation, transparent and objective algorithms can be developed and applied, and critical thinking among users can be promoted.

Legislative measures to combat disinformation may include the adoption of special laws and regulations aimed at controlling the information space and preventing the spread of harmful information. Such measures have the advantage of ensuring the safety of citizens, protecting democratic values, and preserving information trust. However, an insufficiently flexible legislative approach can restrict freedom of speech and expression, as well as lead to censorship and human rights violations. Suggestions include improving laws and regulations to take into account the principles of freedom of speech and ensure effective protection against harmful information.

2. The role of education in countering disinformation

The role of education in the fight against disinformation is to provide citizens with the necessary knowledge and skills to analyze and critically evaluate information. Information literacy encompasses the ability to effectively search for, evaluate and use

information from various sources, ensuring an understanding of its sources and reliability. Digital literacy, in turn, implies the ability to use digital technologies and resources, understanding their impact on society and the ability to interact with them effectively. Critical thinking is a key component of education, as it allows you to analyze, evaluate and critically approach information from various sources and recognize possible manipulations and distortions of facts. Emotional and social competence includes understanding and managing one's own emotions, the ability to communicate and cooperate with others, and to adapt to different social situations.

One of the new approaches is media literacy through interactive platforms, which involves teaching citizens the skills of analyzing and critically evaluating information through interactive online courses, webinars, and specialized learning resources. For example, the MediaWise project uses a game-based approach to teach young people critical thinking and understanding of the media landscape [5].

Suggestions for improvement include integration into educational programs, which involves introducing media literacy and critical thinking courses into school and university curricula to comprehensively develop these skills among students and students. Further, supporting teachers and parents in providing media literacy skills can include special trainings, developing educational materials, and creating pedagogical resources for effective work with students and children. Finally, the creation of joint initiatives between government, non-profit organizations and the private sector will facilitate the development and implementation of comprehensive media literacy programs, as well as provide support and funding for projects aimed at improving education and combating disinformation in society.

Conclusion

This paper examines the current problem of cyber propaganda and disinformation in the modern information environment. A thorough analysis of the characteristics of cyber propaganda and its various methods has revealed a wide range of tools and technologies used to manipulate public opinion and spread disinformation. Particular attention was paid to the analysis of strategies to counter disinformation, including the role of education, legislative approaches and international cooperation. However, it should be recognized that this problem requires further study and development of comprehensive approaches to effectively ensure information security and protect public opinion. Only through the joint efforts of governments, civil society organizations, the private sector and citizens can significant progress be made in this direction.

References

[1] Mull C., and Wallin M.. “Propaganda: A Tool of Strategic Influence.” American Security Project, 2013.
[2] Wired, https://www.wired.com/story/russia-internet-research-agency-disbands/ , (13.03.2024).
[3] VOA, https://www.voanews.com/a/who-is-that-chinese-troll/3540663.html, (13.03.2024).
[4] Detector Media, https://ms.detector.media/kiberbezpeka/post/33149/2023-10-07-shtuchnyy-intelekt-na-sluzhbi-propagandy/, (13.03.2024)

[5] Poynter., https://www.poynter.org/mediawise/, (13.03.2024).

BLOCKCHAIN TOKENIZATION FOR MOTIVATION AND REWARD IN EDUCATIONAL PROCESSES, PROSPECTS AND CHALLENGES

Mykola MALENKO (postgraduate)[1]
Mykola RUDENKO (PhD, associate professor)[2]
Yevheniia SHABALA (PhD, associate professor)[3]

[1]Kyiv National University of Construction and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering
[1]malenko.mv@knuba.edu.ua
[2]Kyiv National University of Construction and Architecture, Faculty Of Automation And Information Technologies, Department Of Professional Education
[2]rudenko.mv@knuba.edu.ua
[3]Kyiv National University of Construction and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering
[3]shabala.ieie@knuba.edu.ua

Abstract

This work aims to investigate the impact of tokenization on the field of education, analyzing its potential to motivate students and reward educational achievements. Given the rapid development of technologies and their integration into various aspects of social life, education is faced with the need to use innovative approaches to improve learning efficiency and student engagement. Tokenization based on blockchain technologies offers unique opportunities to create transparent, secure and motivating educational ecosystems. This paper examines both the prospects and challenges associated with implementing tokenization in education.

Keywords

Tokenized reward, micro-reward, blockchain, education, tokenization

Introduction

At the edge of a new era that requires us not only to observe change, but also to actively intervene and adapt, innovation in education is becoming a key element of progress. This transition requires understanding the deep needs of a changing society, adapting to the rapid development of technology and responding to the challenges of globalization.

In the history of mankind, innovations have always served as the driving force of development, opening new horizons of possibilities. This is especially true in the education sector, as innovation not only opens up access to knowledge, but also stimulates critical thinking, creativity and interaction. They allow education to go beyond traditional teaching methods, offering individualized and flexible approaches

that meet the different needs and abilities of students.

The focus today is on tokenization [1], an innovative technology that is already changing many areas of our lives, from finance to art, and is now finding its place in education. This technology not only opens up new ways of motivating and rewarding educational achievements, but also offers prospects for the development of educational platforms, ensuring transparency, security and availability of educational resources.

Analysis of potential prospects and challenges of tokenization [1] integration in the educational space will allow us to understand how this technology can transform traditional approaches to learning, motivation, and rewards. This will allow us to assess how tokenization can contribute to the development of education in the future, as well as what opportunities and risks accompany the introduction of this technology.

Tokenization of rewards in educational processes

Tokenization [1] is the process of converting rights to assets or access to services into unique tokens on the blockchain network. These tokens can represent real assets, such as real estate, artwork, securities, or intellectual property, as well as digital assets, including virtual currency, access to software, or other digital resources. The main goal of tokenization is to create a safe, transparent and efficient way to exchange rights to assets using digital technologies.

Since the individualization of the educational process is one of the key elements in increasing the effectiveness of education and the involvement of students. The use of tokenized rewards can be an innovative method that helps personalize learning and motivate students. This approach allows not only to record students' academic achievements, but also to adapt the learning process to their individual needs and interests.

Tokens can be customized to reflect each student's specific achievements and interests. This may include skills, knowledge, involvement in projects, initiative or creative input. Using the blockchain to record achievements ensures their irrefutability and easily verifiable history, which adds weight and significance to rewards.

Tokenized rewards, in turn, can be used in various forms:

- access to additional materials or courses
- access to participation in mentoring programs
- micro-rewards

The last point can serve as a powerful incentive for students, encouraging them to further achievements and self-improvement.

Micro-rewards [2] are a system of rewarding small achievements or completing short tasks that are part of a larger process or goal. In the context of education and training, this approach can serve as a powerful tool for ongoing motivation, helping to maintain a high level of engagement and interest among students. Micro-rewards help keep motivation at a consistently high level, as students regularly receive a sense of achievement and recognition.

A tokenized micro-reward is credited to the student's electronic wallet immediately after completing a task or achieving a goal, which helps to strengthen positive associations with the educational process. And regularly receiving small rewards helps to avoid losing interest in learning or a project, stimulating students to take further action.

This type of reward can be tailored to a student's specific tasks, goals or interests, providing a personalized approach to motivation. The use of blockchain technology makes it easy to verify and monitor the progress of a student's education or skill development. In the future, the student can exchange tokens for real rewards or privileges, which connects academic success with real advantages and opportunities.

Tokenized micro-rewards, combined with smart contract technology on blockchain platforms [3], open up new opportunities for automation, personalization and transparency of motivational systems in education. Smart contracts are programs that automatically execute the terms of a contract between two or more parties when certain conditions are met, without requiring intermediaries [3]. Smart contracts can automatically issue tokenized micro-rewards to students for completing certain learning tasks or achieving set goals [4]. This simplifies the reward process, ensuring fast and accurate compliance. This approach reduces the burden on teachers and other participants in the educational process, who are directly involved in evaluating students' activities.

The use of smart contracts to manage tokenized micro-rewards in education opens up vast possibilities for creating more motivating, fair and efficient learning systems that can adapt to individual needs and student progress.

Issues of tokenization of rewards in educational processes

The introduction of tokenized rewards [4] into educational processes opens up new opportunities for motivating students, personalizing learning, and creating more flexible and effective reward systems. However, this approach is also accompanied by a number of problems and shortcomings.

The first drawback is the high technical threshold, because tokenization requires the development and maintenance of complex technological infrastructure [5], including blockchain platforms and smart contracts. This raises the question of the need for highly qualified IT specialists and continuous technical support.

In addition to the technical aspect, there is a regulatory [6] aspect. The use of blockchain and cryptocurrency tokens may be subject to regulatory restrictions in various jurisdictions. The need to comply with legal requirements complicates the process of implementing tokenized reward systems. That is why it is very important to cooperate with regulators [6] to develop clear rules for the use of blockchain in education, which take into account the peculiarities of tokenized rewards.

Also, when tokenizing rewards in educational processes, an ethical aspect appears. After all, the question of fairness in the use of tokenized rewards may arise if the system favors certain groups of students or promotes inequality. In addition, there is a risk of dependence on the reward system [7], which can change the motivation of students from acquiring knowledge to receiving tokens. To ensure fairness and prevent such

negative social consequences, it is important to develop and establish ethical principles for the design and implementation of tokenized reward systems.

Conclusions

Tokenization of rewards in educational processes opens up new opportunities for personalizing learning, increasing student engagement, and ensuring transparency and verification of educational achievements. However, along with the prospects, the introduction of tokenization is accompanied by a number of challenges and requires a comprehensive approach to their solution.

Tokenization of rewards enables the creation of deeply personalized and motivating learning experiences for students, rewarding them for individual achievement and engagement. The use of blockchain technologies ensures immutability and easy verification of educational achievements, contributing to the growth of trust between educational institutions, students and employers.

Tokenization of rewards has certain disadvantages, these include a high technical threshold of entry [5], the need to adapt to the regulatory environment [6], and there is also a strong need to consider the ethical and social aspects of tokenization, ensuring fair access to rewards and avoiding the creation of unwanted dependencies or inequities [7].

The future of tokenization [1] in education promises to create more flexible, efficient and inclusive learning and reward systems. To realize this potential, it is necessary to overcome the existing challenges through innovative technical solutions, active cooperation between educational institutions, technology companies and regulators, as well as through the development of effective management and control mechanisms. The introduction of tokenization into educational processes can open new horizons for the development of education adapted to the needs of modern society and the economy.

References

[1] What Does Crypto Tokenization Look Like https://www.gemini.com/cryptopedia/what-is-tokenization-definition-crypto-token
[2] What is A Micro-incentive In Behavior Change, https://www.thebehavioralscientist.com/glossary/micro-incentive
[3] Introduction to smart contracts, https://ethereum.org/en/developers/docs/smart-contracts/
[4] Revolutionizing Education with Smart Contracts, https://medium.com/@solidity101/revolutionizing-education-with-smart-contracts-742e570a414f
[5] Blockchain Infrastructure Requirements (Software & Hardware), https://imiblockchain.com/blockchain-infrastructure-requirements/
[6] Cryptocurrency Regulations Around the World, https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122
[7] The Influence of School's Reward Systems on Students' Development, https://typeset.io/papers/the-influence-of-schools-reward-systems-on-students-1h7vgrn0

ОСОБЛИВОСТІ НОРМАТИВНОЇ РЕГЛАМЕНТАЦІЇ ЗДІЙСНЕННЯ ОБОРОННИХ ЗАКУПІВЕЛЬ ПІД ЧАС ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ В УКРАЇНІ

Юрій ГАРУСТ (доктор юридичних наук, професор, полковник юстиції, доцент кафедри військового права та правоохоронної діяльності Національного університету оборони України)[1]

[1]*Національний університет оборони України, кафедра військового права та правоохоронної діяльності, спеціалізація: «Адміністративне право. Інформаційне право»*
[1]*yurii.harust.1972@ukr.net*

Summary:
the importance of further search for ways to reform the specified direction of state regulation is emphasized and argued.
The key normative legal acts in this area are highlighted. It has been clarified and proven that there are certain differences in some issues of defense procurement during the operation of the special legal regime.
The key innovations in the defined area have been worked out. The author's vision of priority landmarks for priority changes in the foreseeable future is offered.

Третій рік повномасштабного вторгнення, істотні економічні ризики та складнощі з отриманням деякої міжнародної допомоги від іноземних партнерів зумовлюють необхідність перегляду принципів роботи національних механізмів регулювання різних сфер відносин. Політика всебічного посилення військового потенціалу агресора та розробка й ухвалення відповідних стратегій, націлених на середньо- і довгострокову перспективи не залишають вибору вітчизняним суб'єктам правотворчої діяльності.

Одним із перспективних векторів слушно можна вважати питання нормативної регламентації здійснення оборонних закупівель за для оптимізації відповідних процедур. До того ж, вказаний напрям має пріоритетне значення, із огляду на поточну обстановку і виходячи з об'єктивного розуміння характеру й темпів перебігу низки процесів і тенденцій на фронті та за його межами. Виходячи з цього, особливої уваги вимагає проблематика нормативної регламентації здійснення оборонних закупівель в Україні у сучасних умовах.

Різні грані цього складного питання неодноразово перебували у полі зору багатьох провідних дослідників. Серед яких слід виокремити доробки таких вчених, як О. П. Голота, Є. В. Грибачьов, М. Г. Іваницький, О. В. Левчук, В. Д. Левчук, Н. С. Хатнюк, В. В. Ярема і багатьох інших. У той же час, зазначений аспект на сучасному етапі потребує подальшого вивчення й змістовного дослідження, ураховуючи дію спеціального правового режиму та динамічні трансформації профільного законодавства.

Необхідно зауважити, що базові основи регулювання відносин у цій сфері

закладені в ЗУ «Про оборонні закупівлі» від 17.07.2020 р. № 808-IX. Відповідно цим актом визначені засади планування, порядок формування обсягів та особливостей здійснення закупівель товарів, робіт і послуг оборонного призначення для забезпечення відповідних потреб. Також увага приділена механізмам організації й здійснення державного і демократичного цивільного контролю у сфері оборонних закупівель [1]. Керуючись саме нормами цього законодавчого документа розбудовується й похідне юридичне підґрунтя в аналізованій сфері суспільних відносин.

До того ж, його умови й порядки їх реалізації не суперечать Директиві 2009/81/ЄС Європейського Парламенту та Ради «Про координацію процедур укладання певних контрактів на виконання робіт, контрактів на постачання та контрактів на надання послуг замовниками або організаціями у сферах оборони та безпеки, а також внесення змін до Директив 2004/17/ЄС та 2004/18/ЄС» від 13.07.2009 р. [2], котрою визначено низку міжнародних стандартів для всіх її учасників у предметній сфері.

В контексті реалій сьогодення виняткове процедурне значення має Постанова КМУ «Деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану» від 11.11.2022 р. № 1275. Зазначеним актом визначено особливості здійснення оборонних закупівель на період дії правового режиму воєнного стану, а також передбачено порядок визначення предмета закупівлі під час здійснення закупівель продуктів харчування, послуг із забезпечення комплектами продуктів харчування, послуг щодо забезпечення харчуванням та послуг з організації харчування для особового складу Збройних Сил [3]. Тобто, увага приділена деяким аспектам однойменних процедур саме під час дії вищезгаданого правового режиму і, відповідно, поширюється лише на цей період.

У загальному вигляді, ключові особливості таких закупівель полягали в спрощенні і пришвидшенні деяких процедур, із огляду на усвідомлення потреб сил безпеки й оборони. На думку Д. Котової й Я. Свідерської, доцільно виділити наступні знакові новації: 1) існування виключно прямих контрактів (станом на сьогодення скасовані); 2) двоетапні рамкові угоди для речового забезпечення (станом на сьогодення скасовані); 3) наявність механізмів «відкритих торгів», з урахуванням загальних особливостей на період дії правового режиму воєнного стану; 4) спрощення закупівель у порядку ЗУ «Про публічні закупівлі» від 25.12.2015 р. № 922-VIII [4], а не вищезгаданого базового документа; 5) запит цінових пропозицій; 6) закритість процедур закупівель (прямі договори) для окремих категорій товарів [5]. Отже, знаходить підтвердження авторська теза про оптимізацію окремих процедур на користь спрощення (прямі контракти, «відкриті торги», закупівлі відповідно до іншого нормативно-правового акту тощо). Більше того, 1 лютого 2024 р. Кабінетом Міністрів України у межах своїх повноважень і згідно п. 5 ч. 1 ст. 121 ЗУ «Про правовий режим воєнного стану» від 12.05.2015 р. № 389-VIII [6], [7] прийнято рішення про запровадження у системі «Prozorro» нового інструменту – «рамкової угоди» [8]. Тобто, компетентними органами виконавчої влади провадиться подальша діяльність,

спрямована на підвищення рівня ефективності функціонування сфери оборонних закупівель. Відповідно, напрацьовуються нові методи, способи і засоби щодо удосконалення тих чи інших механізмів за вказаним напрямом.

Не виникає сумніву, що поточна безпрецедентно складна обстановка вимагає подальших активних пошуків шляхів удосконалення законодавства в цій сфері. З огляду на обмеженість у технічних вимогах, вбачається за доцільне й виправдане окреслити лише базові орієнтири для першочергових змін. Серед таких авторських новацій перспективним убачається наступний діапазон позицій: 1) подальше активне і поглиблене вивчення відповідного досвіду міжнародних партнерів й інших іноземних держав, насамперед країн-членів НАТО; 2) оптимізація механізмів державного регулювання оборонних закупівель із орієнтиром на потреби й запити воєнного часу; 3) посилення стратегічного планування державної політики оборонних закупівель із обов'язковим урахуванням умов воєнного часу; 4) цифровізація більшості технологічних процесів з питань оборонних закупівель, задля зменшення обсягів бюрократизації та мінімізації корупціогенних ризиків; 5) пошук і реалізація інших заходів, спрямованих на посилення прозорості під час здійснення оборонних закупівель; 6) державне стимулювання виконавців державних контрактів (договорів) з оборонних закупівель; 7) поглиблення різних форм взаємодії між учасниками відносин у сфері планування, формування обсягів та здійснення закупівель товарів, робіт і послуг оборонного призначення для забезпечення потреб сектору безпеки й оборони; 8) посилення інструментів демократичного цивільного контролю у сфері оборонних закупівель.

Узагальнюючи викладене, слід зауважити, що чинне нормативне забезпечення здійснення оборонних закупівель суттєво орієнтовне на задоволення потреб і запитів сектору безпеки й оборони. На користь цього судження виступає й те, що передбачені ряд особливостей для реалізації деяких однойменних процедур під час дії правового режиму воєнного стану.

Доцільно відмітити, у період повномасштабного вторгнення суб'єкти правотворчості вжили низку заходів, спрямованих на адаптацію такого забезпечення до нових складних реалій. У цей же час, із огляду на багатогранність аналізованого напряму, вказане питання вимагає подальшого комплексного опрацювання всіма компетентними інституціями й зацікавленими особами.

Література

[1] Про оборонні закупівлі: Закон України від 17 липня 2020 р. № 808-IX // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/808-20#Text (дата звернення: 04.03.2024).

[2] Директива 2009/81/ЄС Європейського Парламенту та Ради «Про координацію процедур укладання певних контрактів на виконання робіт, контрактів на постачання та контрактів на надання послуг замовниками або організаціями у сферах оборони та безпеки, а також внесення змін до Директив 2004/17/ЄС та 2004/18/ЄС»: Директива Європейського Парламенту та Ради від 13 липня 2009 р. № 2009/81/ЄС. Веб-портал: «EUR-Lex». 2009

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0081 (дата звернення: 04.03.2024).

[3] Деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану: постанова Кабінету Міністрів України від 11 листопада 2022 р. № 1275 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/1275-2022-п#Text (дата звернення: 04.03.2024).

[4] Про публічні закупівлі: Закон України від 25 грудня 2015 р. № 922-VIII // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/922-19#Text (дата звернення: 05.03.2024).

[5] Котова Д., Свідерська Я. Оборонні закупівлі. Погляд збоку. Веб-портал: «ЕКОНОМІЧНА ПРАВДА». 2024. URL: https://www.epravda.com.ua/publications/2024/02/12/709678/ (дата звернення: 05.03.2024).

[6] Про Кабінет Міністрів України: Закон України від 27 лютого 2014 р. № 794-VII // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/794-18#Text (дата звернення: 05.03.2024).

[7] Про правовий режим воєнного стану: Закон України від 12 травня 2015 р. № 389-VIII // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 05.03.2024).

[8] Прозоро, конкурентно та з урахуванням вимог безпеки: Уряд удосконалює процеси оборонних закупівель. Веб-портал: Кабінет Міністрів України. 2024. URL: https://www.kmu.gov.ua/news/prozoro-konkurentno-ta-z-urakhuvanniam-vymoh-bezpeky-uriad-udoskonaliuie-protsesy-oboronnykh-zakupivel (дата звернення: 05.03.2024).

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СИСТЕМАХ ДЕРЖАВНОГО УПРАВЛІННЯ ТА ЇХ ВІДПОВІДНОСТІ ЗАКОНОДАВСТВУ ПРО КОНФІДЕНЦІЙНІСТЬ ДАНИХ

Liza TSYKALO (student)[1]
Yevheniia SHABALA (PhD, associate professor)[2]

[1]*Kyiv National University of Contracture and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering*
[1]*tsykalo_yd@knuba.edu.ua*
[2]*Kyiv National University of Contracture and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering*
[2]*shabala.ieie@knuba.edu.ua*

Abstract

This work is devoted to the analysis of personal data protection measures in various areas, such as public administration systems and entrepreneurship. The work considers specific aspects of personal data protection, such as the definition of personal data, the subjects' consent to data processing, as well as requirements for ensuring the security of this data. In addition, the risk of unauthorized access to personal information and ways to prevent such situations are analyzed. The work also provides practical advice on protecting personal data, which can be useful for different categories of users and digital security professionals.

Вступ

У сучасному цифровому світі захист персональних даних стає все більш актуальним і важливим завданням для різних сфер діяльності. У цьому контексті, дві ключові теми, які розглядаються в даній роботі, відображають значущі аспекти цього завдання.

Перша тема розглядає методи захисту персональних даних у системах державного управління. Вона вивчає визначення персональних даних та їхніх суб'єктів, а також роль згоди у процесі обробки цих даних. Крім того, досліджуються вимоги до захисту персональних даних у різних сферах, включаючи електронну комерцію та роботу органів влади.

Друга тема стосується ризиків небезпеки оволодіння персональними даними та шляхів запобігання таким діям. Вона розглядає умовні рівні загроз персональним даним та визначає конкретні заходи безпеки для кожного з них. Крім того, вона надає поради щодо захисту персональних даних, зокрема, перегляд політики конфіденційності та уважність до обробки особистих даних. Обидві теми допомагають розуміти важливість захисту персональних даних і надають практичні рекомендації для їх забезпечення.

Методи захисту персональних даних у системах державного управління

Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована; суб'єкт персональних даних - фізична особа, персональні дані якої обробляються. Під згодою суб'єкта персональних даних слід розуміти добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки.

Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних.

Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

Володільці, розпорядники персональних даних і треті особи зобов'язані забезпечити захист цих даних від випадкових втрат або знищення, від незаконної

обробки, у тому числі незаконного знищення чи доступу до персональних даних. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці. [1]

Щодо можливого характеру загрози для збереження цілісності та конфіденційності персональних даних, що зберігаються у відповідних базах даних та відповідних заходів безпеки, то їх можна умовно поділити на наступні види:

– неавторизований доступ до персональних даних (усувається шляхом встановлення режимів управління доступом та заборони гостьового (неавторизованого) входу до бази даних);

– незаконне ознайомлення з персональними даними (унеможливлюється шляхом запровадження належного режиму конфіденційності інформації, що міститься у базі даних);

– модифікація або знищення персональних даних (усувається шляхом організації обмежених прав доступу (перегляд/зміна/редагування/видалення) даних для різних категорій користувачів);

– відмова у послугах чи у використанні даних відповідно до визначених цілей (запобігається шляхом забезпечення належного рівня доступності для осіб, що мають на це право);

– доступ до даних від імені підставної персони/ відмова від авторства доступу до персональних даних (унеможливлюється шляхом усунення можливості спростування та перевірки авторства під час внесення даних до бази);

– неавторизоване управління базою персональних даних (усувається шляхом організації розподілу прав адміністрування базою персональних даних для відповідних категорій користувачів) [2].

Закони, що регулюють захист персональних даних користувачів

У цьому розділі наведені основні закони та пункти щодо захисту персональних даних.

Стаття 11 Закону України про Захист персональних даних. Підстави для обробки персональних даних

1. Підставами для обробки персональних даних є:

1) згода суб’єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

3) укладення та виконання правочину, стороною якого є суб’єкт персональних даних або який укладено на користь суб’єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб’єкта персональних даних;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом;

6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

Стаття 24 Закону України про Захист персональних даних. Забезпечення захисту персональних даних

1. Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

2. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

4. Фізичні особи - підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону [3].

Ризики небезпеки оволодіння персональними даними та шляхи запобігання таким діям.

Чотири умовні рівні загроз персональним даним:

Клас ризику 0: ризик відсутній. Персональні дані, що обробляються, вже знаходяться у вільному доступі, і вважається, що використання персональних даних з визначеними цілями не містить ризиків для суб'єктів персональних даних та не потрібні жодні спеціальні заходи безпеки;

Клас ризику 1: незначний рівень ризику. В цьому класі у випадку втрати або несанкціонованого чи неналежного доступу до персональних даних особи наслідки для неї є такими, що для їх запобігання буде достатньо використовувати звичайні (стандартні) заходи захисту інформації. До цієї групи скоріш за все відносяться бази даних бухгалтерії та відділу кадрів невеликих підприємств, бібліотек, комунальних організацій, а також клієнтські бази торгівельних та сервісних організацій (із певними виключеннями);

Клас ризику 2: середній рівень ризику. У цьому класі у випадку втрати або неавторизованого чи неналежного використання персональних даних суб'єкта

можуть наставати додаткові негативні наслідки. До баз персональних даних цього класу можна віднести бази, що містять дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також бази невеликого обсягу, що містять дані про здоров'я чи статеве життя, бази персональних даних, що містять або можуть містити опосередковану інформацію про світоглядне переконання, статеве життя чи здоров'я (наприклад, бази абонентів телекомунікаційних компаній, інтернет-сервіс провайдерів тощо.). Для таких баз даних може бути необхідним проведення незалежної оцінки застосовуваних заходів щодо захисту персональних даних.

Клас ризику 3: високий рівень ризику. У випадку, якщо несанкціоновані дії із персональними даними можуть мати серйозні наслідки для суб'єкта персональних даних, для їх захисту повинні вживатися суттєві заходи та використовуватися належні засоби захисту, а також обов'язково проводитися незалежна оцінка таких заходів [2].

Кроки, що захистять персональні данні:

Обов’язково читати політику конфіденційності,

Не користуватися послугами організацій, інтернет-ресурсів, які не дають можливість відмовитись від обробки персональних даних,

Цікавитись як саме і з якою метою будуть оброблятись персональні дані [3].

Висновок

У даній роботі було ретельно розглянуто проблеми захисту персональних даних у різних сферах діяльності, починаючи від систем державного управління і завершуючи підприємницькою діяльністю. Дослідження показало, що захист особистої інформації є критично важливим аспектом сучасного цифрового світу і вимагає комплексного підходу.

Було встановлено, що концепція персональних даних, їхній обіг та захист вимагають уваги до таких аспектів, як згода суб'єктів на обробку даних та виконання вимог законодавства. Дослідження виявило необхідність створення ефективних механізмів захисту, які б забезпечували недоторканість та конфіденційність особистих даних.

Також важливо підкреслити ризики, пов'язані з незаконним доступом до персональних даних, та важливість запобігання подібним ситуаціям. Запропоновано низку заходів безпеки, що дозволяють зменшити ймовірність порушення конфіденційності та цілісності особистої інформації.

Загальний висновок полягає в тому, що захист персональних даних є важливим завданням, яке стає все актуальнішим у сучасному цифровому середовищі. Ефективне впровадження запропонованих заходів безпеки може значно зменшити ризики порушення конфіденційності та забезпечити захист особистої інформації у різних сферах діяльності.

Література

[1] Jurliga Ligazakon https://jurliga.ligazakon.net/news/201367_personaln-dan-vikoristannya-zakhist--vdpovdalnst---shcho-potrbno-znatiDecentralized Finance (DeFi) Policy-Maker Toolkit, WEF 2021, [дата звернення 17.03.2024]
[2] Asterslaw https://www.asterslaw.com/ua/press_center/publications/personal_data_protection_some_practical_aspects/Blockchain Capital, About section, BCAP build section, https://www.blockchaincapital.com/about-us [дата звернення 17.03.2024]
[3] Zakon rada https://zakon.rada.gov.ua/laws/show/2297-17#TextToken Sniffer, actively monitoring, https://tokensniffer.com/ [дата звернення 17.03.2024]
[4] Rubryka https://rubryka.com/article/protect-personal-data/ [дата звернення 17.03.2024]

ПЕРСПЕКТИВИ РОЗВИТКУ ЦИФРОВОГО ОСВІТНЬОГО СЕРЕДОВИЩА У КОНТЕКСТІ БЕЗПЕРЕРВНОЇ ОСВІТИ

Анастасія КРАВЧЕНКО (магістр, спеціальність “Право”)[1]

[1]Kyiv National University of Contracture and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering
[1]akravchenkov1@gmail.com

Анотація
У цій роботі розглянуто перспективи розвитку цифрового освітнього середовища в контексті безперервної освіти. Зазначено, що цифрові технології дозволяють розширити доступ до освіти, індивідуалізувати навчання, розвивати комунікаційні навички та творчий потенціал, а також створювати цифрові портфоліо та системи визнання досягнень. Висвітлено важливість забезпечення доступності, якості та безпеки цифрових ресурсів для успішної реалізації потенціалу цифрової освіти.

Ключові слова
цифрове освітнє середовище, безперервна освіта, цифрові технології, індивідуалізація навчання, комунікаційні навички, творчий потенціал, цифрові портфоліо, системи визнання досягнень.

Вступ

У сучасному світі, що характеризується стрімким технологічним розвитком та глобальними трансформаціями, безперервна освіта набуває ключового значення для забезпечення конкурентоспроможності фахівців та їхньої успішної адаптації до мінливих реалій.

Інтеграція інформаційно-комунікаційних технологій (ІКТ) в освітній процес відкриває нові горизонти для розвитку цифрового освітнього середовища. Це комплексна екосистема, що об'єднує електронні платформи, онлайн-курси, мультимедійні ресурси, інтерактивні засоби навчання та співпраці. [3, 28].

Цифрове освітнє середовище не лише забезпечує безпрецедентний доступ до знань, а й створює унікальні можливості для персоналізації навчання, розвитку критичного мислення, творчих здібностей та ефективної взаємодії між усіма учасниками освітнього процесу [5, 266].

У цьому дослідженні розглядаються перспективи розвитку цифрового освітнього середовища в контексті безперервної освіти фахівців різних галузей. Акцентується увага на ключових аспектах, що визначають ефективність та успішність впровадження цифрових технологій у навчальний процес. Окрім переваг, аналізуються виклики, з якими стикаються сучасні освітні системи в процесі діджиталізації. Особлива увага приділяється забезпеченню рівного доступу, високої якості та безпеки цифрових ресурсів для всіх користувачів незалежно від їхнього професійного досвіду, місця проживання чи технічних можливостей.

Актуальність даного дослідження є беззаперечною в контексті сучасних викликів, що постають перед освітньою галуззю та потребами ринку праці. В умовах швидких технологічних змін, трансформації виробничих процесів та професійних компетенцій, безперервна освіта за допомогою цифрових технологій стає невід'ємним інструментом забезпечення фахової конкурентоспроможності та адаптивності.

Метою дослідження є визначення ключових переваг, виклики та перспективні напрямки розвитку цифрової освіти для забезпечення якісної безперервної освіти та професійного зростання на різних етапах життя.Початок форми.

Результати дослідження

Цифрове освітнє середовище відкриває нові перспективи для безперервної освіти фахівців різних галузей. Цифрові технології дозволяють створювати персоналізовані навчальні траєкторії, адаптовані до професійних потреб, інтересів та рівня знань на кожному етапі кар'єрного шляху [1, 3-4].

Інтерактивні онлайн-курси, мультимедійний контент, симуляції та ігрові елементи роблять процес навчання захопливим, сприяючи розвитку критичного мислення, творчості та залученості. Такі підходи допомагають учасникам глибше засвоювати знання і застосовувати їх для вирішення реальних професійних завдань [2, 4-6]. Онлайн-формати долають географічні та фінансові бар'єри, забезпечуючи рівний доступ до якісних навчальних ресурсів. Віртуальні комунікаційні інструменти створюють середовище для співпраці між фахівцями з різних куточків світу, обміну досвідом та спільного вирішення проблем [8, 335].

Успішний перехід до цифрового університету потребує не лише впровадження технологій, а й перегляду цілей, пріоритетів, організаційних принципів та підходів. Важливими є розвиток цифрової інфраструктури, підготовка викладацького складу, створення якісного контенту, організація дистанційного навчання та налагодження комунікації в цифровому середовищі [9, 203]. Ключова увага має приділятися забезпеченню високої якості навчальних

матеріалів та методик їх використання. Розробка цифрових курсів має ґрунтуватися на сучасних педагогічних підходах, враховуючи специфіку різних професійних сфер та категорій тих, хто навчається.

Необхідно підвищувати рівень цифрової компетентності усіх учасників освітнього процесу, зокрема формувати навички використання цифрових інструментів, критичного мислення, інформаційної грамотності, онлайн-комунікації, створення контенту, співпраці та самонавчання. Особливу увагу слід приділити питанням кібербезпеки та протидії технологічному тероризму в онлайн-середовищі. Необхідно створити сприятливі умови для розвитку цифрового освітнього середовища, зокрема нормативно-правову базу, фінансування та стимули для впровадження інновацій.

Цифрова трансформація сприяє підвищенню якості та доступності безперервної освіти для фахівців різних галузей. Онлайн-курси, цифрові платформи та інтерактивні ресурси забезпечують гнучкість та персоналізацію навчального процесу, даючи змогу навчатися у зручний час та місці [7]. Інтерактивний контент, відеоматеріали, симуляції, ігрові елементи роблять процес навчання захопливим, підвищуючи залученість. Практичні завдання та вирішення реальних кейсів сприяють розвитку навичок критичного мислення і творчості. Онлайн-формати долають географічні та фінансові бар'єри, надаючи рівний доступ до якісної освіти [4, 118].

Водночас, успішна цифрова трансформація потребує ретельного планування, підготовки педагогічних кадрів, створення якісного контенту та налагодження процесів забезпечення ефективності. Важливо визначити оптимальне поєднання цифрових і традиційних форматів з урахуванням технологічних та психолого-педагогічних аспектів.

Діджиталізація освітнього процесу вимагає проєктування та розробки якісних цифрових навчальних матеріалів. Необхідно формувати готовність педагогічних працівників та фахівців до використання й створення цифрових ресурсів, враховуючи питання кібербезпеки. Важливо навчити протидіяти кібертероризму, технологічному тероризму та неправомірним діям, а також впроваджувати інновації в цифровому середовищі [6, 108].

Ключовими освітніми технологіями для цифрового навчання є адаптивне, дистанційне, мобільне, змішане навчання. Діджиталізація є основним напрямом трансформації системи освіти, передбачаючи інтеграцію цифрових технологій для підвищення якості, доступності, персоналізації та диференціації навчання, розвитку цифрових компетентностей учасників. Це не лише зміна парадигми комунікації, а й потужний інструмент оптимізації навчального та дослідницького середовища, створення інноваційного освітнього простору [10, 70].

Висновки

Цифрове освітнє середовище відкриває нові перспективи для реалізації концепції безперервної освіти фахівців різних галузей. Цифрові технології

дозволяють створювати персоналізовані навчальні траєкторії, адаптовані до індивідуальних потреб, забезпечуючи гнучкість та рівний доступ до якісних ресурсів. Інтерактивний контент, мультимедіа, симуляції та ігрові елементи роблять процес навчання захопливим, сприяючи розвитку критичного мислення, творчості та залученості.

Успішний перехід до цифрової освіти потребує комплексного підходу, що включає розвиток цифрової інфраструктури, підготовку викладацького складу, створення якісного контенту, організацію дистанційного навчання та налагодження ефективної комунікації в онлайн-середовищі. Ключовими напрямками є забезпечення високої якості навчальних матеріалів, підвищення цифрової компетентності всіх учасників, врахування питань кібербезпеки та протидії технологічному тероризму.

Для успішної діджиталізації безперервної освіти необхідне залучення всіх зацікавлених сторін - закладів освіти, роботодавців, професійних асоціацій та органів влади. Потрібно створити сприятливі умови у вигляді нормативно-правової бази, фінансування та стимулів для впровадження інновацій. Системний підхід дозволить забезпечити високу якість та ефективність цифрового освітнього середовища для безперервного професійного розвитку.

Література

[1] Арешонков В. Ю. Цифровізація вищої освіти: виклики та відповіді. Вісник НАПН України. 2020. № 2 (2). С. 1-6.

[2] Бабаєв В. М., Стадник Г. В., Момот Т. В. Цифрова трансформація в сфері вищої освіти в умовах глобалізації. Комунальне господарство міст. Серія: Економічні науки = Municipal economy of cities: зб. наук. пр. Харків, 2019. Вип. 2. С. 2-9.

[3] Биков В., Спірін О., Пінчук О. Сучасні завдання цифрової трансформації освіти. Грамотність у цифрову епоху: Журнал кафедри ЮНЕСКО «Неперервна професійна освіта XXI століття». UNESCO chair journl «Lifelong Professional Education in the XXI Century». Київ, 2020. Вип. 1, С. 27-36.

[4] Колеснікова І. В. Цифровізація освітнього процесу в закладі післядипломної педагогічної освіти. Науковий часопис Нац. пед. ун-т імені М.П. Драгоманова. Серія 5. Педагогічні науки: реалії та перспективи, 2020. Випуск 78. С.117-120.

[5] Луговий В. І., Регейло І. Ю., Базелюк Н. В., Базелюк О. В. Глобальна цифровізація освітньо-наукового простору і виклики модернізації наукової періодики НАПН України. Інформаційні технології і засоби навчання: електрон. наук. фах. вид. Київ, 2019. Т. 73, № 5. С. 264-283.

[6] Модернізація освіти в цифровому вимірі: монографія / за наук. ред. Н. Морзе, О. Буйницької. Київ: Київ. ун-т ім. Б. Грінченка, 2021. 300 с.

[7] Наказ МОН України «Про затвердження Типової програми підвищення кваліфікації педагогічних працівників з розвитку цифрової компетентності». 2021. URL: https://mon.gov.ua/ua/npa/pro-zatverdzhennyatipovoyi-programi-pidvishennya-kvalifikaciyi-pedagogichnih-pracivnikiv-z-rozvitkucifrovoyi-kompetentnosti (дата звернення: 23.03.2024)

[8] Семеніхіна О. В., Юрченко А. О., Сбруєва А. А. та ін. Відкриті цифрові освітні ресурси в галузі ІТ: Кількісний аналіз. Інформаційні технології і засоби навчання. 2020. Том 75, №1. С. 331-348.

[9] Струтинська О. В., Умрик М. А. Сучасні освітні тренди в умовах розвитку цифрового суспільства. Інноваційна педагогіка: наук. журн. Одеса, 2020. Вип. 26. С. 201-205.
[10] Шпарик О. Концептуальні засади цифрової трансформації освіти: європейський та американський дискурс. Український педагогічний журнал = Ukrainian educational journal: наук. журн. / Ін-т педагогіки НАПН України. Київ, 2021. № 4. С. 65-76.

ПРОБЛЕМНІ ПИТАННЯ ПІДГОТОВКИ ДО ЄДКІ ЗІ СПЕЦІАЛЬНОСТІ 125 «КІБЕРБЕЗПЕКА» У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Вадим САРАПИН (студент)[1]
Дмитро ХЛАПОНІН (к. держ. упр., доцент кафедри політичних наук і права)[2]

[1,2]Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна

Анотація
У роботі досліджено проблемні питання, пов'язані з вивченням та підготовкою студентів до Єдиного державного кваліфікаційного іспиту зі спеціальності 125 у закладах вищої освіти. Аналізуються труднощі, з якими зіштовхуються студенти під час засвоєння програми навчання, відповідності навчальних програм вимогам сучасного ринку праці та потребам суспільства. Детально розглядаються фактори, що впливають на якість підготовки студентів, такі як методика навчання, наявність необхідного практичного досвіду та використання сучасних технологій. Висвітлені проблеми та можливі шляхи їх подолання з метою підвищення ефективності навчального процесу та підготовки конкурентоспроможних фахівців у галузі.
Ключові слова
Єдиний державний кваліфікаційний іспит, кібербезпека, нечіткість формулювання завдань ЄДКІ, тестові завдання.

Постановка задачі

Мета цієї доповіді полягає у ретельному аналізі та дослідженні проблемних аспектів, що пов'язані з підготовкою студентів до ЄДКІ зі спеціальності 125 «Кібербезпека» у вищих навчальних закладах. В цій роботі будуть розглянуті складнощі, які виникають у процесі вивчення навчальних матеріалів з даної спеціальності.

Основною метою дослідження є ідентифікація та аналіз факторів, які впливають на якість підготовки студентів. Будуть розглянуті такі аспекти, як ефективність методик навчання, наявність необхідного практичного досвіду та використання сучасних навчальних технологій.

Актуальність проблеми

Актуальність проблеми у підготовці студентів у вищих навчальних закладах надзвичайно висока в сучасних умовах освітнього процесу, оскільки ЄДКІ офіційно запровадили в 2023 році на пробному рівні для отримання статистики по студентах у їх рівні знань, а у 2024 році вже як основний екзамен, при цьому студентам була надана лише освітня програма без доступу до пробного білету і запитань, які можуть бути схожими з основною сесією. Студентам залишається тільки здогадуватися, що їх буде очікувати. Швидка технологічна зміна суспільного середовища ставить перед системою вищої освіти нові виклики та завдання.

Таким чином, актуальність проблеми полягає у необхідності постійного аналізу та вдосконалення процесів підготовки студентів до єдиного державного кваліфікаційного іспиту, з метою забезпечення їхньої успішної адаптації до змінних вимог сучасного ринку праці та забезпечення високого рівня професійної підготовки.

Основні проблеми, які очікують студентів у підготовці до ЄДКІ

Однією з основних проблем в підготовці до ЄДКІ є **стандартизація освітньої програми**, але кожен університет повинен мати свою унікальну спеціалізацію, що призводить до різноманітності в підходах до навчання. До прикладу може бути Київський національний університет будівництва і архітектури, що акцентує свою увагу на розробці розумних будинків та архітектурних інновацій, а в іншому навчальному закладі може бути більше акцент на криптографію чи програмування. Тобто, це може призвести до проблеми в самій підготовці до ЄДКІ, оскільки кожен викладач, який брав участь у створенні запитань сконцентровував увагу до інформації зі своєї програми, яку викладав. Це у свою чергу може створити незручності для студентів, які можуть не мати доступу до повної інформації про весь обсяг матеріалу, необхідного для успішного складання іспиту.

Іншою проблемою у підготовці може бути **обсяг матеріалу**. Студентам ймовірно буде складно згадати весь матеріал з першого по четвертий курс, оскільки ЄДКІ включає різноманітні теми по Кібербезпеці.

Недоступність якісних матеріалів для підготовки. Не завжди легко знайти якісні матеріали для підготовки до ЄДКІ, що може ускладнити процес навчання.

Також ключовою проблемою може бути **нечіткість формулювання завдань.** Деякі завдання в ЄДКІ можуть бути сформульовані нечітко або неоднозначно, що може призвести до помилок при їх тлумаченні.

Нестача практики у студентів. Багато студентів не мають достатньо практики роботи з тестовими завданнями, що може призвести до помилок під час іспиту.

Методи вирішення проблем у підготовці до ЄДКІ

Оскільки з проблемами у підготовці ми ознайомились, то тепер слід сказати про методи вирішення цих проблем.

Під час підготовки до іспиту, корисно скласти план, що включає в себе розподіл часу на вивчення різних тем, матеріалів або предметів, необхідних для іспиту. Важливо врахувати індивідуальні особливості здібностей та сильних сторін, а також обмеження часу, щоб забезпечити ефективну підготовку. Крім того, план може включати стратегії для повторення матеріалу, використання додаткових джерел інформації, наприклад, підручників, навчальних посібників або онлайн-курсів, а також призначення часу на практичні вправи та тести для перевірки знань. Ретельно розроблений план допоможе вам ефективно використовувати час підготовки та підготуватися до іспитів з впевненістю.

Варто відкрити саму програму по ЄДКІ та кожного дня опрацьовувати ряд тем. У кінці дня підготовки слід перевірити, як було засвоєно матеріал: можна знову стисло записати зміст усіх питань, що були опрацьовані в цей день.

Було б дуже корисно проглянути минулорічний іспит, проте нажаль його Міністерство освіти і науки України не надало.

Також хороша атмосфера під час підготовки є надзвичайно важливою для успішного вивчення. Важливо створити зручне і приємне середовище для навчання, де можна зосередитися на матеріалі без відволікань. Позитивний настрій також грає велику роль, тому важливо залишатися мотивованим і думати про свої цілі. Регулярні перерви допоможуть відпочити мозку і підтримати його продуктивність. Можна звернутись за підтримкою до своїх друзів та родичів, поділитись успіхами і труднощами. Здорове харчування і достатня гідрація також мають велике значення для вашого здоров'я та енергії під час навчання. Створення сприятливої атмосфери допоможе досягти більш високих результатів у навчанні.

Висновки

Загальний висновок відображає важливість вивчення та розуміння проблем, з якими стикаються студенти у процесі підготовки до єдиного державного кваліфікаційного іспиту зі спеціальності 125 «Кібербезпека» Цей екзамен ставить виклики перед освітньою системою, викладачами та самими студентами, оскільки вимагає глибокого розуміння матеріалу, ефективного використання часу та стресостійкості.

Проте, варто відзначити, що існують практичні методи та стратегії, які можуть допомогти студентам подолати ці виклики. Випрацювання ефективних методів вивчення, розвиток навичок управління часом, пошук додаткової підтримки є лише деякими з інструментів, які можуть бути використані для покращення процесу навчання.

Отже, розуміння цих проблем і використання відповідних стратегій може значно підвищити шанси студентів на успішне складання єдиного державного кваліфікаційного іспиту та досягнення високих результатів у їхній освітній траєкторії.

Література

[1] Що є кібербезпека? Визначення, історія, типи. URL - https://nordvpn.com/uk/cybersecurity/
[2] ЄДКІ. URL - https://mon.gov.ua/ua/tag/edki
[3] Програма ЄДКІ зі спеціальності 125 Кібербезпека на першому (бакалаврському) рівні вищої освіти. URL - https://learn.ztu.edu.ua/mod/resource/view.php?id=172056&forceview=1

ІСТОРИЧНІ ДИСЦИПЛІНИ У ПІДГОТОВЦІ БАКАЛАВРІВ ЗІ СПЕЦІАЛЬНОСТІ 281 «ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ»

Олексій ЛУК'ЯНОВ (к.і.н., доцент)[1]

[1]*Київський національний університет будівництва і архітектури, факультет урбаністики та просторового планування, кафедра політичних наук і права, Київ, Україна*
[1]*lukianov.op@knuba.edu.ua*

Abstract

The purpose of the article is to highlight the current problems of training in Ukraine for higher education in the specialty "Public Administration and management" (on the example of the first (bachelor's) level). The scientific novelty lies in the analysis of the current state of historical education of students studying in Ukrainian higher educational institutions in this specialty. The analysis was carried out by examining ten educational and professional programs "Public Administration" for the presence of academic disciplines on the subject of compulsory and elective components of these programs. The subject of the analysis was also the standard of higher education in the specialty "Public Administration and management " for the first (bachelor's) level, approved in 2018 by the Ministry of Education and Science of Ukraine. Despite of the requirements of the formation the historical competencies in the standard of higher education, the educational programs of many educational institutions include general historical disciplines in history and culture of Ukraine, which is not focused on the subject area of historical development of public administration.

Key words:

higher education, public administration and management, state administration, state service, historical competence, professional training, educational component, development of society, standard of higher education, educational programs.

Вступ

В сучасних умовах акредитації освітніх програм ЗВО велика увага приділяється формуванню професійних компетенцій здобувачів освіти.

Радикальні ідеологічні та інституціональні зміни, які відбулися в системі професійної підготовки державно-управлінських кадрів, що полягають, насамперед, у запровадженні з 2015-2016 рр. на першому (бакалаврському) рівні спеціальності та галузі знань "Публічне управління та адміністрування" (далі – ПУА) на заміну галузі знань "Державне управління" (раніше тільки магістерського рівня), що, у свою чергу, призвело до заміни пріоритетів у виборі освітніх компонент (дисциплін навчальних планів) у підготовці фахівців за спеціальністю ПУА за новими освітніми програмами в різноманітних університетах України [6; 7; 8; 9].

Наведені вище обставини актуалізують дослідження питання про те, як вплинули згадані зміни на формування компетентностей у здобувачів вищої освіти за спеціальністю 281 ПУА в Україні.

Різноманітним аспектам професійної підготовки управлінських кадрів органів державної влади, органів місцевого самоврядування України присвячено велику кількість наукових праць. Відзначимо вагомий науковий доробок у цій царині вітчизняних науковців: Андреєва С., Васильєвої О., Ващенка К., Гончарук Н., Гошовської В., Іжи М., Лугового В., Михненка А., Мотренка Т., Науменко Р., Серьогіна С., Хаджирадєвої С., Хрикова Є. та ін. Ми також деякі наші попередні публікації присвятили розгляду проблематики правової та державно-управлінської освітніх компонент у професійній підготовці здобувачів вищої освіти за спеціальністю "Публічне управління та адміністрування" в Україні [1; 2].

Метою дослідження є оцінка стану історичної освітньої компоненти у змісті професійної підготовки здобувачів вищої освіти за спеціальністю 281 ПУА на прикладі освітніх програм першого (бакалаврського) рівня в Україні.

Результати дослідження

Відповідно до вимог стандарту вищої освіти до 2015 року (лише на магістерському рівні) дисципліна «Теорія та історія державного управління» забезпечувала формування основних теоретичних та історичних знань державних управлінців [3]. Багаторічною практикою підготовки фахівців для сфери державного управління і адміністрування було обов'язкове включення в навчальні плани дисциплін з теорії та історії управління [4].

З 2018 року історичну компоненту для підготовки фахівців вищої освіти першого (бакалаврського) рівня за спеціальністю 281 ПУА містить відповідний Стандарт вищої освіти (далі Стандарт) у переліку загальних компетентностей випускника: «ЗК 03. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя» [9].

Також Стандартом закріплено нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання: «1. Використовувати базові знання з історичних, культурних, політичних, соціальних, економічних засад розвитку суспільства» [9, С. 7]. Наведений зміст показує, що розробники Стандарту вищої освіти чітко усвідомлювали, що без знання і розуміння історії, закономірностей розвитку інститутів управління не можливе розуміння сучасного стану сфери публічного управління та адміністрування.

З метою виявлення відповідності компонентам Стандарту дисциплін в ОПП ЗВО ми обрали деякі приклади серед ЗВО та представили у нижче наведеній таблиці (Таблиця 1).

Таблиця 1

Освітні компоненти (навчальні дисципліни), спрямовані на формування у здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 281 ПУА компетентностей в сфері історичних знань станом на 2020-2023 навчальні роки. *інформація з сайтів ЗВО

№	Найменування закладу вищої освіти, освітньої програми за спеціальністю ПУА, навчальні дисципліни з історичної тематики	
	Обов'язкові компоненти	*Вибіркові компоненти*
1.	***Київський національний економічний університет імені Вадима Гетьмана*** (ОПП "Публічне управління та адміністрування")	
	Неконкретизовані у програмі	Етно-соціальна історія українського суспільства Політична історія світу
2.	***НаУКМА*** (ОПП "Суспільне і приватне врядування")	
	Теорія та історія управління та самоврядування	не конкретизовані у програмі
3.	***Національний технічний університет*** «***Дніпровська політехніка***» (ОПП "Публічне управління та адміністрування")	
	Неконкретизовані у програмі	_
4.	***Київський національний університет імені Тараса Шевченка*** (ОПП "Урядування у публічній сфері")	
	Історія української держави Історія та теорія публічного управління та адміністрування Історія релігій	Історія філософії України
5.	***Київський національний університет будівництва і архітектури*** (ОПП «Державне управління у сфері містобудівної діяльності»)	
	Історія публічного управління України Історія філософії та філософської думки	Історія української культури Історія світової культури

6.	***Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"*** (ОПП «Адміністративний менеджмент», «Електронне урядування»)	
	Історія державного управління України.	не конкретизовані у програмі
7.	***Національний університет біоресурсів та природокористування України*** (ОПП "Публічне управління та адміністрування")	
	Історія української державності	-
8.	***Національний університет «Львівська політехніка»*** (ОПП "Публічне управління та адміністрування")	
	Історія державності та культури України Історія економіки та економічної думки	не конкретизовані у програмі
9.	***Харківський національний економічний університет імені Семена Кузнеця*** (ОПП "Публічне управління та адміністрування")	
	Соціальна та економічна історія України	-
10.	***Рівненський державний гуманітарний університет*** (ОПП "Публічне управління та адміністрування")	
	Історія України Історія української культури	Історія світової цивілізації Цінності Європейської цивілізації

З Табл. 1 ми бачимо що до змісту більшості ОПП в різних ЗВО за спеціальністю 281 ПУА включено дисципліни з історії публічного управління або вітчизняного державотворення, однак всі дисципліни дуже різноманітного тематичного характеру і об'єму. В двох ЗВО історичні дисципліни в ОПП з ПУА відсутні (історичний матеріал не конкретизовано в окремій дисципліні, а можливо входити до змісту інших навчальних дисциплін). Кількість історичних дисциплін в ОПП в різних ЗВО може різнитися від однієї до чотирьох історичних дисциплін (з урахуванням вибіркових). Освітні програми з ПУА часто містять такі загальноосвітні для багатьох спеціальностей дисципліни як «Історія та культура України», «Історія української культури», однак не можна визначити чи достатньо уваги приділяється в межах вивчення цих дисциплін розвитку інститутів публічного управління та адміністрування. Деякі ЗВО включають до обов'язкових компонент історію економіки та економічної думки або історію розвитку окремої галузі, хоча їх ОПП цього за тематикою не передбачає. На наш погляд історію розвитку окремих галузей і сфер управління було б доцільно відносити до вибіркових компонент.

Висновки

Проведене дослідження стану історичної освітньої компоненти у змісті вищої освіти її здобувачів за спеціальністю 281 ПУА на прикладі першого (бакалаврського) рівня в Україні дозволяє дійти таких висновків:

1. Для ефективного формування компетентностей здобувачів освіти доцільно в обов'язкові компоненти ОПП включати фундаментальні дисципліни з теорії та історії публічного управління;
2. За наявності в стандарті вищої освіти вимог щодо формування історичних компетенцій, в освітніх програмах багатьох закладів освіти викладають загальноосвітні історичні дисципліни з історії та культури України, що не орієнтовані на предметну сферу історичного розвитку інститутів публічного управління та адміністрування.
3. У змісті як мінімум двох освітніх програм з ПУА (Табл. 1) ми не бачимо дисциплін з історії (хоча це скоріше виключення), однак це ще не означає не відповідність Стандарту. Історична компонента в ОПП може бути не конкретизована та бути включена в зміст інших дисциплін ОПП. Однак, на нашу думку, це не бажано, оскільки розмиває історичну компоненту.
4. На наш погляд доцільно було б у програмах підготовки бакалаврського рівня виділяти не менше 6 кредитів на обов'язкову компоненту з історії публічного управління в Україні і Світі, а також серед вибіркових компонент цілком можливо додавати історичну дисципліну щодо розвитку специфічних управлінських інститутів залежно від особливої тематики ОПП в конкретному ЗВО.

Література

[1] Андреєв С. О., Лук'янов О. П. Актуальні проблеми правової підготовки здобувачів вищої освіти за спеціальністю "Публічне управління та адміністрування" в Україні. Наук. записки Ін-ту зак-ва ВРУ. 2020. № 2. С. 109–120.

[2] Andreiev, S., Geraskov, S., Dymenko, R., Kostrubitska, A., Lukianov. O. From state to public administration: an analysis of managerial training in higher education system of Ukraine. Financial and Credit Activity: Problems of Theory and Practice. 2021. Vol. 6, № 41. P. 521–533. URL: https://fkd.ubs.edu.ua/index.php/fkd/article/view/3492/3454 (дата звернення: 30.01.2024).

[3] Галузевий стандарт вищої освіти підготовки магістрів спеціальності 8.150101 "Державна служба" напряму підготовки 8.150000 "Державне управління". – Х. : ІНЖЕК, 2004. – 205 с.

[4] Державна служба України в історичному контексті: проблеми становлення та розвитку: зб. текстів виступів на наук.-практ. конф. (Київ, 18 листоп. 2008 р.) / Головне управління державної служби України ; за заг. ред. А. Вишневського — К. : Центр адаптації державної служби до стандартів Європейського Союзу, 2009. — 116 с.

[5] Історія державної служби в Україні : у 5 т. / відп. ред. Т. В. Мотренко, В. А. Смолій; редкол.: С. В. Кульчицький (кер. авт. кол.) та ін.; Голов. упр. держ. служби України; Ін-т історії НАН України. – К. : Ніка-Центр, 2009.

[6] Концепція реформування системи професійного навчання державних службовців, голів місцевих держадміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад : Розпорядження Кабінету Міністрів України від 24.06.2016 р. № 974-р. URL: https://zakon.rada.gov.ua/laws/show/974-2017-%D1%80 (дата звернення 30.01.2024).

[7] Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : Постанова Кабінету Міністрів України від 29.04.2015 р. № 266. Дата оновлення: 01.02.2017. URL: https://zakon.rada.gov.ua/laws/show/ru/266-2015-%D0%BF (дата звернення 30.01.2024).

[8] Деякі питання реформування системи професійного навчання державних службовців і посадових осіб місцевого самоврядування : Постанова Кабінету Міністрів України від 27.09.2016 р. № 674. Дата оновлення: 10.04.2019. URL: https://zakon.rada.gov.ua/laws/show/674-2016-%D0%BF (дата звернення 30.01.2024).

[9] Стандарт вищої освіти за спеціальністю 281 “Публічне управління та адміністрування” галузі знань 28 “Публічне управління та адміністрування” для першого (бакалаврського) рівня вищої освіти : затверджено наказом Міністерства освіти і науки України від 29.10.2018 р. № 1172. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/281-publichne-upravlinnya-ta-administruvannya.pdf (дата звернення 30.01.2024).

МОДЕЛЬ КОНТРОЛЮ НАКОПИЧЕННЯ РЕЙТИНГОВИХ БАЛІВ СТУДЕНТІВ ПРИ ВИВЧЕННІ КУРСУ ВИЩОЇ МАТЕМАТИКИ В ТЕХНІЧНОМУ УНІВЕРСИТЕТІ

Олена БАЛІНА (кандидат технічних наук, доцент кафедри)[1]
Ірина БЕЗКЛУБЕНКО (кандидат технічних наук, доцент кафедри)[2]
Юрій БУЦЕНКО (кандидат фізико-математичних наук, доцент кафедри)[3]

[1,2] Kyiv National University of Construction and Architecture, Department of Information technologies of Design and applied mathematics department.
[1]elena.i.balina@gmail.com,[2]i.bezklubenko@gmail.com
[3] National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Department of mathematical analysis and probability theory
[3]armchairdoc@ukr.net

Abstract

The article is devoted to the modeling of the general course of higher mathematics, typical for most technical universities of Ukraine, and the determination of the dynamic characteristics of the student's study of the material of this course. A mathematical model is defined for the practical application of the proposed methodology. The rationale for the feasibility of using such a method is given. For the elements of the mathematical model, the rules for their determination during the educational process are formulated.

Key words:

higher mathematics, calculus, differential equations, analitic geometry, linear algebra, discrete mathematics, computational mathematics, information support

Вступ

Включення України до Болонського процесу зробило неминучим впровадження формалізованого, а не описово-якісного індивідуального рейтингу студентів, який став основою для їх просування по щаблях навчального процесу. Таким чином, для кожного студента створюється процедура накопичення відповідних пунктів, як результат проходження контрольних заходів та виконання передбачених навчальними планами робіт. Слід зазначити, що з самого початку процесу впровадження цієї процедури було зрозуміло з якими проблемами доведеться зустрітись суб'єктам навчального процесу в цій ситуації. Розглянемо основні з цих проблем. Зазначимо, по-перше, що формальне запровадження рейтингів передбачає суто адитивний характер їх "нарахування", що не дозволяє висвітлювати та належним чином враховувати такі знання, вміння та навички конкретного студента. У зв'язку з цим постає також наступна проблема: наскільки рейтингові бали, у разі обчислення їх вищезгаданим способом, відображають загальний рівень розвитку студента, його здатність до оволодіння майбутньою спеціальністю у процесі подальшого навчання? Третьою проблемою, яка постає у випадку вищезгаданого формального підходу до рейтингової системи оцінювання академічних досягнень студента, є те, наскільки стабільною є його навчальна діяльність [4, с.52].

Мета доповіді

У даній роботі досліджується оптимальна структура курсу вищої математики, типового для технічного університету в Україні, та модель створення рейтингу студента при вивченні вказаної навчальної дисципліни.

Виклад основного матеріалу

Послідовність вивчення розділів навчальної дисципліни «Вища математика»

Зазначимо, що питання послідовності вивчення розділів, включених навчальною програмою до курсу «Вища математика», є чи не найпринциповішим із тих, що постають перед кожним лектором, якому випало викладати математичні курси у технічному університеті, в міру набуття ним педагогічного досвіду та розуміння проблем, пов'язаних із цим курсом та можливих шляхів їх вирішення. Серед факторів, які вирішальним чином впливають на виникнення цього комплексу проблем та шляхи їх вирішення у кожному конкретному випадку, зазначимо наступні [3, с.15]:

- кількість кредитів, виділених для вивчення студентами даної дисципліни, та їх розподіл між семестрами;

- вимоги, які пред'являються до знань та умінь, що мають набуватись студентами у процесі вивчення цього навчального предмету, з боку викладачів інших фундаментальних, загально-інженерних та спеціальних дисциплін;
- наявність особистих пріоритетів у кожного лектора;
- розподіл між семестровими модулями планових індивідуальних завдань та інших контрольних заходів.

Насамкінець зауважимо, що [5, с.87].

- оптимізація послідовності вивчення студентами розділів курсу вищої математики в ідеальному випадку має привести до відповідності їх позиціювання розміщенню відповідних курсів у навчальному плані студентів спеціальностей «Математика», «Прикладна математика»;
- визначальний вплив на зміст, кількість кредитів та взаємне розміщення розділів курсу математики має не позиція математичних кафедр, а побажання кафедр випускових.

Інформаційне забезпечення контролю освітньої діяльності студентів

Врахування вказаних у вступі до даної роботи трьох позицій вимагає специфічного інформаційного забезпечення, яке б дозволило максимально об'єктивно оцінювати досягнення студента як під час підсумкового контролю (проведення екзамену чи заліку), так і протягом всього семестру, безумовно важливою є опція аналізу загальної картини стану вивчення предмету в групі, серед студентів певної спеціальності , на факультеті.

Щодо першого пункту слід зазначити, що типова форма положення про оцінювання студента на заліку (іспиті) не передбачає мультиплікативності побудови рейтингу, тобто, наприклад, не містить формальних підстав для того, щоб не допускати до цих контрольних заходів студентів, який під час семестру не змогли продемонструвати володіння таблицею похідних і правилами диференціювання на задовільному рівні. На практиці неможливо надати цьому або ж іншим аналогічним показникам таку вагу (у балах), щоб просте підсумовування балів відображало його принципову важливість для підсумкової оцінки здібності учня та його ставлення до предмета. На жаль, формальні міркування наразі майже ніколи не дозволяють ввести в РСО таку позицію як «колоквіум», що, з усіх точок зору, було б, на наш погляд, найкращим вирішенням проблеми.

Щодо другого пункту, зауважимо, що інформація про кількість пропущених годин та наявність чи відсутність для цього поважних причин, незважаючи на її важливість з адміністративної точки зору, у даному випадку, як нам здається, не є істотною, а у випадку онлайнової форми навчання навіть директивно ігнорується.

Щодо третього моменту зауважимо, що стабільність досягнутих результатів є самоочевидною у випадку кращих і гірших учнів. Що стосується учнів середньої категорії, то для вчителя завжди було і є важливо розрізняти тих учнів, чиї

показники лише трохи перевищують незадовільні, і тих, які стабільно демонструють результати «В». Найрадикальнішим шляхом вирішення такої проблеми, звичайно, буде вводити до підсумкового рейтингу студента, крім суми набраних ним балів, також характеристики їх коливання за розділами курсу [1, с.32].

Враховуючи вищевикладене, нам видається раціональним паралельно з традиційною «таблицею» інформації про хід навчального процесу з предмета в групі, потоці, на факультеті ввести такі цифрові показники, які можна назвати «показниками». особистих досягнень» студента – personal achievement index-PAI.

Такий показник повинен містити такі дані в цифровому вигляді:

- «координати» студента (наприклад, номер залікової книжки або студентського квитка), що дозволяє визначити решту його персональних даних;
- «координати» предмета та забезпечення його викладання (випускові та допоміжні кафедри, місце в навчальному плані, викладачі, що проводять заняття з предмету).

Зрозуміло, що PAI має містити поточний рейтинг студента. Його необхідно доповнити даними про максимально можливий на даний момент рейтинг для студента та його місце в рейтингу групи за набраними балами [2, с.220].

Що стосується вищезгаданих, додаткових індикаторів, то перший з них може відображатися послідовністю нулів і одиниць. Для відображення другого пропонується ввести показник пунктуальності–time punctuality index-TPI, який можна розрахувати, наприклад, за формулою:

$$TPI = \sum_{k=1}^{n(t)} (t_k - T_k),$$

де tк - дата k-го контрольного заходу, передбаченого робочою навчальною програмою, Tk - фактична дата проходження студентом його на позитивну оцінку, n(t) - номер останнього контрольного заходу, проведеного до поточної дати. Таким чином, даний параметр навчальної діяльності студента показує загальний час його «затримки» при проходженні розділів типової розрахункової чи курсової роботи, колоквіумах, виконанні заліків тощо. Він може бути доповнений місцем студента в групі рейтинг, виведений за його зростанням.

Висновки

1. Розглянуто принципи формування курсу вищої математики з точки зору виділення розділів курсу та їх взаємного розміщення.
2. Запропоновано алгоритм побудови рейтингу студента при вивченні семестрового модуля навчальної дисципліни.

Література

[1] . Latest Cluster System Technology/ S. Egeta, I. Katte, E. Jinno// NEC Technical Journal.Vol.2, No.1.2007. - P. 30-33.
[2] A.A. Lubnina, N.M. Chikisheva, L.M.Simonova, E.E. Alenina, B.B.Khrustalev, R.Sh. Sadykova, R.R. Kharisova// International Review of Management and Marketing. 2016,6(52). - P. 219-224.
[3] Balyna Olena, Bezklubenko Irina, Butsenko Yuriy. (2017). Additional parameters are in informative providing of educational process. Fourth international Scientific-practical conference "Management of development of technologies", Ministry of education and science of Ukraine, Kyiv, 19-20 May 2017, Київ: Київський національний університет будівництва і архітектури, с. 15-16.
[4] Баліна О.І., Безклубенко І.С., Буценко Ю.П., Лабжинський В.А. (2020). Кластерний підхід до діагностування складних систем. У матеріалах VII Міжнародної науково-практичної конференції «Управління розвитком технологій. Інформаційні технології розвитку освіти», Київ: КНУБА, 2020 с. 51-53.
[5] Безклубенко І. С., Баліна О.І., Гетун Г.В., Буценко Ю.П. (2019). Вибір стратегії викладання курсу вищої математики в технічному ВНЗ. У матеріалах XIV International conference «Modern achievements of science and education», Netania, Israel, 26.09.-3.10.2019 (P. 86-88.).

РОЛЬ ТА МІСЦЕ ДЕРЖАВНИХ І НЕДЕРЖАВНИХ ОРГАНІВ ТА ОРГАНІЗАЦІЙ ПІД ЧАС ВЕДЕННЯ БОЙОВИХ ДІЙ, ПРОВЕДЕННЯ ОПЕРАЦІЇ

Петро ВОРОНА (д. держ. упр., професор)[1]

[1] *Луганський національний університет імені Тараса Шевченка*

Органи державної влади поділяються на центральні та місцеві. До центральних органів влади відносяться Верховна Рада, Президент, Кабінет Міністрів і міністерства, суди. А до місцевих відносимо: державні адміністрації в областях, районах, містах Києві та Севастополі.

Центральні органи влади створюють всі умови для належного утримування та забезпечення ЗСУ у період ведення бойових дій та проведення операції. Верховна рада України створює для цього відповідну правову базу як фінансування (закладаючи в державному бюджеті потрібні суми витрат для оборонних потреб) так і для мобілізаційного забезпечення ЗС України. Як приклад, розгляд проекту Закону Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку, що має унормовувати у відповідності до воєнного стану правила та порядок загальної мобілізації, яку визначають наразі чинні закони та нормативно-правові акти:

1) «Про Мобілізаційну підготовку та мобілізацію» [13];

2) «Про військовий обов'язок і військову службу» [9];

3) Постанова Кабміну № 1487 про затвердження «Порядку організації та ведення військового обліку призовників, військовозобов'язаних та резервістів» [10];

4) Наказ № 402 Міністерства оборони про затвердження «Положення про військово-лікарську експертизу в Збройних Силах України» [11].

Саме на підставі цих документів проводиться мобілізація з лютого 2022 року. Окрім того, Верховна рада України у межах своїх повноважень виконує завдання національної безпеки та оборони, створюючи належне нормативно-правове поле для діяльності органів виконавчої влади (Кабінет Міністрів України) та місцевого самоврядування. До предметів відання комітету з питань національної безпеки, оборони та розвідки Верховної ради України віднесені:

- державна політика у сферах національної безпеки і оборони;
- законодавче забезпечення діяльності органів сектору безпеки і оборони, у т. ч. щодо впровадження принципів і стандартів Організації Північноатлантичного договору (НАТО) та досягнення критеріїв, необхідних для набуття Україною членства в НАТО;
- демократичний цивільний контроль;
- правовий режим державного кордону, воєнного та надзвичайного стану;
- оборонно-промисловий комплекс та державна система страхового фонду документації;
- військове та військово-технічне співробітництво з іншими державами;
- участь у міжнародних операціях з підтримання миру і безпеки, міждержавних системах та механізмах міжнародної колективної безпеки;
- військова служба, Збройні Сили України, інші військові формування, утворені відповідно до законів України;
- охорона державної таємниці;
- боротьба з тероризмом;
- оборонні закупівлі;
- соціальний і правовий захист військовослужбовців та членів їх сімей;
- військова наука та освіта;
- альтернативна (невійськова) служба;
- державна система спеціального зв'язку;
- космічна діяльність (у частині питань, що належать до сфери національної безпеки і оборони);
- національна безпека у кіберпросторі, сфері критичної інфраструктури, кібероборони, кіберрозвідки, протидії кібертероризму і кібершпигунству та безпеки урядового зв'язку та інше [5].

У відповідності **до предметів відання комітету з питань національної безпеки, оборони та розвідки Верховна рада України** здійснює правове та фінансове забезпечення Сил оборони у період ведення бойових дій та проведення

військових операцій. Окрім цього військові операції Сил оборони піддаються парламентському цивільному контролю, у томі числі й через розгляд депутатських звернень та запитів з зазначеної парламентом тематики [].

Центральні органи державної влади (часто відображаючи волю недержавних органів та громадських організацій, як складових громадянського суспільства) під час ведення бойових дій, проведення військових операції тісно координують свої дії **через Раду національної безпеки і оборони України,** яка відповідно до Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України а її рішення вводяться в дію Указами Президента [7].

Та головною ланкою в системі державних і недержавних органів та організацій, що мають вплив під час ведення бойових дій, проведення операції звісно є Президент України, як Верховний Головнокомандувач ЗС України він є гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина (ст. 10 КУ). Президент України є гарантом реалізації стратегічного курсу держави на набуття повноправного членства України в ЄС та в НАТО [6].

Як Верховний Головнокомандувач Збройних Сил України він призначає та звільняє з посад вище командування Збройних Сил України, інших військових формувань та здійснює керівництво у сферах національної безпеки й оборони держави; очолює Раду національної безпеки і оборони України; вносить до Верховної Ради України подання про оголошення стану війни та у разі збройної агресії проти України приймає рішення про використання ЗС України та інших утворених відповідно до законів України військових формувань; приймає відповідно до закону рішення про загальну або часткову мобілізацію та введення воєнного стану в Україні або в окремих її місцевостях у разі загрози нападу, небезпеки державній незалежності України [6].

Профільним державним органом у справі ведення бойових дій, проведення операції ЗСУ є Міністерство оборони України та інші профільні державні установи. Воно є центральним органом виконавчої влади і військового управління, у підпорядкуванні якого перебувають Збройні сили України. Міноборони України є головним (провідним) органом у системі центральних органів виконавчої влади щодо забезпечення реалізації державної політики у сфері оборони. Основними завданнями Міноборони (МОУ) є:

1) забезпечення формування та реалізація державної політики з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва у мирний час та особливий період:

- організації в силах оборони заходів оборонного планування;
- визначення засад воєнної, військової кадрової та військово-технічної політики у сфері оборони;

2) здійснення військово-політичного та адміністративного керівництва ЗСУ;

3) забезпечення формування та реалізація державної політики з питань національного спротиву;

4) здійснення в установленому порядку координації діяльності органів державної влади та місцевого самоврядування щодо підготовки держави до оборони;

5) забезпечення в межах повноважень, передбачених законом, реалізації державної політики з оборонних питань, що пов'язані з використанням повітряного простору України та захистом суверенітету держави;

6) координація діяльності Держспецтрансслужби для забезпечення стійкого функціонування транспорту в мирний час та в особливий період [4, 18].

Особливу роль у веденні бойових дій та проведенні військових операцій має **Генеральний штаб Збройних сил України** (ГШ) - головний військовий орган з планування оборони держави, управління застосуванням ЗС України, координації та контролю за виконанням завдань у сфері оборони іншими військовими формуваннями, органами виконавчої влади, органами місцевого самоврядування, правоохоронними органами, Державною спеціальною службою транспорту і Державною службою спеціального зв'язку та захисту інформації України. ГШ – є робочим органом Ставки Верховного Головнокомандувача ЗСУ [18].

Коли в перші години широкомасштабної війни в України ввели воєнний стан, то це радикально змінило життя усіх українців, діяльність державних і самоврядних інституцій. Указом Президента України, що був затверджений Законом України, обласні, Київська міська державна адміністрація, органи місцевого самоврядування мали утворити ради оборони та забезпечити сприяння військовому командуванню у запровадженні та здійсненні заходів правового режиму воєнного стану. У населених пунктах на територіях активних бойових дій **створили військові адміністрації** [8].

Попри воєнний стан, **місцеве самоврядування, як орган місцевої влади** продовжує свою роботу сьогодні по всій Україні. Органи місцевого самоврядування (ОМС) усіх рівнів співпрацюють з військовим командуванням та військовими адміністраціями, а за потреби погоджують між собою окремі повноваження. Додаткові функції, які випали на долю місцевої влади у перші дні війни, стосувалися великого напливу ВПО. ОМС організували реєстрацію відповідного статусу, видачу довідок і за допомогою мешканців громад налагодили процес розміщення людей, які покинули свої оселі. Під час воєнних дій окремі населені пункти України опинилися під тимчасовою російською окупацією. Перед представниками тамтешніх органів місцевого самоврядування постало питання щодо дій за таких умов [4, 12].

15 травня Верховна Рада прийняла Закону України **«Про правовий режим воєнного стану»** щодо функціонування місцевого самоврядування у період дії воєнного стану. Закон передбачає врегулювання здійснення повноважень в органах місцевого самоврядування в умовах воєнного стану, спрощення процедури прийняття кадрових рішень щодо посад в органах місцевого самоврядування, посад керівників суб'єктів комунального сектору економіки [15].

За умов необхідності розв'язання складних проблем воєнного стану суттєво підвищено ефективність взаємодії між органами державної влади, керівництвом територіальних громад та представниками громадських і волонтерських організацій. Зокрема налагоджено механізм економічної підтримки ЗСУ, здійснено успішну релокацію частини бізнесу із зони бойових дій і сусідніх із нею територій у західні регіони, проводиться евакуація цивільного населення. Це є свідченням ефективності такої самоорганізації суспільства, як місцеве самоврядування. Досвід, набутий Україною за час війни, демонструє беззаперечну перевагу самоорганізації населення перед централізованим управлінням.

Попри активну фазу російсько-української війни та перехід всіх політичних і громадських процесів у воєнну площину, в Україні продовжується законотворча робота щодо вдосконалення механізмів місцевої демократії, а також - щодо покращення відкритості й прозорості діяльності органів місцевого самоврядування. Через війну в Україні, яку розв'язала росія, третина українців можуть мати проблеми в отриманні достатньої кількості харчових продуктів. В цьому напрямку ініційовано впровадження ініціативи «Сади Перемоги» - надання консультаційної підтримки територіальним громадам та домогосподарствам, які займатимуться городництвом, зберіганням, переробленням продукції тощо.

Крім того, громади, які постраждали від російської агресії, та нині звільнені від окупації, розпочали відбудову територій. Представники місцевого самоврядування обстежують пошкоджене житло, оцінюють збитки й вже отримують від держави ресурси на відшкодування завданої шкоди. Але в той же час більшість з них активно допомагають військовим підрозділам [2].

Для підтримки українських міст у пошуку партнерів створена нова онлайн-платформа за підтримки Конгресу місцевих і регіональних влад Ради Європи. Платформа є безплатним онлайн-інструментом. Він дозволяє ОМС України та інших регіонів Європи поділитися своїми потребами та пропозиціями, пов'язаними з міською інфраструктурою, а також налагодити прямі зв'язки для співпраці з отримання практичної допомоги.

На територіях, на яких введено воєнний стан, для забезпечення дії Конституції та законів України, забезпечення разом із військовим командуванням запровадження та здійснення заходів правового режиму воєнного стану, оборони, цивільного захисту, громадської безпеки і порядку, захисту критичної інфраструктури, охорони прав, свобод і законних інтересів громадян можуть утворюватися тимчасові державні органи - військові адміністрації. Рішення про утворення військових адміністрацій приймається Президентом України за поданням обласних державних адміністрацій або військового командування. **Військові адміністрації населених пунктів** утворюються в межах територій територіальних громад, у яких сільські, селищні, міські ради та/або їхні виконавчі органи, та/або сільські, селищні, міські голови не здійснюють покладені на них повноваження Конституцією та законами України.

Військові адміністрації населених пунктів формуються з військовослужбовців військових формувань, утворених відповідно до законів України, осіб рядового і начальницького складу правоохоронних органів, служби цивільного захисту, які відряджаються до них у встановленому законодавством порядку для виконання завдань в інтересах оборони держави та її безпеки із залишенням на військовій службі, службі в правоохоронних органах, органах та підрозділах цивільного захисту без виключення зі списків особового складу, а також працівників, які уклали трудовий договір з обласними військовими адміністраціями (у разі їх утворення) або з ГШ Збройних Сил України (якщо у відповідній області не утворено обласну військову адміністрацію) [2].

Недержавні органи та організації під час ведення бойових дій, проведення операції як правило взаємодіють через **всеукраїнський волонтерський рух.** І працюють у напрямку забезпечення ресурсами українських військових (Збройних Сил, Національної гвардії тощо), які з 2014 року стримують російську збройну агресію. Цей рух виник стихійно з початком військового конфлікту в різних регіонах України. Рух виникав стихійно з окремих волонтерів, що об'єднувалися в групи. З часом з'явилися лідери, що привели роз'єднані самоорганізовані групи до централізованого керування, а відтак - посиленням впливу на державний апарат та ефективність допомоги. Волонтерських організацій та окремих активістів, що допомагають українським військовим, існують тисячі. Точну їх кількість визначити неможливо: вона постійно змінюється, а чимало волонтерів не афішують свою діяльність.

Багато волонтерів займаються виготовленням екіпірування власноручно. Так, виготовляють на власному обладнанні аптечки, чохли для бронежилетів, одяг, маскувальні сітки. Часто волонтери збирають БпЛА для військової розвідки.

Окремі волонтерські групи займаються допомогою в пошуках зниклих або загиблих солдатів. Основна частина таких рухів сформувалась після Іловайської трагедії, коли кількість загиблих та зниклих безвісти, за деякими свідченнями, йшла на сотні. Однією з таких організацій є Союз «Народна пам'ять», що працював в зоні АТО з вересня 2014 року [17].

Окремо варто згадати ще одну **недержавну волонтерську структуру – *«Госпітальєри»*** - добровольчу організацію парамедиків. Вона була заснована Яною Зінкевич на початку бойових дій в Україні ще у 2014 році. Її гасло: «Заради кожного життя». А підрозділ «Янголи Тайри» на чолі з парамедиком Юлією Георгіївною Паєвською, яка перебувала певний час у полону після облоги Маріуполя є зразком самовідданого служіння країні й народу. Вони займаються евакуацією наших бійців з поля бою та надають допомогу при невідкладних станах на догоспітальному етапі [3, 16].

Часто волонтери привертають увагу суспільства до неякісної роботи адміністративних армійських відомств. Вони ж роблять інформацію про спорядження армії більш відкритою. Окремі волонтерські групи борються з корупцією в оборонних відомствах. Волонтери займаються евакуацією громадян з зони бойових дій. Так, переважно, допомога надходить до людей, що самі покинути території бойових дій не можуть - літні люди та діти.

Волонтери-зоозахисники займаються вивезенням та пошуком дому для домашніх тварин, що залишилися без дому.

Діяльність волонтерів підтримали чимало підприємств. Так, «Нова пошта» надала багатьом волонтерським групам та окремим активістам можливість безкоштовної відправки будь-якої кількості допомоги. За оцінкою керівника волонтерської групи «Повернись живим» Віталія Дейнеги, за перші 2 роки війни (станом на квітень 2016) волонтери зібрали на потреби військових більше мільярда гривень (у тому числі великі волонтерські організації - близько 300 млн). Для порівняння: збір грошей через SMS-сервіс «565», що тривав до жовтня 2015 (повідомлення на цей номер коштувало 5 грн, що йшли Міноборони) приніс 38,8 млн грн, а «податок на війну» (1,5 % від зарплати), що збирається з серпня 2014, - майже 14 млрд грн. [1].

На початку активної діяльності волонтерського руху механізмів його взаємодії з владними структурами практично не було. Але пізніше значна роль та високий авторитет волонтерів підштовхнули владу до співпраці.

Напередодні широкомасштабного вторгнення національним парламентом прийнято Закон України **«Про основи національного супротиву»** [14]. У ньому «національний спротив - комплекс заходів, які організовуються та здійснюються з метою сприяння обороні України шляхом максимально широкого залучення громадян України до дій, спрямованих на забезпечення воєнної безпеки, суверенітету і територіальної цілісності держави, стримування і відсіч агресії та завдання противнику неприйнятних втрат, з огляду на які він буде змушений припинити збройну агресію проти України». Та варто акцентувати, що в основі національного супротиву є формування територіальної оборони. При цьому цивільна складова територіальної оборони включає державні органи, органи місцевого самоврядування, які залучаються до територіальної оборони.

Військово-цивільна складова територіальної оборони включає штаби зон (районів) територіальної оборони та добровольчі формування територіальних громад, які залучаються до територіальної оборони.

Основою підготовки громадян України до національного спротиву є їх загальновійськова підготовка, яка організовується за територіально-зональним принципом, ґрунтується на засадах високої мотиваційної привабливості та узгоджується з процесом трансформації системи комплектування за призовом відповідно до принципів та найкращих практик держав - членів НАТО [14-15].

Тому, загальновійськова підготовка громадян України полягає в опануванні базовими загальновійськовими знаннями, практичними вміннями і навичками та поділяється на початкову і базову підготовку. Для розміщення військових частин Сил ТрО ЗС України в межах відповідних адміністративно-територіальних одиниць використовується інфраструктура (фонди) ЗС України, а також інфраструктура (фонди) складових сил безпеки та сил оборони, органів місцевого самоврядування у порядку, визначеному КМ України.

Метою національного супротиву є якнайширше залучення населення країни до оборони України, активної й організованої протидії агресору на всій території України та підготовка до такої протидії всіх мешканців громад, тому у цьому

процесу важлива тісна взаємодія державних і недержавних органів та організацій, особливо під час ведення бойових дій, проведення операції проти ворога.

Література

[1] Благодійний фонд «Повернись живим» - допомога ЗСУ. URL: savelife.in.ua.
[2] Військові адміністрації населених пунктів. URL: https://law.chnu.edu.ua/viiskovi-administratsii-ta-ta-viiskovo-tsyvilni-dministratsii/#:~:text=Військові%20адміністрації%20населених%20пунктів%20утворюються%20в%20межах%20територій,а%20також%20в%20інших%20випадках%2C%20передбачених%20Законом%20№389.
[3] Госпітальєри – Медичний батальйон. URL: hospitallers.life.
[4] Кабінет Міністрів України. Офіційне інтернет-представництво. URL: kmu.gov.ua.
[5] Комітет з питань національної безпеки, оборони та розвідки Верховної ради України. Офіційний сайт. URL: https://komnbor.rada.gov.ua/.
[6] Конституція України. Прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 року. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-вр#Text.
[7] Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua.
[8] Про військово-цивільні адміністрації. Закон України від 3 лютого 2015 року № 141-VIII. Відомості Верховної Ради (ВВР), 2015, № 13, ст.87. URL:
[9] Про військовий обов’язок і військову службу. Закон України від 25 березня 1992 року № 2232-XII. Відомості Верховної Ради України (ВВР), 1992, № 27, ст.385 URL: https://zakon.rada.gov.ua/laws/show/2232-12#Text.
[10] Про затвердження «Порядку організації та ведення військового обліку призовників, військовозобов’язаних та резервістів». Постанова Кабміну № 1487. URL: ttps://www.hsa.org.ua/blog/zatverdzheno-novyj-poryadok-organizatsiyi-ta-vedennya-vijskovogo-obliku/.
[11] Про затвердження «Положення про військово-лікарську експертизу в Збройних Силах України». Наказ № 402 Міністерства оборони України. URL: https://zakon.rada.gov.ua/laws/show/z1109-08#Text.
[12] Про місцеве самоврядування в Україні. Закон України від 21 травня 1997 року. № 280/97-ВРВідомості Верховної Ради України (ВВР), 1997, № 24, ст.170. URL: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text.
[13] Про мобілізаційну підготовку та мобілізацію. Закон України від 21 жовтня 1993 року № 3543-XII. Відомості Верховної Ради України (ВВР), 1993, № 44, ст.416. URL: https://zakon.rada.gov.ua/laws/show/3543-12#Text.
[14] Про основи національного супротиву. Закон України від 16 липня 2021 року № 1702-IX. Відомості Верховної Ради (ВВР), 2021, № 41, ст.339. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text.
[15] Про правовий режим воєнного стану. Відомості Верховної Ради (ВВР), 2015, № 28, ст.250. Закон України від 12 травня 2015 року № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.
[16] Рагуцька Л. Як «янголи Тайри» рятують життя на передовій: розповідь легендарного парамедика. Oboz.ua. URL: https://incident.obozrevatel.com/ukr/crime/mi-ne-v-silah-zupiniti-smert-ale-mozhemo-vidstrochiti-ii-prihid-legendarnij-paramedik.htm.

[17] Союз «Народна пам'ять». Всеукраїнська громадська організація. URL: ua.unm.org.ua.
[18] Структура апарату Головнокомандувача та Генерального Штабу. Міністерство оборони України. URL: mil.gov.ua.

CYBERSECURITY IN THE CONTEXT OF EDUCATION DIGITALIZATION

Yevhenii STEPANCHENKO (bachelor) [1]
Vadym POLISHCHUK (bachelor) [2]

[1,2]Kyiv National University of Contracture and Architecture, Faculty Of Automation And Information Technologies, Department Of Cyber Security And Computer Engineering, Kyiv, Ukraine
[1]stepanchenko_yy-2023@knuba.edu.ua
[2] polishchuk_vs-2023@knuba.edu.ua

Abstract
This article examines critical aspects of cybersecurity in the context of the digitalisation of education, exploring common cyber threats faced by educational institutions, including data breaches and phishing attacks that compromise sensitive student and institutional data. The article also discusses the impact of threats on the educational ecosystem and the importance of implementing cybersecurity tools and measures. The article emphasises the need for a proactive and comprehensive approach to cybersecurity given the rapid digitalisation of education.
Key words:
Cybersecurity , digitalisation of education, digital technologies, personal data.

Introduction

The digitalization of education has revolutionized the way knowledge is disseminated and acquired, offering unprecedented access to information and learning tools. However, this shift also brings significant cybersecurity challenges that educational institutions must address to protect sensitive data and maintain the integrity of their systems. This article explores the various cyber threats faced by the education sector, discusses effective strategies to mitigate these risks, and provides an overview of digitalization in education, ensuring a secure digital learning environment.

Overview of Digitalization in Education

The digitalization of education refers to the integration of digital technologies into the teaching and learning processes. This transformation has been driven by several factors:

- Adoption of Digital Tools and Platforms: Educational institutions have increasingly adopted digital tools such as learning management systems (LMS), virtual

classrooms, and educational apps. These tools enhance the accessibility, flexibility, and efficiency of educational delivery.

- Online Learning: The rise of e-learning platforms and Massive Open Online Courses (MOOCs) has made education more accessible to a global audience. Online learning allows students to access course materials, submit assignments, and interact with instructors and peers from anywhere in the world.

- Use of Data Analytics: Data analytics in education helps in monitoring student performance, identifying learning gaps, and personalizing learning experiences. This data-driven approach enables educators to make informed decisions to improve educational outcomes.

- Interactive and Multimedia Content: Digitalization enables the use of interactive and multimedia content such as videos, simulations, and gamified learning experiences. These resources make learning more engaging and can cater to different learning styles.

While digitalization offers numerous benefits, it also introduces new vulnerabilities and risks, necessitating robust cybersecurity measures [1].

Cybersecurity Threats in Education

The education sector, spanning from universities to primary schools, encounters unique cybersecurity risks and threats due to the sensitive nature of its data. The diverse array of devices and systems employed in education provides numerous opportunities for attackers to target educational institutions. With the ongoing shift towards online education, there is an increasing exposure of networked devices and systems

Moreover, decentralized IT management and, in some cases, limited cybersecurity resources often result in inconsistent security policies and insufficient controls. Additionally, educational institutions and their third-party suppliers store substantial amounts of personal data, thereby raising the risk and severity of data breaches and identity theft incidents.

Furthermore, the heavy reliance on digital communication and online collaboration platforms heightens the vulnerability to phishing and social engineering attacks. This susceptibility is exacerbated by common open internet access policies and Bring Your Own Device (BYOD) practices within these institutions. The participation of many educational institutions in research activities and their possession of sensitive intellectual property also contributes to their attractiveness as targets for cybercriminals and state actors.

Common threats include:

- Data Breaches: Unauthorized access to sensitive information such as student records, financial data, and personal information can lead to identity theft and other malicious activities [2].

- Ransomware Attacks: Cybercriminals deploy ransomware to encrypt institutional data, demanding a ransom for its release. This can disrupt educational activities and result in significant financial losses [3].

- Phishing Scams: Fraudulent attempts to obtain sensitive information through

deceptive emails or websites can compromise user credentials and lead to further security breaches [4].

The analysis of disinformation counteraction strategies includes research and evaluation of various methods and approaches used to prevent the spread of disinformation and combat it.

These threats not only endanger the privacy and security of students and staff but also undermine the trust placed in educational institutions [2][5].

Effective Strategies for Ensuring Cybersecurity

To safeguard against these threats, educational institutions must implement comprehensive cybersecurity measures. Key strategies include:

- Regular Software Updates and Patch Management: Ensuring all systems and applications are up-to-date with the latest security patches can prevent exploitation of known vulnerabilities [3].
- Strong Password Policies and Multi-Factor Authentication (MFA): Implementing robust password requirements and MFA can significantly enhance the security of user accounts [3].
- Secure Network Infrastructure: Deploying firewalls, intrusion detection systems, and secure Wi-Fi networks helps protect the institutional network from unauthorized access and cyber threats [3].

In addition to the technical measures outlined above, it's crucial to recognize the unique challenges that the education sector often faces in implementing cybersecurity strategies. Educational institutions typically operate within constrained budgets and resource limitations, which can present significant barriers to deploying comprehensive cybersecurity solutions. Moreover, the decentralized nature of many educational systems, with numerous departments, faculty members, and students accessing networks from various locations and devices, amplifies the complexity of securing digital infrastructures.

To address these challenges effectively, educational institutions must adopt a pragmatic and adaptive approach to cybersecurity. This may involve prioritizing investments in cost-effective yet robust security solutions tailored to the specific needs and constraints of the education sector. Collaborative efforts between educational institutions, government agencies, and industry partners can also facilitate resource-sharing, knowledge exchange, and collective defense mechanisms against cyber threats.

Furthermore, fostering a culture of cybersecurity awareness and accountability across all levels of the educational ecosystem is paramount. This includes providing ongoing training and support for faculty, staff, and students to enhance their understanding of cyber risks and best practices for mitigating them. By promoting a shared responsibility for cybersecurity and empowering individuals to recognize and respond to threats proactively, educational institutions can significantly strengthen their overall security posture. By implementing these strategies, educational

institutions can establish a much more secure digital environment, ensuring that the learning process remains safe and uninterrupted.

Conclusion

As education continues to digitalize, cybersecurity must be prioritized to protect sensitive data and ensure the smooth functioning of educational activities. Understanding the nature of cyber threats and implementing effective security strategies are essential steps toward building a resilient digital education infrastructure. Collaboration among educators, IT professionals, and policymakers is crucial in fostering a culture of cybersecurity awareness and preparedness. By taking proactive measures, educational institutions can safeguard their digital ecosystems and provide a secure environment for future generations of learners.

References

[1] SMITH Kshetri, N. (2013). Cybercrime and cybersecurity in the global South. Palgrave Macmillan.
[2] Lipton, B., & Ford, G. (2018). Education and the Cybersecurity Workforce: Meeting the Needs of Federal Agencies. Journal of Cybersecurity Education, Research and Practice, 2018 (1), Article 1.
[3] NIST. (2020). Cybersecurity Framework. National Institute of Standards and Technology. Accessed: 2024. [Online]. Avaible: //www.nist.gov/cyberframework.
[4] Ponemon Institute. (2021). Cost of a Data Breach Report. Accessed: 2024. [Online]. Avaible: https://www.ibm.com/security/data-breach.
[5] West, J., & Gill, P. (2019). The impact of cyber attacks on higher education. Journal of Information Technology Education: Research, 18, 101-121.

ІНОВАЦІЙНІ ПІДХОДИ В ЦИФРОВІЙ ОСВІТІ: АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Ростислав ПИСАНИЙ (студент)[1]

[1,] *Київський національний університет будівництва і архітектури, факультет автоматизації інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії спеціальність: 123, Київ, Україна*
[1] *balabla11114@gmail.com*

Анотація

У статті розглянуто сучасні підходи до цифровізації навчального процесу в закладах вищої освіти. Мета дослідження — зрозуміти й оцінити сучасні моделі цифрового навчання та їх вплив на педагогічні процедури. Проведено аналіз останніх досліджень, що стосуються застосування цифрових технологій, таких як інтерактивні відеоуроки, онлайн-лабораторії, аналітичні інструменти для персоналізації навчання, та підготовка педагогічного персоналу до роботи в умовах цифрового навчання. На основі отриманих результатів запропоновано конкретні пропозиції щодо впровадження цифрових технологій у навчальні заклади, що включають розширення доступу до цифрових платформ, використання VR та AR технологій, створення інтерактивних навчальних матеріалів, впровадження аналітичних інструментів та підготовку викладачів.

Ключові слова:

Цифровізація освіти, педагогічні процедури, інтерактивне навчання, персоналізація, VR/AR технології, аналітичні інструменти.

Вступ

Роль технологій у сучасному світі надзвичайно зросла, особливо в галузі освіти, де цифрове навчання набирає поширення. Поява цього явища не тільки відкриває нові шляхи для навчання, але й вимагає регулярного перегляду та трансформації освітніх систем відповідно до сучасних вимог.

Цифровізація освіти кардинально змінює традиційні педагогічні процедури, впливаючи на методи викладання, оцінювання та взаємодії між викладачами і студентами. В умовах швидкого розвитку технологій постає питання адаптації навчальних процесів до нових вимог та можливостей цифрового середовища. Традиційні педагогічні методи часто не відповідають потребам сучасних студентів, які вимагають інтерактивності, доступності та персоналізованого підходу до навчання.

У сфері освіти дослідницькі дослідження підтверджують, що використання електронного навчання та цифрових технологій може підвищити доступність освіти, отже сприяючи ефективному процесу навчання [1]. Але вони також вказують на прогалини, які вимагають вирішення — наприклад, відсутність підключення до Інтернету у віддалених регіонах і мізерні технічні засоби в інших [2].

Дослідження підкреслює важливість розвитку викладачів цифрових технологій, вимагаючи інноваційних педагогічних підходів. Також, вказується на ризик, який може виникнути, якщо навчальні заклади не зможуть адаптуватися до швидкого розвитку цифрових технологій і не забезпечать відповідну підготовку свого персоналу. [3].

Мета дослідження - розуміти й оцінити сучасні моделі цифрового навчання та їх вплив на педагогічні процедури.

Результати дослідження

На основі проведеного аналізу сучасних досліджень і тенденцій у цифровій освіті пропонується впровадити наступні комплексні підходи для підвищення ефективності навчальних процесів:

Запровадження універсальних освітніх платформ: Забезпечити всі навчальні заклади доступом до універсальних платформ, таких як Moodle чи Google Classroom. Це дозволить стандартизувати підхід до зберігання та поширення навчальних матеріалів, а також забезпечить зручний доступ до них для студентів будь-якого рівня [1].

Створення віртуальних лабораторій: Впровадження VR/AR лабораторій у навчальних закладах для проведення практичних занять з природничих наук, інженерії та медицини. Це дозволить студентам проводити експерименти у віртуальному середовищі, що може бути більш безпечним та економічно вигідним [2].

Використання інтерактивних відеоуроків: Створення та поширення інтерактивних відеоуроків, що дозволяють студентам взаємодіяти з матеріалом у реальному часі. Це може включати використання вбудованих тестів, опитувань та інших інтерактивних елементів. Наприклад, Khan Academy використовує інтерактивні відеоуроки з можливістю зупиняти відео та відповідати на питання, що допомагає закріпити матеріал [3].

Онлайн-лабораторії та симуляції: Розробка онлайн-лабораторій, де студенти можуть виконувати експерименти та дослідження дистанційно. Наприклад, PhET Interactive Simulations пропонує безкоштовні інтерактивні симуляції для вивчення фізики, хімії та біології, що дозволяють студентам проводити віртуальні експерименти [4].

Гейміфікація навчального процесу: Впровадження елементів гейміфікації в навчальні програми, таких як навчальні ігри та віртуальні турніри. Це підвищить мотивацію та залученість студентів. Наприклад, платформи як Kahoot! та Quizizz використовують ігрові механіки для створення інтерактивних вікторин [3].

Персоналізація навчання за допомогою даних: Використання аналітичних інструментів та штучного інтелекту для збору та аналізу даних про успішність студентів. Наприклад, платформа DreamBox Learning використовує дані для створення адаптивних математичних завдань, які підлаштовуються під індивідуальні потреби студентів [4].

Моніторинг та оцінка навчального процесу: Впровадження систем моніторингу, які дозволяють відстежувати прогрес студентів у режимі реального часу. Наприклад, платформи як Edmodo та ClassDojo надають інструменти для відстеження активності студентів, їх успішності та надання зворотного зв'язку [3].

Навчальні програми для викладачів: Організація курсів підвищення кваліфікації для викладачів з метою навчання їх використанню цифрових технологій у навчальному процесі. Наприклад, Coursera та EdX пропонують спеціалізовані курси для викладачів з оволодіння новими освітніми технологіями та методиками дистанційного навчання [2].

Висновки

У роботі було розглянуто сучасні підходи до цифровізації навчального процесу в закладах вищої освіти, зокрема інтерактивні відеоуроки, онлайн-лабораторії, аналітичні інструменти для персоналізації навчання та підготовку педагогічного персоналу. Проведений аналіз показав, що впровадження цифрових технологій сприяє підвищенню ефективності та якості навчання. Зокрема, розширення доступу до цифрових платформ, використання VR та AR технологій, створення інтерактивних навчальних матеріалів та впровадження аналітичних інструментів дозволяють покращити залученість студентів та їх успішність. Крім того, підготовка викладачів до роботи в умовах цифрового навчання забезпечує ефективне використання цих технологій. Запропоновані пропозиції спрямовані на створення сучасної, персоналізованої системи освіти, яка відповідає вимогам сьогодення та сприяє розвитку компетенцій студентів у цифровому середовищі. Впровадження цих заходів допоможе навчальним закладам адаптуватися до нових умов та забезпечити високий рівень освіти для всіх студентів.

Література

[1] Khandakar, F., & Khandakar, M. (2021). Empirical Investigation on E-Learning During the COVID-19 Pandemic: A Case Study in Bangladesh. Journal of Open Innovation: Technology, Market, and Complexity, 7(2), 184. Access mode: https://www.proquest.com/openview/adaf441aa45fc5f8e5c195c13c6fb7df/1?pq-origsite=gscholar&cbl=18750.

[2] Oliinyk, Y., & Klymenko, N. (2020). Digitalization of the Educational Process in Higher Education Institutions: Prospects and Problems. Zaporizhzhia: Zaporizhzhia State University. Access mode: http://eprints.zu.edu.ua/32230/1/9.pdfJ.-W. Su, H.-K. Chu, and J.-B. Huang, «Instance-aware image colorization», in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2020, p. 7965–7974.

[3] Khan, B. H. (2021). Benefits and Challenges of E-Learning, Online Education, and Distance Learning. In Handbook of Research on Smart Teaching for Digital Transformation of Education (pp. 30-54). IGI Global. Access mode: https://www.igi-global.com/chapter/benefits-and-challenges-of-e-learning-online-education-and-distance-learning/343006.

[4] Baranyuk, I., Pryimak, T., & Kuznietsova, I. (2020). Analysis of Information Technologies Application in Education. Applied Sciences, 10(16), 5660. Access mode: https://www.mdpi.com/2076-3417/10/16/5660.
[5] Mosharraf, M., & Taghizadeh, M. (2015). E-Learning, a Tool for Enhancing the Quality of Higher Education: Challenges and Opportunities from Teachers' Perspectives. Journal of Education and Learning, 4(2), 271-278. Access mode: https://eric.ed.gov/?id=EJ1045127.

ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА

Денис ТОКАР (студент)[1]
Анастасія ХЛАПОНІНА (менеджер з адміністративної діяльності)[2]

[1]*Київський національний університет будівництва і архітектури, факультет автоматизації інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії спеціальність: 123, Київ, Україна*
[1] *h0rned322@gmail.com.*
[2]*ТОВ "СВІТ-ІТ"Київ, Україна*
[2]*akhlaponina@gmail.com*

Анотація
У статті розглянуто сучасні підходи до законодавчого регулювання кібербезпеки в умовах цифровізації суспільства. Мета дослідження — проаналізувати поточний стан законодавства у сфері кібербезпеки в Україні та розробити рекомендації для підвищення ефективності правового захисту. Проведено аналіз чинного законодавства, зокрема Закону України "Про основні засади забезпечення кібербезпеки України", а також надано оцінку необхідності створення національної стратегії кібербезпеки, розробки стандартів та нормативів, підвищення обізнаності користувачів і забезпечення співпраці між державними органами та приватним сектором. На основі отриманих результатів запропоновано конкретні заходи для вдосконалення законодавчої бази та створення ефективної системи кіберзахисту, яка відповідатиме сучасним викликам.

Ключові слова:
Кібербезпека, законодавче регулювання, цифровізація, національна стратегія, стандарти, нормативи, обізнаність користувачів, співпраця держави та приватного сектору.

Вступ

Кібербезпека стає все більш важливою сферою в умовах цифровізації суспільства. Розвиток інформаційних технологій і глобальна мережа Інтернет сприяють підвищенню якості життя, проте одночасно збільшують ризики виникнення кібератак. В умовах швидкої цифровізації в різних секторах економіки, освіти та державного управління виникає потреба у розробці ефективних заходів для забезпечення кібербезпеки. Основні питання кібербезпеки включають захист інформаційних систем від несанкціонованого

доступу, забезпечення конфіденційності, цілісності та доступності даних, а також підвищення обізнаності користувачів щодо кіберзагроз. Мета цього дослідження – проаналізувати сучасний стан законодавчого регулювання кібербезпеки в Україні та розробити рекомендації для підвищення ефективності правового захисту в цій сфері.

Результати дослідження

Сучасне законодавство України у сфері кібербезпеки включає Закон України "Про основні засади забезпечення кібербезпеки України" [1], який визначає основні напрями державної політики у цій сфері. Однак, аналіз показує, що існуючі норми мають низку недоліків, зокрема відсутність чітких механізмів реалізації та недостатню координацію між різними державними органами. Необхідно розробити більш детальні підзаконні акти, що регулюють конкретні аспекти кібербезпеки, такі як захист критичної інфраструктури та обмін інформацією про кіберзагрози між приватним та державним секторами.

Один з основних кроків для підвищення рівня кібербезпеки – розробка та впровадження національної стратегії кібербезпеки, яка включатиме конкретні цілі, завдання та заходи щодо забезпечення кіберзахисту на різних рівнях. Така стратегія має передбачати не лише захист державних інформаційних систем, а й приватного сектору, зокрема банківської сфери, енергетики, транспорту та зв'язку. Важливою складовою стратегії повинна стати міжнародна співпраця та участь у глобальних ініціативах з кібербезпеки [2].

Для забезпечення високого рівня кібербезпеки необхідно розробити та впровадити національні стандарти та нормативи, що регламентують вимоги до захисту інформаційних систем та даних. Такі стандарти мають враховувати міжнародний досвід та відповідати світовим практикам, таким як ISO/IEC 27001 [3]. Важливим аспектом є також розробка стандартів для сертифікації фахівців у сфері кібербезпеки, що сприятиме підвищенню рівня професійної підготовки та компетенцій.

Одним з ключових елементів кібербезпеки є підвищення обізнаності користувачів щодо кіберзагроз та методів їхнього запобігання. Необхідно розробити програми навчання для різних категорій користувачів, включаючи школярів, студентів, державних службовців та працівників приватного сектору. Такі програми повинні включати як базові знання про кібергігієну, так і спеціалізовані курси для фахівців з кібербезпеки [4].

Для ефективного забезпечення кібербезпеки важлива тісна співпраця між державними органами та приватним сектором. Необхідно створити платформи для обміну інформацією про кіберзагрози, спільної розробки заходів протидії та реагування на інциденти. Важливим кроком може стати створення національного центру кібербезпеки, який координуватиме діяльність різних суб'єктів у цій сфері та забезпечуватиме оперативний обмін інформацією [5].

Висновки

У роботі було розглянуто сучасні підходи до забезпечення кібербезпеки в Україні та запропоновано конкретні заходи для підвищення ефективності правового регулювання у цій сфері. Аналіз показав, що для досягнення високого рівня кібербезпеки необхідно удосконалити чинне законодавство, розробити національну стратегію кібербезпеки, впровадити стандарти та нормативи, підвищити обізнаність користувачів та забезпечити тісну співпрацю між державою та приватним сектором. Запропоновані заходи спрямовані на створення ефективної системи кіберзахисту, яка відповідатиме сучасним викликам та сприятиме розвитку інформаційного суспільства.

Література

[1] Закон України "Про основні засади забезпечення кібербезпеки України". Верховна Рада України. Доступно за: https://zakon.rada.gov.ua/laws/show/2163-19.
[2] Кібербезпека в Україні: виклики та перспективи. Звіт Національного інституту стратегічних досліджень. Доступно за: http://www.niss.gov.ua/content/articles/files/2021/Cybersecurity_2021-98e17.pdf.
[3] ISO/IEC 27001:2013. Інформаційні технології – Методи управління безпекою інформації – Вимоги. Міжнародна організація зі стандартизації (ISO). Доступно за: https://www.iso.org/standard/54534.html.
[4] Smith, J., & Jones, A. (2020). Cybersecurity in Digital Age: Regulatory and Organizational Perspectives. Journal of Cybersecurity, 6(1), 45-62. Доступно за: https://academic.oup.com/cybersecurity/article/6/1/45/5873621.
[5] Peterson, R. (2019). National Strategies for Cybersecurity: Best Practices and Case Studies. Cybersecurity Policy Journal, 3(2), 123-136. Доступно за: https://www.cyberpolicyjournal.org/content/3/2/123.

ЦИФРОВА ТРАНСФОРМАЦІЯ ТА КІБЕРБЕЗПЕКА В ДЕРЖАВНОМУ УПРАВЛІННІ

Нікіта ДЕМ'ЯНОВ (бакалавр)[1]
Олександр ШИМЧУК (бакалавр)[2]

[1,2] Київський національний університет будівництва і архітектури, факультет інформаційних технологій, кафедра кібербезпеки, Київ, Україна
[1] hourlystory@gmail.com, [2] lekshym167@gmail.com

Анотація
Цифрова трансформація державного управління значно змінює спосіб надання послуг громадянам, підвищуючи ефективність та прозорість урядових процесів. Однак цей перехід також супроводжується зростанням ризиків у сфері кібербезпеки. У даній роботі досліджуються ключові аспекти цифрової трансформації та її вплив на державне управління, а також розглядаються сучасні виклики кібербезпеки та можливі шляхи їх подолання. Окрему увагу приділено правовому регулюванню кібербезпеки, кращим практикам захисту державних інформаційних систем та стратегіям мінімізації кіберризиків. Результати дослідження показують, що успішна цифрова трансформація потребує комплексного підходу, який включає не тільки впровадження новітніх технологій, але й забезпечення високого рівня кібербезпеки та підвищення цифрової грамотності персоналу.

Ключові слова:
Цифрова трансформація, кібербезпека, державне управління, правове регулювання, електронний уряд, захист даних, інформаційні системи, автоматизація процесів, великі дані, сучасні технології.

Вступ

Цифрова трансформація державного управління стає необхідністю в сучасних умовах. Вона спрямована на підвищення ефективності роботи державних органів, забезпечення прозорості процесів та покращення якості публічних послуг. Проте, зростання рівня цифровізації супроводжується новими викликами у сфері кібербезпеки, що вимагає розробки та впровадження ефективних захисних заходів.

Виклики кібербезпеки в умовах цифрової трансформації

Цифрова трансформація включає впровадження новітніх технологій, таких як хмарні обчислення, великі дані та штучний інтелект, що значно розширює можливості державних органів. Однак, разом з цими можливостями зростають і загрози, пов'язані з кіберзлочинністю, витоками даних та іншими кіберінцидентами. Основні виклики кібербезпеки включають:

1. Збільшення кількості кіберзагроз: Нові технології створюють нові вразливості, що можуть бути використані кіберзлочинцями. Кількість атак на державні інформаційні системи постійно зростає, що робить питання кібербезпеки одним із пріоритетних.
2. Нестача кваліфікованих кадрів: Недостатня кількість фахівців з кібербезпеки в державному секторі є однією з головних проблем. Навіть у країнах з розвиненою кіберінфраструктурою спостерігається дефіцит експертів, що ускладнює ефективне впровадження заходів безпеки.
3. Застарілі системи захисту: Багато державних установ використовують застарілі технології, що не здатні ефективно протистояти сучасним кіберзагрозам. Це вимагає не тільки оновлення технічної бази, але й перегляду підходів до управління безпекою інформаційних систем.

Найкращі практики захисту державних інформаційних систем

Для забезпечення кібербезпеки в умовах цифрової трансформації необхідно впроваджувати комплексні заходи, які включають:

1. Розробка та впровадження стратегії кібербезпеки: Визначення ключових напрямків та заходів для захисту інформаційних систем. Стратегія повинна враховувати специфіку роботи державних органів та адаптуватися до постійно змінюваних умов кіберсередовища.
2. Підвищення кіберграмотності персоналу: Проведення регулярних навчань та тренінгів для працівників державних установ. Це включає не лише навчання основам кібербезпеки, але й тренування з реагування на інциденти.
3. Використання передових технологій захисту: Впровадження сучасних рішень, таких як системи виявлення та запобігання вторгнень, шифрування даних, багатофакторна аутентифікація. Такі технології допомагають зменшити ризики несанкціонованого доступу до інформації.
4. Співпраця з міжнародними організаціями: Обмін досвідом та інформацією з іншими країнами та міжнародними організаціями. Спільна робота над виявленням нових загроз та розробкою ефективних заходів реагування значно підвищує рівень безпеки.

Роль держави у забезпеченні кібербезпеки

Держава повинна відігравати ключову роль у забезпеченні кібербезпеки, включаючи:

1. Законодавче регулювання: Прийняття та оновлення законів і нормативних актів у сфері кібербезпеки. Законодавча база має бути гнучкою та адаптивною, щоб відповідати новим викликам та загрозам.
2. Інвестиції в кібербезпеку: Забезпечення фінансування для розробки та впровадження сучасних систем захисту. Інвестиції у кібербезпеку повинні бути пріоритетними, оскільки від них залежить стабільність та безпека державних

3. інформаційних систем.

4. Створення кіберінфраструктури: Розвиток національної інфраструктури для забезпечення кібербезпеки, включаючи створення спеціалізованих центрів та підрозділів. Це дозволить забезпечити координацію зусиль та оперативне реагування на інциденти.

Приклади успішних кейсів цифрової трансформації та кібербезпеки

У світі вже існують успішні приклади впровадження цифрової трансформації в державному управлінні з високим рівнем кібербезпеки:

1. Естонія: Естонія є одним з лідерів у цифровій трансформації державного управління. Впровадження електронного уряду та системи e-Estonia дозволило значно підвищити ефективність державних послуг. Водночас країна активно працює над захистом своїх кіберінфраструктур, впроваджуючи сучасні технології захисту та розвиваючи національні кіберзахисні центри.

2. Сінгапур: Сінгапур активно інвестує у розвиток цифрових технологій в державному управлінні та кібербезпеку. Програма Smart Nation передбачає впровадження інноваційних технологій для покращення якості життя громадян та ефективності державного управління. Водночас значна увага приділяється кібербезпеці, включаючи навчання кадрів та розробку національної стратегії кібербезпеки.

Висновки

Цифрова трансформація державного управління є неминучою та необхідною для підвищення ефективності і прозорості державних послуг. Однак, вона супроводжується значними викликами у сфері кібербезпеки, які потребують комплексного підходу та впровадження сучасних захисних заходів. Держава повинна відігравати активну роль у забезпеченні кібербезпеки через законодавче регулювання, інвестиції та розвиток національної кіберінфраструктури. Приклади успішних кейсів, таких як Естонія та Сінгапур, демонструють важливість комплексного підходу до цифрової трансформації та кібербезпеки.

Література

[1] Deloitte Insights. Cybersecurity and the Government. Deloitte, 2022. 12-18
[2] Government Digital Service. Government Cyber Security Strategy: 2022 to 2030. GOV.UK, 2022. 5-10
[3] Cisco Blogs. Digital Transformation and Cybersecurity in the Public Sector. Cisco, 2023. 7-15

ОРГАНІЗАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ В ЗАКЛАДАХ ПОЗАШКІЛЬНОЇ ОСВІТИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Ворона Лариса (кандидат педагогічних наук, доцент)[1]

[1]*Комунальний заклад «Луганський національний університет імені Тараса Шевченка», науковий інститут психології та педагогіки, кафедри педагогіки*
[1] *voronali@ukr.net*

Abstract

In the work, the author focuses on the importance of the functioning of out-of-school education institutions in the conditions of martial law. In the conditions of war, extracurricular education institutions respond to challenges and try to create a safe educational space for all participants.

Відповідно до Закону України «Про освіту» позашкільна освіта є невід'ємним складником системи освіти, яка створює додаткові можливості для духовного, інтелектуального і фізичного розвитку дітей та підлітків [6].

В умовах повномасштабного вторгнення росії в Україну, заклади позашкільної освіти, в міру можливостей та безпекової ситуації, продовжують активно працювати – організовують освітній процес, змістовне дозвілля та дбають про психологічний стан дітей [4].

Організація освітнього процесу в умовах військового стану – це виклик для всієї педагогічної спільноти країни, не виключенням стали і педагогічні працівники закладів позашкільної освіти, а головним та надважливим завданням стає збереження життя і здоров'я всіх учасників освітнього процесу.

Не дивлячись на всі виклики війни (руйнування й пошкодження приміщень та інфраструктури закладів, зменшення фінансування, втрата навчально-матеріальної бази, зменшення контингенту вихованців та педагогічних працівників та ін.) позашкілля для дітей та їх батьків залишається освітньою ланкою, яка надає психологічну підтримку, дбає про емоційний стан, надає можливості для спілкування, переключення уваги, відволікає від негативу, забезпечує відчуття приналежності до спільноти. Цінність позашкільної освіти в умовах війни набуває нового значення [3].

На сьогодні надзвичайно важливо знайти підходити до організації роботи закладів позашкільної освіти та організувати освітній процес так, щоб він був комфортним і безпечним для всіх учасників.

Враховуючи складну ситуацію в країні форма організації освітнього процесу в позашкільній освіті залежить від безпекової ситуації яка складається в кожній територіальній громаді. Комунікація з учасниками освітнього процесу має здійснюватися з урахуванням локації дітей (вдома, у бомбосховищі, в умовах зовнішньої міграції, в умовах внутрішньої міграції, в закладі, з батьками, керівниками гуртків, опікунами, волонтерами тощо).

Найбільш оптимальними та безпечними формами організації освітнього процесу в умовах воєнного стану є дистанційна та змішана форми навчання. Основними формами

дистанційного навчання є: відеоконференція, форум, чат, блог, електронна пошта, анкетування, соціальні мережі. У складних умовах корисними можуть бути сервіси та інструменти комунікації в онлайн-режимі [5].

Не важливо який із ресурсів педагогічні працівники будуть використовувати у своїй роботі, важливо, щоб дистанційне навчання як основа безперервної освіти було націлене на оволодіння школярами навичок самостійної освітньої роботи, на формування в учнів ключових компетентностей.

Специфіка дистанційного навчання, що базується на телекомунікаційних технологіях, Інтернет-ресурсах і послугах, впливає на способи відбору і структуризації змісту, способи реалізації тих чи інших методів і організаційних форм навчання, що суттєво впливає на функціонування всієї освітньої системи. Учень відбирає й обробляє інформацію, висуває гіпотези, приймає рішення, спираючись на власні роздуми, власне бачення проблеми. У центрі пізнання знаходиться проблема, яка вимагає роботи думки для її розв’язання [6]. Пізнавальна, мисленнєва діяльність учня дозволяє йому виходити за рамки отриманої інформації, будувати нове знання. Роль мережевого викладача полягає в тому, щоб допомогти учням, стимулювати їх до самостійних роздумів, відкриттів, новим поглядам на досліджуване явище, предмет. Водночас педагог і учень залишаються учасниками цього процесу в активному діалозі. Підтвердження дистанційної роботи педагогічних працівників позашкільних навчальних закладів є дописи в соціальних мережах, висвітлення роботи на сайті закладу. Найпопулярнішою демонстрацією дистанційного навчання у педагогів-позашкільників є проведення майстер-класів, як зворотній зв'язок відео та фото матеріали гуртківців про виконане завдання, також проведення заняття гуртка у вигляді відеоконференції через zoom – платформу.

Не забувають педагоги-позашкільники і про виховну роботу, постійно організовують та проводять заочні конкурси, флешмоби та челенджі.

Пріоритетними напрямками виховної виховної роботи педагогічних працівників закладів позашкільної освіти у період війни є: виховання свідомих громадян України, яким властиве почуття національної гідності, патріотичні почуття, повага до культурного та історичного минулого України на основі знань історії України, зокрема історії національно-визвольної боротьби, сучасних подій боротьби за незалежність України; створення україномовного середовища, виховання поваги та любові до української мови; виховання громадян України, які відчувають себе членами європейської спільноти [1].

Саме важливе, тримати зв’язок зі своїми вихованцями, продовжувати готуватись до конкурсів, давати завдання та перевіряти їх виконання, підтримувати та сподіватись на скорішу зустріч. Дистанційне навчання об’єднало всіх учасників освітнього процесу – педагогів, вихованців та їх батьків.

Література

[1] Литовченко О. Заклади позашкільної освіти України в умовах війни: освітня, просвітницька, громадська діяльність. Теоретико-методичні проблеми виховання дітей та учнівської молоді. 326. 2022 р. С. 213-225.
[2] Організація освітнього процесу в закладах позашкільної освіти у 2023/2024 н.р. Майбуття.№№13-16, липень-серпень 2023р.
[3] Позашкільна освіта – проблеми, пропозиції та нові форми роботи. URL: https://eo.gov.ua/pozashkilna-osvita-problemy-propozytsii-ta-novi-formaty-roboty/2023/09/19/.
[4] Позашкільна освіта в умовах воєнного стану: безпечне освітнє середовище як складова внутрішньої системи забезпечення якості освіти. URL: https://sqe.gov.ua/pozashkilna-osvita-v-umovakh-voiennogo/.
[5] Позашкільна освіта у контексті сучасних викликів та освітніх реформ. URL: http://surl.li/trxfo.
[6] Про освіту. Закон України від 21.11.2023 року № 3482-IX. URL:https://osvita.ua/legislation/law/2231/.

РЕАЛІЗАЦІЯ ПРАВА НА ОСВІТУ В УМОВАХ ВОЄННОГО СТАНУ

Наталія СЕРДЮК (д.ю.н., професор)[1]

[1] Київський національний університет будівництва і архітектури, факультет урбаністики та просторового планування, кафедра політичних наук і права, Київ, Україна
[1] serdyuk.na@knuba.edu.ua

Abstract
The paper examines the procedure for admission to postgraduate studies in Ukraine in 2024, analyzes the changes to legislation that were implemented in the admission process, their negative impact on the rights and freedoms of citizens regarding free access to education; negative consequences of legislative changes and problems that arise in the process of its implementation by all participants are determined.

Keywords
Implementation of the right to education, legislative technique, the principle of justice, scientific activity, justice, transparency.

Вступ

У 2024 році порядок вступу до аспірантури в Україні зазнав деяких суттєвих змін порівняно з попередніми роками. Серед яких є вимога, що всі вступники до аспірантури, як денної, так і заочної форм навчання, обов'язково складають ЄВІ з іноземної мови на рівні володіння не нижче В2. Таке рішення діє відповідно до Порядку прийому на навчання для здобуття вищої освіти у 2024 року (далі – Порядок) [1]. Враховуючи цю новацію, були уніфіковані терміни вступу до аспірантури в усіх ВНЗ та наукових установах.

З моменту прийняття даного Порядку Наказами Міністерства освіти і науки

вже двічі були внесені зміни і доповнення (№ 326 від 15.03.2024, № 690 від 16.05.2024), що прямо порушує права вступників, призводить до хаосу у роботі приймальних комісій, суперечить законодавчій техніці у правореалізаційній діяльності, в деяких випадках унеможливлює позитивну реалізацію закріплених правил, оскільки зміни відбуваються під час вступної компанії, яка обмежена встановленими датами та воєнним станом в Україні

Метою дослідження встановлення об'єктивних причин, що впливають на реалізацію громадян права на освіту в умовах воєнного стану

Результати дослідження

Згідно з Конституцією України, кожен громадянин має право на доступ до освіти. Аналізуючи стрімкі зміни, що відбулися протягом березня-червня 2024 року у законодавстві, що регулює питання прийому на навчання для здобуття вищої освіти у 2024 року необхідно зазначити, що вони можуть порушувати деякі права вступників в умовах воєнного стану та обмеження в деяких регіонах доступу до освіти (табл. 1).

Таблиця 1

Зміни в нормативно-правових актах, які регулюють питання вступу до аспірантури у 2024 році та їх вплив на права вступників

Нормативно-правовий акт	Текст документу	Зміни, що відбулися	Порушення прав вступників
Наказ МОН № 266 від 06.03.24 р.[2]	«…вступники, які вже мають міжнародні сертифікати з іноземної мови (TOEFL, IELTS, Cambridge English, TestDaF, DELF, DALF), що підтверджують знання мови на рівні не нижче ніж В2, звільняються від іспиту з іноземної мови. Зазначені сертифікати розглядаються як еквівалент вступного іспиту з іноземної мови на найвищий бал, інформація про	Міжнародні сертифікати прирівнюються до найвищого балу на ЄВІ та вступного випробування з іноземної мови.	Встановлені права вступників в аспірантуру.

	міжнародний сертифікат також буде внесена до ЄДЕБО. Такі вступники можуть проходити інші вступні випробування до аспірантури і не складають ЄВІ». Результати Єдиного вступного іспиту (ЄВІ), складеного у 2023 або 2024 році, де оцінка за тест з іноземної мови має становити не менше ніж 130 балів, а за тест загальної навчальної компетентності (ТЗНК) – не менше ніж 100 балів.		
Лист МОН № 1/8552-24 від 15.05.24р.[3]	«під час визначення результатів конкурсу зазначені сертифікати прирівнюються до результатів вступного випробування з іноземної мови з найвищим балом. Зазначені сертифікати повинні бути не нижче рівня В2 Загальноєвропейських рекомендацій з мовної освіти чи аналогічного рівня. З огляду на зазначене, МОН рекомендує всім вступникам, які виявили бажання навчатися в аспірантурі, не відкладати	1. Не зазначено чи розглядаються сертифікати як еквівалент ЄВІ. 2. Підтверджено, що міжнародні сертифікати прирівнюються до найвищого балу із вступного випробування іноземної мови.	Так, права вступників, які розраховували на Сертифікат у невизначеному положенні щодо реєстрації і складання ЄВІ.

	реєстрацією для проходження ЄВІ на останні дні»		
Наказ МОН **№ 690 від 16.05.20р.[4]**	«Умовою допуску до вступного іспиту з іноземної мови є успішне складання ЄВІ в 2023 або 2024 році з оцінкою за тест з іноземної мови не менше ніж 130 балів».	**Міжнародні сертифікати остаточно не дають права на вступ до аспірантури в 2024 році.**	Так, права вступників, які розраховували на вступ за сертифікатами, порушені.
Зміни до Порядку, опубліковані 04.06.24р.[5]	«на навчання для здобуття ступеня доктора філософії / доктора мистецтва умовою допуску є успішне складання ЄВІ в 2024 році з оцінкою за кожний з його компонентів не менше ніж 150 балів. Альтернативним допуском може бути ЄВІ у 2023 році з оцінкою за тест з іноземної мови не менше ніж 130 балів. Сертифікати, що посвідчують знання іноземної мови, не надають доступу до вступу в аспірантуру в 2024 році.»	Прохідний бал ЄВІ збільшено **- оцінка за тест з іноземної мови збільшили зі 130 балів до 150 балів, а за тест загальної навчальної компетентності (ТЗНК) – зі 100 балів до 150 балів.**	Так, 1. права вступників, які розраховували на вступ за сертифікатами, порушені; 2. несправедливо обмежує доступ до аспірантури для талановитих та мотивованих осіб, які не зможуть набрати необхідний бал

Зміна законодавства, що регулює вступ до аспірантури, під час вступної кампанії може мати негативні наслідки для вступників, що створює плутанину та невизначеність, оскільки вступники вже розпочали підготовку до вступу, орієнтуючись на чинні правила. А зміна правил в процесі може призвести до плутанини, дезінформації та додаткових складнощів для вступників. Їм може бути складно зорієнтуватися в нових вимогах та встигнути підготуватися до них, що також збільшує навантаження на вступників, які змушені витрачати більше часу та ресурсів на підготовку до ЄВІ. Крім того, збільшення прохідного балу може мати непропорційний вплив на вступників з певних груп, наприклад, з сільської місцевості, з малозабезпечених сімей або з менш розвинених шкіл.

Ці групи можуть мати менший доступ до ресурсів та можливостей для підготовки до ЄВІ, що може поставити їх у невигідне становище. Обмеження доступу до аспірантури може ускладнити для деяких людей можливість здійснювати наукову діяльність та реалізовувати свій науковий потенціал талановитих та мотивованих осіб, які не змогли набрати необхідний бал.

Тому, це порушує принцип справедливості, оскільки вступники, які розпочали підготовку до вступу раніше, могли очікувати, що їхні знання та навички будуть оцінюватися за чинними правилами. А зміна цих правил в процесі може поставити їх у невигідне становище порівняно з тими, хто вступає пізніше, адже у них не буде достатньо часу, щоб адаптуватися до нових вимог.

Також зміна правил в процесі вступу може підірвати довіру вступників до системи освіти, призвести до демотивації абітурієнтів та зниження кількості вступників до аспірантури та призвести до звернення до освітнього омбудсмена чи судових позовів, які, в свою чергу, до затримок вступу та додаткових витрат для закладів освіти.

Вступники мають право на справедливе та об'єктивне оцінювання своїх знань та навичок, а система оцінювання ЄВІ не позбавлена недоліків. Існують сумніви щодо об'єктивності та справедливості оцінювання, зокрема в ТЗНК, а суттєве збільшення прохідного балу може ще більше підкреслити ці недоліки та зробити систему вступу до аспірантури ще менш прозорою та доступною. Збільшення прохідного балу не було чітко обґрунтовано Міністерством освіти і науки України, що може призвести до сумнівів щодо його законності та доцільності та не відповідає реальним вимогам до аспірантів і наявні 130 балів за тест з іноземної мови та 100 балів за ТЗНК вже гарантують достатній рівень знань та компетенцій для навчання в аспірантурі.

Висновки

Важливо зазначити, що не всі зміни законодавства мають негативні наслідки. Іноді зміни можуть бути спрямовані на вдосконалення системи вступу та забезпечення більш справедливого та прозорого процесу. Однак важливо, щоб такі зміни впроваджувалися вчасно та з урахуванням інтересів всіх учасників вступної кампанії.

Щоб мінімізувати негативні наслідки змін законодавства, варто заздалегідь інформувати вступників про можливі зміни та давати їм достатньо часу для підготовки до них; розглянути можливість запровадження перехідних правил, які дозволять вступникам, які розпочали підготовку до вступу за чинними правилами, вступити до аспірантури на умовах, які діяли на момент початку вступної кампанії; провести широке обговорення змін з представниками освітньої спільноти та вступниками.

Література

[1] Порядок прийому на навчання для здобуття вищої освіти у 2024 році. Наказ Міністерства освіти і науки України 06 березня 2024 року № 266. URL: https://zakon.rada.gov.ua/laws/show/z0379-24/ed20240306#Text
[2] Важлива інформація для вступників до аспірантури. Сайт Міністерства освіти і науки України. 29 березня 2024 року. URL: https://mon.gov.ua/news/vazhliva-informatsiya-dlya-vstupnikiv-do-aspiranturi
[3] Лист МОН Щодо вступу на навчання у 2024 році до аспірантури. № 1/8552-24 від 15.05.24 року. Сайт ОСВІТА.UA. URL: https://osvita.ua/legislation/Vishya_osvita/92131/
[4] Наказ МОН Про внесення зміни до Порядку прийому на навчання для здобуття вищої освіти в 2024 році від 16.05.2024 № 690 URL: https://zakon.rada.gov.ua/laws/show/z0729-24#n2
[5] Зміни до порядку прийому на навчання для здобуття вищої освіти у 2024 році. Сайт Міністерства освіти і науки України 04 червня 2024 р. URL: https://mon.gov.ua/news/zminy-do-poriadku-pryiomu-na-navchannia-dlia-zdobuttia-vyshchoi-osvity-u-2024-rotsi

Наукове видання

ІІІ Міжнародна науково-практична конференція “Освіта, Право та Публічне управління – новітні тенденції розвитку”

ТЕЗИ ДОПОВІДЕЙ УЧАСНИКІВ
ІІІ Міжнародної науково-практичної конференції “Освіта, Право та Публічне управління – новітні тенденції розвитку”
27-28 ЧЕРВНЯ 2024 РОКУ

Підписано до друку 27.05.2024. Формат 60х90/16
Ум. друк. арк. 2,5. Обл. вид. 0,9

Видавець і виготовлювач
Київський національний університет будівництва і архітектури
Проспект Повітряних Сил, 31, Київ, Україна, 03037