ПрАТ «ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

Кваліфікаційна наукова праця
на правах рукопису

ПОЛІЩУК ВОЛОДИМИР ПАВЛОВИЧ

УДК 342.95(477)

ДИСЕРТАЦІЯ
АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ ТА ПОВОЄННОЇ ВІДБУДОВИ УКРАЇНИ

081 – Право

Подається на здобуття ступеня доктора філософії за спеціальністю 081 – Право.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Поліщук В. П.

Науковий керівник:
Денега Олег Петрович
доктор юридичних наук, професор

Київ – 2025

АНОТАЦІЯ

Поліщук В. П. Адміністративно-правові засади забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 Право. – ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом». – Київ, 2025.

Дисертацію присвячено науковому аналізу адміністративно-правового регулювання забезпечення кібербезпеки в Україні в контексті умов воєнного стану та перспективи повоєнної відбудови. Визначено позитивні та негативні аспекти сучасного стану адміністративно-правового забезпечення кібербезпеки. Одержані в процесі дослідження наукові результати дають підстави для висновків, які мають як теоретичне, так і практичне значення.

Розглянуто концептуальні основи формування та розвитку правового регулювання кібербезпеки і конфіденційності в Інтернеті.

В Україні триває процес правового забезпечення кібербезпеки та конфіденційності в Інтернеті. Україна ратифікувала низку міжнародних документів з цього питання та має власну законодавчу базу.

Досліджено визначення правового статусу кібератак та кібервійськових операцій крізь призму міжнародного права та забезпечення глобальної кібербезпеки. До основних характерних ознак кіберконфліктів, які відмежовують їх від інших загроз національної безпеки віднесено: просторові межі, можливість глобального розвитку в найкоротші терміни, відсутність суб’єктної прив’язки до конкретних дій в кіберпросторі.

Акцентовано увагу на тому, що трансформація конфліктної активності в кіберпростір провокує швидку глобалізацію конфронтації з можливістю залуження міжнародних акторів, які мають вплив на міжнародні процеси.

Враховуючи специфіку кіберпростору, зроблено висновок, що кібератака потенційно може спровокувати міжнародний конфлікт, в тому числі в просторі територіально визначеному, оскільки:

а) в умовах глобальної взаємодії інформаційних інфраструктур окремих країн украй важко розрахувати межі й наслідки такої атаки;

б) деякі заходи, що вживаються постраждалою стороною, можуть бути непропорційними через складність ідентифікації джерела або можливість помилок у судженнях.

Встановлено, що в інформаційному суспільстві сформовано уявлення про кіберконфлікт як спосіб впливу на масову свідомість, за допомогою спотворення реальності щодо наслідків конфронтації сторін. Результатом кіберконфлікту можуть бути політичні рішення глобального значення, які мають вагомий вплив на процес прийняття найважливіших політичних рішень. Політична еліта використовує результати конфронтації, як площину для легітимації персональних рішень та реалізації цілей геополітичного рівня.

Зазначено, що трансформація у військових атак у кібервійськові є проявом осучаснення ведення військових дій та реалізації глобалізаційних змін. Тому, кібервійськові атаки стають невід'ємною формою існування демократичного устрою, у зв'язку з цим, виникає потреба у формуванні системи реагування органами управління, на небезпеку, яку вони можуть нести суспільству. Проаналізовано досвід Сполучених Штатів Америки та Китайської Народної Республіки щодо впорядкування відносин з приводу забезпечення кібербезпеки.

Досліджено різні типи кіберзлочинів та їхні особливості, а також методи та інструменти, які використовуються кіберзлочинцями, а також заходи, які можна вжити для захисту від кіберзлочинів; роль правоохоронних органів та міжнародної співпраці у боротьбі з кіберзлочинністю. Автор розглядає актуальні тенденції та прогнози розвитку кіберзлочинності в Україні та міжнародний досвід боротьби з кіберзлочинами.

У роботі зроблена спроба ознайомитися з розвитком нових форм вчинення кіберзлочинів у контексті історичного розвитку.

Кіберзлочини часто складні для розслідування через брак кваліфікованих кадрів, необхідних інструментів та міжнародної співпраці. Кіберзлочинці часто ховаються за анонімністю, що ускладнює їх ідентифікацію та притягнення до відповідальності. Законодавство у сфері кіберзлочинності постійно еволюціонує, адже не завжди встигає за темпами розвитку нових технологій. Зазначається, що кіберзлочинність є серйозною загрозою для суспільства, тому необхідні спільні зусилля держави, приватного сектору та громадян для її подолання.

Боротьба з кіберзлочинністю та забезпечення кібербезпеки – одна з найактуальніших проблем сьогодення. Показано, що це питання, яке потребує комплексного підходу, що містить як правові, так і технічні аспекти.

Визначено поняття «кібербезпека», «кіберзахист», «кібератака», «кібервійськова операція», «кіберзлочинність» та «злочинність у сфері комп'ютерної інформації».

Узагальнено і проаналізовано методи та інструменти кіберзахисту.

Розроблено рекомендації щодо розвитку кібербезпеки.

Результати дослідження можуть бути використані для розробки та вдосконалення політики кібербезпеки на державному та приватному рівні.

Доведено, що розслідування кібератак як воєнних злочинів може допомогти притягнути винних до відповідальності, а також запобігти подібним злочинам у майбутньому.

Виконано комплексний аналіз поточного стану кіберзлочинності та її впливу на національну безпеку. Основна увага зосереджена на виявленні ключових загроз у цифровому просторі та розробці стратегій їх запобігання та протидії з метою забезпечення безпеки держави. Проаналізовано динаміку та еволюцію кіберзлочинності, оцінено її вплив на різні аспекти національної безпеки, включаючи інформаційну, економічну та військову сфери, а також розробку стратегій і методів протидії державним і приватним структурам кіберзагрозам.

Показано, що кіберзлочинність постійно розвивається, що пов'язано з появою нових IT-технологій та збільшенням кількості користувачів, залучених

до інформаційних процесів. Визначено основні категорії злочинів: незаконне завантаження або використання програмного забезпечення, шахрайство та атаки з використанням вразливостей систем.

Відзначається необхідність об’єднання зусиль різних суб’єктів у кібербезпеці з особливим наголосом на ролі держави. У науковій роботі підкреслюється, що кібербезпека в державному управлінні досягається шляхом уніфікації методів обміну даними, використовуючи транспортні протоколи, такі як HTTP.

Зазначено, що вивчення інформаційного протистояння потребує детального аналізу основних сфер кіберзахисту, включаючи стратегії протидії системам державного управління, інформаційній та розвідувальній діяльності, радіоелектронній боротьбі, психологічному протистоянню, хакерським операціям, кібер- та мережевим війнам, економічній інформаційній війні та міжнародній інформації. тероризм. У науковій роботі підкреслюється, що міжнародний інформаційний тероризм в епоху інформаційного протистояння набуває нового значення, зокрема, через використання терористами інформаційної структури для формування мережевих методів та впливу на об’єкти інформаційної інфраструктури.

Питання впливу кібербезпеки є першочерговим для функціонування фінансової установи. Тому її забезпечення стає пріоритетним в організації подальшої діяльності самого закладу. В дисертації виконано аналіз сучасних тенденцій забезпечення кібербезпеки фінансових установ та її ролі в їх функціонуванні.

Описано теоретичні основи концепції кіберзахисту. Окреслено специфіку кібербезпеки та провідні технологічні рішення для досягнення цих цілей. Особлива увага приділяється сучасним, інноваційним рішенням для підтримки стабільності фінансових установ та можливості подальшого розвитку.

Важливим напрямом досліджень є розкриття практичного досвіду інформаційних корпорацій щодо надання технічних рішень для забезпечення безпеки фінансових операцій та підтримки світової фінансової системи. У

дослідженні представлено досвід українських фінансових установ, які використовують змінні стратегії цифрового захисту та підтримують свою функціональність на основі ефективної системи кібербезпеки в умовах глобального військового конфлікту.

Запропоновано систему сучасних програмних, апаратних та управлінських рішень для підвищення якості кібербезпеки в умовах зростання кібератак і цифрових загроз стабільності фінансових установ. Результати дослідження можуть бути корисними для подальших аналітичних досліджень ефективності кібербезпеки та стабільності фінансових установ.

Сформульовано наступні основні проблеми та актуальні виклики сьогодення в сфері забезпечення кібербезпеки та кіберзахисту, протидії кіберзагрозам, таким як кібератаки та кіберзлочинність, в умовах воєнного стану та повоєнної відбудови України:

недостатній рівень кіберзахисту критичної інфраструктури;

недостатнє фінансування кібербезпеки;

дефіцит кваліфікованих спеціалістів;

високий рівень кіберзагроз;

низький рівень обізнаності громадян;

слабка координація між органами влади;

відсутність кіберстрахування;

низька кіберкультура в бізнесі;

відсутність стандартів кібербезпеки для блокчейн-технологій;

недостатній рівень міжнародної співпраці.

Запропоновано шляхи вирішення зазначених проблем у сфері кібербезпеки України, створення сучасної ефективної системи забезпечення кібербезпеки та кіберзахисту, що на даний час є вкрай актуальним питанням для нашої держави, шляхом вдосконалення нормативно-правового регулювання адміністративно-правових засад забезпечення кібербезпеки. Зокрема, розроблено законопроєкт, яким запропоновано системне та комплексне вдосконалення забезпечення кібербезпеки України.

Ключові слова: кіберзагрози, кібербезпека, кібербулінг, мережевий етикет, приватність, віртуальний простір, правове регулювання, Інтернет, кібератака, кібервійськова операція, глобалізація, конфронтація, міжнародне право, кіберзлочинність, комп'ютерні злочини, шахрайство, крадіжка особистих даних, шпигунство, критична інфраструктура, захист інформації, міжнародна співпраця, цифровий захист.

SUMMARY

Polishchuk V. P. Administrative and legal principles of ensuring cyber security in the conditions of martial law and post-war reconstruction of Ukraine. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the Doctor of Philosophy degree in specialty 081 − Law. – PrJSC «Higher educational institution «Interregional Academy of Personnel Management». – Kyiv, 2025.

The dissertation is devoted to the scientific analysis of the administrative and legal regulation of cyber security in Ukraine in the context of martial law conditions and the perspective of post-war reconstruction. The positive and negative aspects of the current state of administrative and legal support for cybersecurity are identified. The scientific results obtained in the research process provide grounds for conclusions that have both theoretical and practical significance.

The dissertation focuses on the conceptual framework for the formation and development of legal regulation of cybersecurity and privacy on the Internet.

In Ukraine, the process of legal support for cybersecurity and privacy on the Internet is ongoing. Ukraine has both ratified several international documents related to this issue and has its own legislative framework.

Investigated to determining the legal status of cyber attacks and cyber military operations through the prism of international law and ensuring global cyber security.

The main characteristic features of cyber conflicts, which distinguish them from other threats to national security, include: spatial boundaries, the possibility of global development in the shortest possible time, the lack of subject attachment to specific actions in cyberspace.

Attention is focused on the fact that the transformation of conflict activity into cyberspace provokes a rapid globalization of confrontation with the possibility of involving international actors who have an influence on international processes.

Taking into account the specifics of cyberspace, it is concluded that a cyberattack can potentially provoke an international conflict, including in a territorially defined space, because:

a) in the conditions of global interaction of the information infrastructures of individual countries, it is extremely difficult to calculate the limits and consequences of such an attack;

b) individual measures of the affected party may be disproportionate due to the difficulty of determining the source and the probability of an erroneous assessment of the situation.

It has been established that the information society has formed an idea of cyber conflict as a way of influencing the mass consciousness by distorting reality regarding the consequences of the confrontation between the parties. The result of a cyber conflict can be political decisions of global importance, which have a significant impact on the process of making the most important political decisions. The political elite uses the results of the confrontation as a platform for legitimizing personal decisions and realizing goals at the geopolitical level.

It is noted that the transformation from military attacks to cyber attacks is a manifestation of the modernization of military operations and the implementation of globalization changes. Therefore, cyber military attacks become an integral form of the existence of a democratic system, in connection with this, there is a need for the formation of a system of response by management bodies to the danger that they can bring to society. The experience of the United States of America and the People's Republic of China in regulating relations regarding the provision of cyber security is

analysed.

The dissertation examines the different types of cybercrimes and their characteristics, as well as the methods and tools used by cybercriminals, as well as measures that can be taken to protect against cybercrimes; the role of law enforcement agencies and international cooperation in the fight against cybercrime. The author examines current trends and forecasts of the development of cybercrime in Ukraine and international experience in combating cybercrime.

The work attempts to familiarize with the development of new forms of committing cybercrimes in the context of historical development.

Cybercrimes are often difficult to investigate due to a lack of skilled personnel, necessary tools and international cooperation. Cybercriminals often hide behind anonymity, making it difficult to identify and prosecute them. Legislation in the field of cybercrime is constantly evolving, because it does not always keep up with the pace of development of new technologies. It is important to note that cybercrime is a serious threat to society, therefore joint efforts of the state, private sector and citizens are necessary to overcome it.

Fighting cybercrime and ensuring cyber security is one of the most urgent problems today. This is an issue that requires a comprehensive approach that includes both legal and technical aspects.

The concepts of «cybersecurity», «cyberdefense», «cyberattack», «cybermilitary operation», «cybercrime» and «crime in the field of computer information» are defined.

Cybersecurity methods and tools are summarized and analysed.

Recommendations for the development of cybersecurity are developed.

Research results can be used to develop and improve cyber security policy at the state and private level.

It has been proven that the investigating cyber-attacks as war crimes can help bring perpetrators to justice and prevent similar crimes in the future.

The present research is a comprehensive analysis of the current state of cybercrime and its impact on national security. The focus is on identifying key threats

in the digital space and developing strategies to prevent and counteract them in order to ensure state security. The dynamics and evolution of cybercrime were analysed, its impact on various aspects of national security was assessed, including the information, economic and military spheres, as well as the development of strategies and methods for countering cyber threats to state and private structures.

The research has shown that cybercrime is constantly evolving, which is related to the emergence of new IT technologies and an increase in the number of users involved in information processes. The major categories of crimes are identified: illegal downloading or use of software, fraud and attacks exploiting vulnerabilities of systems.

The necessity of joint efforts of various subjects in cybersecurity is also noted with a special emphasis on the role of the state. The dissertation emphasizes that cybersecurity in public governance is achieved through the unification of data exchange methods, using transport protocols such as HTTP.

The study of information confrontation requires a detailed analysis of the main areas of cyber defence, including strategies for countering public governance systems, information and intelligence activities, electronic warfare, psychological confrontation, hacker operations, cyber and network warfare, economic information warfare and international information terrorism. The dissertation emphasizes that international information terrorism in the era of information confrontation is gaining new importance, in particular, due to the use of the information structure by terrorists to form network methods and influence information infrastructure facilities.

The issue of the impact of cybersecurity is a top priority for the functioning of a financial institution. Therefore, its provision becomes a priority in organizing the further activities of the institution itself. The dissertation aims to analyse the current trends in ensuring the cybersecurity of financial

institutions and its role in their functioning. The dissertation describes the theoretical foundations of the cyber protection concept. The author also outline the specifics of cybersecurity and the leading technological solutions for achieving these goals. Special attention is paid to modern, innovative solutions to maintain the stability of financial institutions and the possibility of further development.

An important area of research is the disclosure of the practical experience of information corporations in providing technical solutions to ensure the security of financial transactions and support the global financial system. The study presents the experience of Ukrainian financial institutions that use variable digital defence strategies and maintain their functionality based on an effective cybersecurity system in the context of a global military conflict.

A system of modern software, hardware and management solutions is proposed to improve the quality of cybersecurity in the face of increasing cyberattacks and digital threats to the stability of financial institutions. The research findings may be helpful for further analytical studies on the effectiveness of cybersecurity and the stability of financial institutions.

The following main problems and current challenges of today in the field of ensuring cybersecurity and cyber defence, countering cyber threats, such as cyber attacks and cyber crime, in the conditions of martial law and post-war reconstruction of Ukraine have been formulated:

insufficient level of cyber protection of critical infrastructure;

insufficient funding for cybersecurity;

shortage of qualified specialists;

high level of cyber threats;

low level of citizen awareness;

weak coordination between authorities;

lack of cyber insurance;

low cyber culture in business;

lack of cybersecurity standards for blockchain technologies;

insufficient level of international cooperation.

Ways have been proposed to solve the above-mentioned problems in the field of cybersecurity of Ukraine, to create a modern effective system of ensuring cybersecurity and cyber protection, which is currently an extremely urgent issue for our state, by improving the regulatory and legal regulation of the administrative and legal principles of ensuring cybersecurity. In particular, a draft law has been developed, which

proposes a systematic and comprehensive improvement of ensuring cybersecurity in Ukraine.

Key words: cyber threats, cybersecurity, cyberbullying, netiquette, privacy, virtual space, legal regulation, Internet, cyber attack, cyber military operation, globalization, confrontation, international law, cyber-crime, computer crimes, fraud, identity theft, espionage, critical infrastructure, information protection, international cooperation, digital protection.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

А. Статті в наукових виданнях України, включених до переліку наукових фахових видань України

1. В. Поліщук. Кіберзлочини та кібербезпека: боротьба з комп'ютерними злочинами і кібератаками. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2023. № 3(66). С. 44 – 47. DOI: https://doi.org/10.32689/2522-4603.2023.3.7.

2. **Поліщук В. П.**, Панасевич Л. А. Міжнародне право і кібербезпека: визначення правового статусу кібератак та кібервійськових операцій. *Юридичний науковий електронний журнал*. 2024. № 2. С. 503 – 506. DOI: https://doi.org/10.32782/2524-0374/2024-2/124.

Б. Статті в періодичних наукових виданнях, проіндексованих у наукометричній базі даних Scopus

3. **V. Polishchuk**, V. Yurakh, O. Kravchenko, W. Warawa, I. Kulchii. Legal Regulation of Cybersecurity and Privacy on the Internet as SDG's. *Journal of Lifestyle*

and SDGs Review. 2024. v. 4, n. 1. С. 01 – 22. DOI: https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01666.

4. V. Ievdokymov, A. Frikel, **V. Polishchuk**, S. Savchuk, I. Klimova. Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention. *Economic Affairs*. 2024. Vol. 69, Issue 1 Special. pp. 61 – 69. DOI: https://doi.org/10.46852/0424-2513.1.2024.8.

5. **V. Polishchuk**, N. Fedirko, D. Grytsyshen, K. Ohdanskyi, V. Kotkovskyy. Stability of financial institutions under the influence of cyber threats. *Edelweiss Applied Science and Technology*. 2024. v. 8, n. 6. С. 2501 – 2509. DOI: https://doi.org/10.55214/25768484.v8i6.2498.

Праці, які додатково відображають наукові результати дисертації (Матеріали наукових конференцій)

6. В. П. Поліщук. Визначення правового статусу кібератак та кібервійськових операцій. *Проблеми модернізації України. Випуск 17. Матеріали IX Міжнародної науково-практичної конференції «Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності»*. (м. Київ, 23-24 травня 2024 р.). Київ, 2024. С. 373 – 375. URL: https://research.maup.com.ua/assets/files/conferency/17-problemi-modernizacii.pdf.

7. Поліщук В. Права людини в умовах кіберпростору: баланси між безпекою та приватністю. *Міжнародна науково-практична конференція «Інновації та їхній вплив на економіку та суспільство».* (м. Суми, 25 жовтня 2024 р.). Суми, 2024. С. 136 – 138. URL: https://researcheurope.org/wp-content/uploads/2024/11/re-25.10.24.pdf.

ЗМІСТ

ВСТУП

Актуальність теми. Технологічний розвиток надав людству багато очевидних переваг. Однак це також створило серйозні виклики та загрози національній безпеці, критичній інфраструктурі, приватним особам і державам, а також міжнародній спільноті. В Україні ці питання загострилися російсько-українською війною.

В Україні також триває процес правового урегулювання питань, пов'язаних з кібербезпекою та захисту персональних даних в Інтернеті.

Станом на теперішній час, значно зросла кількість кібератак як в Україні, так і в інших країнах. Розвиток впорядкування суспільних відносин у напрямку цифровізації є притаманним для багатьох розвинутих країн світу. Однак, для українського суспільства процес нормативної та інституціональної форм трансформації триває в умовах російсько-української війни, яка однозначно встановила єдиний напрямок суспільних інтересів та консолідацію українського суспільства.

Сучасний розвиток цифрових технологій, електронної комерції та автоматизації діяльності як державних органів і установ, так і приватних підприємств пропонує низку переваг для ефективного управління та зручності користувачів у отриманні їх послуг. Проте забезпечення кібербезпеки залишається актуальною проблемою, оскільки цифрове середовище залишається вразливим у сучасному технологічному світі.

За останнє десятиліття зросла кількість зловмисних атак на органи державної влади, об'єкти критичної інфраструктури, фінансові установи тощо. Тому завдання пошуку ефективних технологічних рішень і адміністративно-правових засад забезпечення кібербезпеки є вирішальними для їх подальшого розвитку.

Війна в Україні викликала глобальну конкуренцію між різними державами щодо посилення кібербезпеки та розробки ефективних методів і моделей управління.

Для створення комплексного уявлення про забезпечення кібербезпеки, заслуговують на увагу й праці таких вчених, як: Д. В. Дубов, В. О. Жадько, Ю. В. Завгородня, Л. І. Кормич, О. І. Харитоненко, Ю. С. Полтавець та інших. Міжнародний досвід щодо протидії кіберконфліктам і кібератакам досліджується в працях зарубіжних вчених, а саме: Ю. Тор, Р. Горва, М. Смеетс, Т. Рід, Д. Пуйвельде, А. Брантлі тощо. Попри тривалість наукових досліджень у сфері кібербезпеки, слід визнати, що на даний час питання визначення правового статусу кібератак та кібервійськових операцій, ефективної протидії кіберзлочинності та кібертерору досліджено фрагментарно, що обумовило актуальність обраної проблематики.

Отже, серед науковців питання впливу кібербезпеки на стабільність функціонування державних інституцій, об’єктів критичної інфраструктури та приватних установ вбачається суттєвим та актуальним і потребує подальшого дослідження.

Актуальність теми дисертації також обумовлена необхідністю внесення обґрунтованих пропозицій щодо вдосконалення національного законодавства з питань адміністративно-правового забезпечення кібербезпеки.

Зв’язок роботи з науковими програмами, планами, темами. Обрана тема дослідження належить до пріоритетних у галузі адміністративного права. Напрям дисертаційного дослідження обрано на основі Цілей сталого розвитку України на період до 2030 року, підтриманих Указом Президента України від 30 вересня 2019 року № 722, проголошених резолюцією Генеральної Асамблеї Організації Об’єднаних Націй від 25 вересня 2015 року № 70/1; з урахуванням положень Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447; Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392; Доктрина інформаційної безпеки України, затвердженої Указом Президента

України від 25 лютого 2017 року № 47; Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685. Дисертаційне дослідження виконано в межах Загального плану науково-дослідної роботи ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» на 2019–2024 рр.: «Дослідження теоретико-методологічних основ розвитку української державності в контексті світових модернізаційних процесів формування національних громадянських суспільств: політичний, юридичний, економічний, соціальний, психологічний та управлінський аспекти» (номер державної реєстрації – 0119U100492). Дисертація відповідає основним науковим напрямкам діяльності Міжрегіональної Академії управління персоналом з тем «Актуальні питання державотворення та захисту прав людини в Україні» (номер державної реєстрації – 0123U104042) та «Актуальні питання юридичної науки та практики» (номер державної реєстрації – 0123U104485).

Мета і завдання дослідження.

Мета роботи – визначення особливостей адміністративно-правових засад забезпечення кібербезпеки в Україні та проблем щодо ефективного забезпечення кібербезпеки, що виникли у зв'язку з умовами воєнного стану, викликів щодо повоєнної відбудови України, а також недоліків й прогалин у нормативно-правових актах, що визначають адміністративно-правові засади забезпечення кібербезпеки, та запропонувати шляхи їх вирішення.

Для досягнення поставленої мети в роботі необхідно було виконати наступні ***завдання:***

1. Визначити поняття, сутність та ознаки адміністративно-правового забезпечення кібербезпеки.

2. Встановити види об'єктів кібербезпеки та кіберзахисту.

3. Дослідити організаційно-адміністративні засади системи забезпечення кібербезпеки та кіберзахисту.

4. Окреслити систему суб'єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу.

5. Проаналізувати типи та особливості кіберзлочинів, а також сучасний стан кіберзлочинності та її вплив на безпеку держави.

6. Визначити правовий статус кібератак та кібервійськових операцій.

7. Визначити ключові загрози, що виникають у цифровому просторі, та запропонувати ефективні стратегії та методи, які можуть використовувати державні установи та приватний сектор для запобігання та мінімізації ризиків, спричинених кіберзагрозами.

8. Розробити пропозиції щодо вдосконалення нормативно-правового регулювання забезпечення кібербезпеки та посилення кібербезпеки держави на різних рівнях – від окремого користувача до національних державних органів, в умовах воєнного стану та викликів щодо повоєнної відбудови України.

Об'єктом дослідження є адміністративно-правові відносини, які виникають у сфері забезпечення кібербезпеки України.

Предмет дослідження – адміністративно-правові засади забезпечення кібербезпеки України.

Методи дослідження.

Методологічна основа дисертаційного дослідження представлена сучасними загальними та спеціальними методами наукового пізнання, вибір яких був обумовлений предметом, метою і завданнями дисертаційного дослідження. За допомогою формально-логічного та системного методу були визначені поняття кібербезпеки, кіберзахисту, кібератак, кібервійськових операцій, кіберзлочинності та злочинності у сфері комп'ютерної інформації (підрозділи 1.1, 1.2, 1.3, 2.1, 2.2). Для аналізу законодавчої бази у сфері кібербезпеки застосовано методи індукції та дедукції (підрозділи 1.1, 1.2, 1.3, 2.1, 2.2). Метод аналогії допоміг простежити специфіку правового регулювання кібербезпеки та приватності в Інтернеті в законодавстві різних країн, у тому числі й України (підрозділ 1.3). Соціологічний метод допоміг у вивченні думок та пропозицій юристів щодо практичного правового забезпечення кібербезпеки та конфіденційності у віртуальному просторі (підрозділ 1.3). За допомогою порівняльно-правового методу проаналізовано зарубіжний досвід формування та

розвитку законодавчої бази регулювання кіберпростору (підрозділи 1.1, 1.3, 2.1, 2.2). Історико-правовий метод був застосований при дослідженні зародження та еволюція засад кібербезпеки (підрозділ 1.1). Застосування аналітичного методу надало можливість оцінити найбільш оптимальні засоби забезпечення стабільності фінансового сектору серед найбільших банківських установ (підрозділ 3.2). Використання методів узагальнення та прогнозування, формально-догматичного методу зумовило виявлення недосконалостей правового регулювання сфер дослідження та розроблення пропозицій щодо внесення змін до національного законодавства (підрозділ 3.3).

Особливе місце відводиться юридичному методу наукового пізнання. Застосовано метод аналізу при вивченні наукової літератури. Також зустрічається структурно-функціональний метод та прогнозування. Використано статистичний метод.

Метод контент-аналізу використовувався для систематичного та об’єктивного вивчення вмісту документів, законів, веб-ресурсів та інших джерел, пов’язаних з електронними відкриттями.

Дані були зібрані шляхом систематичного аналізу нормативно-правових документів і наукових праць, а також аналітичних публікацій широкого кола експертів на відповідних інформаційних ресурсах.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним з перших в Україні комплексним дослідженням, спрямованим на аналіз адміністративно-правового забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України. В результаті дослідження сформульовано нові науково-обґрунтовані теоретичні положення та пропозиції щодо вдосконалення національного законодавства, яке здійснює адміністративно-правове регулювання забезпечення кібербезпеки, зокрема:

вперше:

сформульовано визначення правового статусу кібератак та кібервійськових операцій;

запропоновано авторську методику впровадження механізмів захисту об’єктів кіберзахисту в період воєнного стану та повоєнного відновлення України;

запропоновано комплексний підхід до кіберзахисту, який поєднує різні методи та інструменти;

внесено пропозицію щодо поліпшення обізнаності населення з кібербезпеки шляхом реалізації Кабінетом Міністрів України відповідної інформаційної політики;

сформульовано основні напрямки удосконалення адміністративно-правових засад кібезбезпеки стосовно забезпечення стабільності функціонування фінансових установ та розроблено комплекс необхідних організаційно-адміністративних заходів;

визначено такі основні проблеми та актуальні виклики сьогодення в сфері забезпечення кібербезпеки та кіберзахисту, протидії кіберзагрозам, таким як кібератаки та кіберзлочинність, в умовах воєнного стану та повоєнної відбудови України:

недостатній рівень кіберзахисту критичної інфраструктури;

недостатнє фінансування кібербезпеки;

дефіцит кваліфікованих спеціалістів;

високий рівень кіберзагроз;

низький рівень обізнаності громадян;

слабка координація між органами влади;

відсутність кіберстрахування;

низька кіберкультура в бізнесі;

відсутність стандартів кібербезпеки для блокчейн-технологій;

недостатній рівень міжнародної співпраці;

запропоновано включити до національного законодавства низку положень з метою вирішення зазначених проблем у сфері кібербезпеки України, створення сучасної ефективної системи забезпечення кібербезпеки та кіберзахисту, які б дозволили підвищити рівень кіберзахисту критичної інфраструктури,

організувати підготовку висококваліфікованих спеціалістів з кібербезпеки на рівні найкращих сучасних стандартів, підвищити рівень обізнаності громадян з кібергігієни та способів убезпечення від наявних кіберзагроз, підвищити рівень кібербезпеки і кіберкультури в бізнесі, посилити координацію між органами влади в питаннях моніторингу, узагальнення досвіду та своєчасного напрацювання і прийняття рішень щодо кібербезпеки, запровадити кіберстрахування, впровадити високі стандарти кібербезпеки для блокчейн-технологій, посилити рівень міжнародної співпраці щодо обміну досвідом, впровадження сучасних найкращих світових практик та об'єднання зусиль із зарубіжними партнерами в сфері забезпечення кібербезпеки та кіберзахисту, а також протидії кіберзлочинності та кібертероризму;

удосконалено:

поняття та зміст визначення кібербезпеки;

класифікацію принципів дотримання мережевого етикету (культури віртуального спілкування);

адміністративно-правові засади забезпечення кібербезпеки та кіберзахисту в Україні щодо боротьби комп'ютерними злочинами й кібератарками;

адміністративно-правові засади, що регулюють протидію кібербулінгу (кібернасильництву);

адміністративно-правові засади, що регулюють відповідальність за скоєння кіберзлочиннів;

поняття та зміст визначення злочинності у сфері комп'ютерної інформації;

класифікацію ключових загроз, що виникають у цифровому просторі, та адміністративно-правові методи запобігання та протидії цим загрозам у контексті забезпечення безпеки держави;

методи забезпечення кібербезпеки державних систем;

дістали подальшого розвитку:

нормативне визначення кіберзлочинності та приватності у віртуальному просторі;

нормативне визначення кіберконфліктів;

напрямки, які є ключовими при розробці стратегій кібербезпеки.

Практичне значення одержаних результатів. Викладені в дисертації висновки та пропозиції надалі можуть бути використані:

у науково-дослідній сфері – для дослідження теоретично-практичних проблем адміністративно-правового забезпечення кібербезпеки в Україні як в умовах воєнного стану, так і повоєнної відбудови;

у правотворчості – для доповнення та внесення змін до нормативно-правових актів, що регулюють забезпечення кібербезпеки в Україні;

у правозастосовній діяльності – використання одержаних результатів дослідження сприятимуть удосконаленню практики застосування положень національного законодавства з питань адміністративно-правового забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України;

у навчальному процесі – тези, положення та висновки, наведені у дисертації можуть використовуватись у навчальному процесі закладів вищої освіти при викладанні, підготовці до лекційних та практичних занять, розробці спеціалізованих навчальних курсів, написанні навчальних посібників та науково-дослідницькій роботі студентів спеціальностей «Право», «Кібербезпека та захист інформації», «Фінанси, банківська справа, страхування та фондовий ринок» і «Публічне управління та адміністрування».

Особистий внесок здобувача. Дисертація виконана здобувачем самостійно з використанням останніх досягнень порівняльного правознавства, адміністративного права, міжнародного права і кримінального права. Основні положення та висновки було сформовано на основі власних досліджень автора та обговорювалися й аналізувалися разом з науковим керівником. Публікації [1, 6, 7] здійснені без співавторства. У роботах [2 - 5], виконаних здобувачем спільно із співавторами, здобувачу належить участь у постановці задач, проведені науково-теоретичного дослідження адміністративно-правових засад забезпечення кібербезпеки в низці країн та формулюванні висновків. Ідеї та пропозиції співавтора наукової публікації у дисертації не використовувалися,

використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Апробація результатів дисертації. Основні положення, одержані узагальнення та висновки дисертаційної роботи були представлені дисертантом на засіданнях кафедри національної безпеки Інституту безпеки Міжрегіональної Академії управління персоналом та були оприлюднені на міжнародних науково-практичних конференціях: IX Міжнародної науково-практичної конференції «Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності». (м. Київ, 23-24 травня 2024 р.); Міжнародна науково-практична конференція «Інновації та їхній вплив на економіку та суспільство». (м. Суми, 25 жовтня 2024 р.).

Публікації. Основні результати досліджень дисертаційної роботи та пропозиції були викладені у двох наукових статтях, опублікованих у наукових фахових виданнях України, трьох статтях, опублікованій у міжнародних журналах, індексованих у наукометричній базі Scopus, а також у двох матеріалах та тезах доповідей в збірниках праць вказаних міжнародних конференцій, які додатково відображають наукові результати дисертації та є свідченням апробації роботи.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, вступу, трьох розділів, які логічно поєднані у вісім підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 278 сторінок, з них основного тексу – 194 сторінки з 3 рисунками та 4 таблицями. Список використаних джерел становить 233 найменувань і займає 31 сторінку. Додатки розміщено на 53 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

1.1. Поняття та зміст адміністративно-правового забезпечення кібербезпеки

Чимало експертів та науковців, у тому числі Діордіца І. В., цілком слушно зазначають, що все ширше використання в останні 30-40 років у найрізноманітніших сферах життєдіяльності суспільства комп'ютерних і телекомунікаційних технологій, у тому числі Інтернет-технологій, разом з великою кількістю переваг привнесло також і чималу кількість загроз. Реалізація цих загроз може завдати значної шкоди як на мікро, так і на макрорівні в рамках суверенних держав, а також і в світовому масштабі. Це призвело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації цієї нової сукупності загроз. Одночасно з цим виникає термін «кібербезпека» [111].

Бухарєв В. В. також вважає, що велике значення процес «електронного» розвитку відіграє на державному рівні, адже запровадження новітніх технологій відкриває величезні можливості у сфері державобудування. Наразі практично усі органи влади, що існують в Україні, так чи інакше використовують новітні технології, що фактично спричинило перенесення процесу обміну, обробки та пошуку інформації у електронний простір. Нарівні з цим, «цифрова революція» також має низку негативних аспектів, одним з яких є низький рівень кібербезпеки [113].

У цьому сенсі, Коваленко Н. В., розглядаючи кібернетичну безпеку як одну зі складових безпеки держави, деталізує такі аспекти: віртуальний простір не має меж і кордонів, в ньому будь-хто набуває широких можливостей у сфері його використання. Саме цей аспект робить віртуальний або ж кіберпростір, як його частіше називають, надзвичайно зручним середовищем для здійснення

протиправної діяльності. Сюди можна віднести правопорушення і злочини в різних сферах господарювання та управління, хакерські атаки на урядові сайти та банківські бази даних, інші дії, спрямовані на порушення суспільно-політичного ладу [114].

В Стратегії кібербезпеки України, схваленої Рішенням Ради національної безпеки і оборони України від 14 травня 2021 року та затвердженої Указом Президента України від 26 серпня 2021 року № 447, зазначається, що XXI століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій. Питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Стратегія визначає безпечний кіберпростір як запоруку успішного розвитку України [4].

В Стратегії наголошується, що російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України [4].

Стратегією встановлено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [4].

Франсело Д. вказує на те, що термін «кібербезпека» набуває все більшого поширення в останні часи, проте водночас багато керівників служб безпеки і експертів з інформаційної безпеки мають певні непорозуміння щодо правильного використання цього терміну та визначення його контексту [112].

Розглядаючи наукову літературу, бачимо, що і серед науковців також відсутнє єдине тлумачення терміну «кібербезпека». Також різняться визначення «кібербезпеки» в різних нормативно-правових документах.

Очевидно, варто провести аналіз визначень терміну «кібербезпека», які наведені в різних законодавчих та нормативно-правових актах, а також науковій літературі, визначивши його ключові аспекти.

Термін «кібербезпека» вперше почали використовувати в новинних статтях середини 1990-х років у США, коли уряд Сполучених Штатів Америки почав розуміти, наскільки взаємопов'язаними стали їх системи і, отже, під загрозою компрометації [115].

Етимологічно слово «кібербезпека» (cybersecurity, cyber security) походить від двох складових даної правової категорії – кібер та безпека. У Великому тлумачному словнику української мови «кібер» або «кібернетичний» – стосується до кібернетики; який створено, працює на основі принципів, методів кібернетики [134]. А «безпека» – стан, коли кому-, чому-небудь ніщо не загрожує [134].

У Франції Стратегія «Захист і безпека інформаційних систем» 2011 року, що присвячена питанням кібербезпеки країни, містить наступне визначення: кібербезпека – бажаний стан інформаційної системи, в якому вона може протистояти подіям з кіберпростору, які можуть поставити під загрозу доступність, цілісність або конфіденційність даних, що зберігаються, обробляються чи передаються, а також пов'язаних послуг, які ці системи пропонують або роблять доступними [116].

У Стратегії кібербезпеки Німеччини 2021 року зазначено, що кібербезпека – це IT-безпека всіх систем інформаційних технологій, які є та можуть бути взаємопов'язані на рівні даних у кіберпросторі [117]. Стратегія кібербезпеки Німеччини встановлює чотири наскрізні провідні принципи:

1. Встановлення кібербезпеки як спільного завдання уряду, приватної промисловості, наукової спільноти та суспільства.

2. Зміцнення цифрового суверенітету уряду, приватної промисловості, наукової спільноти та суспільства.

3. Зробити цифрову трансформацію безпечною.

4. Встановлення вимірюваних, прозорих цілей [117].

У Національній стратегії кібербезпеки Канади 2022 року кібербезпека означає захист цифрової інформації, а також цілісність інфраструктури розміщення та передачі цифрової інформації. Зокрема, кібербезпека включає

сукупність технологій, процесів, практик і заходів реагування та зменшення впливу, призначених для захисту мереж, комп'ютерів, програм і даних від кібератак, пошкоджень або несанкціонованого доступу з метою забезпечення конфіденційності, цілісності та доступності [118].

Стратегія визначає поняття кібератаки, як атаки, яка передбачає несанкціоноване використання, маніпулювання, переривання або знищення електронної інформації або електронних пристроїв або комп'ютерних систем і мереж, які використовуються для обробки, передачі чи зберігання такої інформації, або доступу до них за допомогою електронних засобів [118].

Національній стратегії кібербезпеки Канади передбачає три основні напрями реалізації:

I. Захист державних систем – захист урядових систем шляхом визначення повноважень та відповідальності, посилення безпеки інформаційних систем на федеральному рівні та підвищення рівня обізнаності уряду в сфері кібербезпеки.

II. Партнерство для захисту життєво важливих кіберсистем за межами федерального уряду – співпраця з нефедеральними кіберсистемами через розвиток партнерських відносин з приватним сектором та суб'єктами критичної інфраструктури.

III. Допомога канадцям у безпеці в Інтернеті – забезпечення безпеки громадян в кіберпросторі, що включає боротьбу з кіберзлочинністю та захист особистих даних [118].

У Стратегії Уряду Канади кібербезпеки підприємств 2024 року кібербезпека означає безпеку передачі електронних даних та інформації в кіберпросторі. Це охоплює технології, процеси, практики, а також заходи реагування та зменшення впливу, призначені для захисту електронної інформації, даних та інформаційної інфраструктури від зловживання, несанкціонованого використання чи збою в кіберпросторі. Кібербезпека доповнює IT-безпеку [119].

Національна стратегія кібербезпеки Турецької Республіки від 29 грудня 2020 року містить таке визначення: кібербезпека – захист інформаційних систем,

що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам [120]. При цьому під кіберпростором розуміється середовище, що складається з інформаційних систем, розподілених по всьому світу, в тому числі мереж, що з'єднують ці системи. Національний кіберпростір визначається як простір, який складається з інформаційних систем суб'єктів, що перебувають під юрисдикцією Турецької Республіки [120].

У Стратегії кібербезпеки Нідерландів на 2022 – 2028 роки від 6 грудня 2022 року наведено наступне визначення: кібербезпека – повний спектр заходів, спрямованих на зниження відповідних ризиків до прийнятного рівня. Заходи можуть бути зосереджені на запобіганні кіберінцидентів і, якщо кіберінцидент все ж таки стався, на виявленні, обмеженні шкоди та відновленні. Що є прийнятним рівнем ризику, визначається оцінкою ризику [121].

Під кіберінцидентом в Стратегії кібербезпеки Нідерландів розуміється – поєднання подій або дій, які можуть призвести до порушення одного чи кількох цифрових процесів. Це включає як кібератаку (зловмисну дію суб'єкта, який має намір порушити один або кілька цифрових процесів за допомогою цифрових засобів), так і збій системи внаслідок природних або технічних причин або людської помилки [121].

Стратегія кібербезпеки Нідерландів визначає, що до збоїв належать ситуації, коли надійність інформаційно-комунікаційних технологій знижується, обмежується доступність або порушується конфіденційність та/або цілісність збереженої в системах інформаційно-комунікаційних технологій інформації [121].

Незважаючи на ускладнення визначення критеріїв кібербезпеки, в Стратегії Нідерландів зроблено вельми важливий в методологічному аспекті висновок – кібербезпека може бути досягнута тільки в системній кореляції з вирішенням проблем захисту та забезпечення основних прав, цінностей і соціально-економічних вигод членів соціуму [122].

В опублікованій 22 листопада 2023 р. Стратегії кібернетичної безпеки Австралії на 2023-2030 роки під кібербезпекою розуміється забезпечення доступності, цілісності та конфіденційності інформаційно-комунікаційних технологій, а також захист людей, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання інформаційно-комунікаційних технологій для цілей сексуальної експлуатації [123].

Важливо зазначити, що відповідно до пункту 5 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2].

Згідно з частиною першою статті 7 Закону України «Про основні засади забезпечення кібербезпеки України» забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки [2].

З урахуванням того, що проблема кібербезпеки носить глобальний характер, важливою є позиція міжнародних організацій.

Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у Рекомендації X.1205 від 18 квітня 2008 року «Мережі передачі даних, відкриті системи комунікацій та безпека» дає таке визначення: кібербезпека – це сукупність інструментів, політик, концепцій безпеки, заходів безпеки, інструкцій, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можна використовувати для захисту кіберсередовища, організації та активів користувачів. Активи організації та користувача включають підключені обчислювальні пристрої, персонал, інфраструктуру, програми, послуги, телекомунікаційні системи та всю інформацію, що передається та/або зберігається в кіберсередовищі. Кібербезпека прагне забезпечити досягнення та підтримку властивостей безпеки організації та активів користувача проти відповідних ризиків безпеки в кіберсередовищі. Загальні цілі безпеки включають наступне:

- доступність;
- цілісність, яка може включати автентичність і неспростовність;
- конфіденційність [124].

В даній дефініції з’являється ще одна категорія «кіберсередовище», припускаю, що його можна ототожнювати із кіберпростором [111].

Відповідно до пункту 1 статті 2 Регламенту Європейського Парламенту і Ради (ЄС) від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) «кібербезпека» означає діяльність, необхідну для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, які зазнають впливу кіберзагроз [131]. А згідно з пунктом 2 статті 4 Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу «безпека мережевих та інформаційних систем» означає здатність мережевих та інформаційних систем витримувати - на певному рівні впевненості - будь-яку дію, що загрожує доступності, справжності, цілісності або конфіденційності збережених або переданих чи опрацьованих даних або пов’язаних послуг, які пропонують такі мережеві та інформаційні системи або які доступні за допомогою таких систем [233].

Стандарт ICO/IEC 27032 надає визначення «кібербезпеки» через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації у кіберпросторі. При цьому, кіберпростором є середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [232].

В цілому слід зазначити, що практично всі національні стратегії щодо забезпечення кібербезпеки і переважна більшість експертів пов’язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп’ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет) [128]. Виходячи з цього, погоджуємося з науковцем Барановим О. А., що основною кваліфікуючою ознакою віднесення до

проблематики кібербезпеки є обов'язкова умова використання комп'ютерних систем і телекомунікаційних мереж [128].

Тепер розглянемо відомі думки науковців, які досліджували це питання.

Згідно з Д. Шацом, Дж. Волл і Р. Башроушу, кібербезпека (вона ж комп'ютерна безпека і безпека інформаційних технологій) – це захист комп'ютерних систем і комп'ютерних мереж від розкриття даних, пошкодження та крадіжки їх обладнання, програмного забезпечення або електронної інформації, а також від порушення або неправильного спрямування наданих ними послуг [125].

Баранов О. А. також звертає увагу, що проблематика кібербезпеки має відношення до обороту інформації, зокрема, до забезпечення суб'єктів інформаційних відносин достовірною, своєчасною та повною інформацією, а також до недопущення несанкціонованого використання і поширення інформації, порушення її цілісності та конфіденційності [128]. І. В. Діордіца зазначає, що наскрізною категорією даної дефініції є «інформація», яка і є основним об'єктом інформаційних правовідносин, що можуть мати місце у кіберпросторі [111].

За А. Калдером, кібербезпека – це використання сучасних технологій, процесів і засобів контролю з метою захистити комп'ютерні системи та мережі, програми, пристрої і дані від кібернетичних атак, а також з метою зниження ризику здійснення кібератаки [126].

І. М. Сопілко зазначає, що система кібербезпеки складається із декількох елементів, координація яких всередині організації має вирішальне значення для успіху всієї програми кібербезпеки. Ці елементи включають наступне: безпеку додатків; безпеку даних; безпеку критично важливої інфраструктури; мережеву і операційну безпеку; хмарну безпеку; планування аварійного відновлення, а разом із ним і забезпечення безперервності бізнесу; фізичну охорону; навчання кінцевих користувачів [127].

Науковець Баранов О. А. в своєму дослідженні робить висновок, що з проблемою кібербезпеки пов’язана проблема нейтралізації негативних інформаційних впливів на технологічному рівні [128].

Низка науковців, досліджуючи проблему забезпечення кібербезпеки в своїх працях розкривають її зміст через необхідність захисту основоположних прав і життєво важливих інтересів людини, суспільства і держави.

Так, Бухарєв В. В. стверджує, що як і будь-яке інше правове явище в державі, основні засади забезпечення кібербезпеки знаходять своє закріплення в нормах Конституції України, тому що цей нормативний акт є основним джерелом національної правової системи. Так, у статті 3 Конституції вказується, що людина, її життя і здоров’я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов’язком держави. Тобто наявність адміністративно-правового механізму охорони кібербезпеки та інших подібних об’єктів є проявом виконання державою своїх обов’язків з приводу забезпечення життєдіяльності населення країни [113].

Деякі українські дослідники вважають, що в контексті нормативно-правового розуміння національної та інформаційної безпеки кібербезпека може визначатися як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем [129].

В. Н. Фурашев визначає кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації [130].

І. В. Діордіца пропонує розуміння «кібербезпеки» (у вузькому сенсі) – стан індивіда, суспільства та держави в якому відсутня будь-яка небезпека. А в

широкому сенсі «кібербезпека» – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі, в якому є можливим безперешкодне створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [111].

Схожої думки дотримується О. А. Баранов, який зазначає, що кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [128].

Окремо виділяють дії, що порушують безпеку інформаційних мереж і систем:

перехоплення електронної комунікації, копіювання або модифікація даних;

неавторизований доступ до комп'ютера або комп'ютерних мереж;

деструктивні атаки на мережі, зокрема атаки на доменні імена, перевантаження мережі штучними повідомленнями, атаки, спрямовані на порушення маршрутизації;

шкідливе програмне забезпечення;

підробка веб-сайтів;

безпекові інциденти як наслідок непередбачених і ненавмисних подій, таких як природні катаклізми, збої у роботі апаратних засобів та програмного забезпечення, людські помилки [135].

Таке визначення більш розвинули В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та С. В. Толюпа. На їх думку, кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечуються їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [132].

Змістовне визначення «кібербезпеки» запропоновано О. Г. Корченко, адже він розкриває сутність кібербезпеки через призму ключових ознак цього явища.

На його погляд, кібербезпекою є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугрупувань розгортаються навколо інформаційного ресурсу, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем [133] та які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об’єктів критично важливої інформаційної і кіберінфраструктури [133].

1.2. Організаційно-адміністративні засади системи забезпечення кібербезпеки та кіберзахисту

Проведене в підрозділі 1.1 наукове дослідження як самого змісту визначення «кібербезпеки», так і різних його аспектів, дало розуміння сутності його значення, а також багатогранності цього правового інституту.

Аналізуючи усі аспекти кібербезпеки, в рамках дисертаційного дослідження, не можемо залишити поза увагою питання організаційно-адміністративних засад системи забезпечення кібербезпеки та кіберзахисту. Проведення наукового дослідження даної проблематики з урахуванням сучасної нормативної бази в сфері регулювання кібербезпеки дозволить більш повно побачити сферу її безпосередньої дії.

Під системою розуміється сукупність яких-небудь елементів, одиниць, частин, об’єднуваних за спільною ознакою, призначенням [134]. Таким чином, система кібербезпеки – сукупність органів, які задіяні до забезпечення кібербезпеки [111].

За В. Шеломенцевим, система кібернетичної безпеки (система кібербезпеки) – сукупність спеціальних суб’єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс

відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються [136].

З таким формулюванням в своєму дослідженні погоджується і Діордіца І. В., який також уточнює і розширює його: система кібернетичної безпеки – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом в кібернетичному просторі для забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [111].

Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкту забезпечення кібербезпеки, пов'язану зі:

створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі;

впорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень [111].

Організаційне забезпечення системи кібербезпеки характеризується місцем і роллю спеціальних суб'єктів (відповідних державних органів та їх спеціалізованих підрозділів), їх функціями, повноваженнями, а також підставами, умовами і напрямами їх взаємодії при здійсненні заходів із забезпечення безпеки у кіберпросторі.

Статтею 5 Закону України «Про основні засади забезпечення кібербезпеки України» суб'єктами забезпечення кібербезпеки визначено:

Президента України – здійснює координацію діяльності у сфері кібербезпеки як складової національної безпеки України;

Національний координаційний центр кібербезпеки – здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України;

Кабінет Міністрів України – забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг);

суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, а саме:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [2].

Причому частина перша статті 8 Закону України «Про критичну інфраструктуру» передбачає, що віднесення об'єктів до критичної

інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України. Віднесення банків, інших об’єктів, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснюється в порядку, встановленому Національним банком України. Віднесення об’єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами [137].

Згідно з частиною п’ятою статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору [2].

Частиною першою статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» визначено, що національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових,

розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [2].

Відповідно до частини другої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» основними суб'єктами національної системи кібербезпеки є:

Державна служба спеціального зв'язку та захисту інформації України,

Національна поліція України,

Служба безпеки України,

Міністерство оборони України та Генеральний штаб Збройних Сил України,

розвідувальні органи,

Національний банк України [2].

Крім того, з метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, рішенням Ради національної безпеки і оборони України від 27 січня 2016 року утворено Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України [138].

Очевидно, що в рамках дисертаційного дослідження варто проаналізувати та співставити терміни кібербезпека та кіберзахист.

Актуальність такого аналізу крім іншого обумовлюється тим, що з робіт деяких науковців іноді бачимо, що ці поняття використовуються як синоніми та вважаються ідентичними, що є вкрай невірним.

Етимологію, зміст та основні аспекти визначення кібербезпеки викладено в підрозділі 1.1.

Щодо терміну «кіберзахист», то він складається з двох складових – «кібернетичний» та «захист». Остання складова, відповідно до Словника української мови за редакцією І. К. Білодіда тлумачиться як оборона чи охорона кого-небудь чи чого-небудь від нападу, замаху, удару чи іншої небезпеки;

пильно стежити за недоторканністю чого-небудь і багато робити для цього [139, с. 380]. Схожий за вимовою та формою термін «захищати», за Словником української мови Б. Грінченко, визначається як заступництво [140, с. 113]. Інша складова поняття походить від назви такої науки як кібернетика, якій відомий український вчений В. М. Глушков надав таке визначення: кібернетика – наука про закономірності обробки, отримання, зберігання, обміну інформацією в складних системах управління, незважаючи на походження останніх (технічне, біологічне, соціальне, тощо) [141, с. 440].

Враховуючи лінгвістичні особливості складових елементів поняття «кіберзахист», термін можна розтлумачити як захисні дії, направлені на забезпечення безпеки у сфері отримання, обробки, зберігання та передачі інформації за допомогою складних систем управління [113].

Бухарєв В. В. висловлює думку, що кібербезпека – це правовий інститут, тобто ціла система юридичних норм, якими регулюється безпечний стан обробки інформації у кіберпросторі. Тут йдеться про цілу сферу діяльності, в рамках якої об’єднуються різні механізми, що функціонують з єдиною метою. Враховуючи цей факт, можна припустити, що кіберзахист є складовим елементом кібербезпеки, тому його розгляд необхідно проводити через призму особливостей останнього інституту [113].

Погоджується з цією тезою в своїх роботах О. В. Коломієць, який стверджує, що поняття кіберзахисту доречно трактувати як сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки [142].

В. П. Шеломенцев пропонує більш широке визначення, який під кіберзахистом розуміє систему заходів правового, організаційного, ресурсно-фінансового, програмно-технічного та іншого характеру, спрямовану на створення умов, за яких виключаються або суттєво утрудняються протиправні посягання на об’єкти такого захисту (певні інформаційні об’єкти кіберпростору). Іншими словами, це діяльність у кіберпросторі з охорони певних його об’єктів

від протиправних посягань (наприклад, кіберзлочинів) і створення перешкод у реалізації загроз кримінального характеру [143].

Відповідно до пункту 7 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [2].

В своєму досліджені Бухарєв В. В стверджує, що під поняттям кіберзахисту слід розуміти систему (механізм) засобів різного характеру, за допомогою яких здійснюється підтримка та забезпечення інституту кібербезпеки. Кіберзахист здійснюється за допомогою використання досить широкого кола правових інструментів, порядок використання яких врегульовано нормами багатьох законодавчих та підзаконних нормативно-правових актів. Розмежування кібербезпеки та кіберзахисту є принципово важливим питанням, адже воно прямо пов’язане із процесом їх реалізації, який при неправильному підході може нанести шкоду охоронюваним законом інтересам та правам людей, які здійснюють різні операції з інформацією в кіберпросторі [113].

Проведенні в дисертаційному дослідженні аналізи змісту і основних аспектів інституту кібербезпеки та механізму кіберзахисту має велике значення для визначення їх об’єктного складу.

Отже, як зазначалося вище, кібербезпека являє собою правовий інститут. А у вигляді правового об’єкта розглядають об’єкт тієї чи іншої правової галузі (нагадаємо, що об’єкт галузі – це сукупність суспільних відносин, в сфері яких між окремими суб’єктами виникають відповідні права і обов’язки) або ж об’єкт правовідносин певного типу.

Зокрема, частиною першою статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» встановлено, що об’єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури [2].

Тоді як, об’єкти кіберзахисту – це ресурси, інформація, системи, мережі, процеси або інші елементи, які підлягають захисту від кіберзагроз.

Так, частина друга статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» об’єктами кіберзахисту визначає:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [2].

Отже, до об’єктів кіберзахисту зазвичай відносяться:

1) інформація, зокрема:

персональні дані (ПІБ, адреса, фінансова інформація);

конфіденційна корпоративна інформація (комерційна таємниця, ноу-хау);

державні секрети та критична інформація;

2) інформаційні системи, зокрема:

корпоративні системи управління (ERP, CRM);

системи обліку та зберігання даних;

бази даних;

3) комп’ютерні мережі, зокрема:

локальні мережі підприємств;

хмарні сервіси;

інтернет-мережі;

4) фізичні пристрої, зокрема:

сервери та серверні кімнати;

робочі станції (комп’ютери, ноутбуки);

мобільні пристрої (смартфони, планшети);

обладнання IoT (інтернет речей);

5) програмне забезпечення, зокрема:

операційні системи;

додатки та сервіси;

захисне програмне забезпечення (антивіруси, системи виявлення вторгнень);

6) комунікаційні засоби, зокрема:

електронна пошта;

месенджери;

відеоконференції;

7) критична інформаційна інфраструктура, зокрема:

енергетичні мережі;

телекомунікації;

транспортні системи;

банківські системи;

8) людський фактор, зокрема:

працівники організації;

користувачі систем;

адміністратори та аналітики безпеки;

9) процеси, такі як:

бізнес-процеси (закупівлі, продажі);

технологічні процеси (виробничі цикли);

процеси управління кібербезпекою;

10) репутація та імідж, зокрема:

довіра клієнтів;

позиція компанії на ринку;

вплив на суспільство;

11) правові та регуляторні аспекти, зокрема:

дані, які підлягають захисту відповідно до закону (наприклад, GDPR);

дотримання стандартів безпеки (ISO/IEC 27001, NIST);

12) веб-ресурси, такі як:

корпоративні веб-сайти;

портали для клієнтів або партнерів;

інтернет-магазини;

веб-додатки;

13) користувацькі облікові записи, а саме:

логіни та паролі користувачів;

сесійні токени;

доступ до багатофакторної автентифікації (MFA);

14) фінансові ресурси, зокрема:

банківські рахунки;

електронні платіжні системи;

криптовалюти та гаманці;

15) архіви даних, зокрема:

архівні сервери;

резервні копії (backups);

магнітні стрічки чи інші носії;

16) критичні технології, зокрема:

системи управління виробництвом (SCADA);

автоматизовані системи промислового управління (ICS);

17) розумні системи (Smart Systems), зокрема:

розумні будинки (smart home);

розумні міста (smart city);

інтелектуальні транспортні системи;

18) хмарні інфраструктури, зокрема:

платформи як послуга (PaaS);

інфраструктури як послуга (IaaS);

програмне забезпечення як послуга (SaaS);

19) Медіа-контент, зокрема:

відео, аудіо та графічні файли;

контент, захищений авторським правом;

стратегії контент-маркетингу;

20) алгоритми та моделі, зокрема:

алгоритми шифрування;

моделі штучного інтелекту;

прогностичні моделі;

21) канали зв’язку, зокрема:

голосові дзвінки;

віртуальні приватні мережі (VPN);

захищені канали для передачі даних;

22) фізичне середовище, зокрема:

центри обробки даних (ЦОД);

системи відеоспостереження;

контроль доступу до приміщень;

23) соціальні мережі, зокрема:

корпоративні акаунти в соціальних мережах;

сторінки бренду або компанії;

дані взаємодії з клієнтами (коментарі, відгуки);

24) навчальні ресурси, зокрема:

платформи онлайн-курсів;

бази знань організації;

документація для користувачів;

25) мобільні додатки, зокрема:

корпоративні мобільні додатки;

додатки для комунікацій (Slack, Teams);

ігрові чи інші розважальні додатки, пов'язані з компанією;

26) інфраструктура резервного відновлення, зокрема:

дата-центри резервного відновлення;

системи аварійного планування;

сценарії реагування на інциденти.

1.3. Правове регулювання забезпечення кібербезпеки та конфіденційності в інтернет

Окрім очевидних переваг, сучасний цифровий світ несе в собі багато загроз. Технологічний прогрес у розвитку цифрових та інформаційних технологій, тобто неймовірне накопичення та генерування інформації, розкриває безпрецедентні можливості для людства. Ступінь і вектори цих можливостей ще не повністю зрозумілі. Однак у той же час революція даних позбавляє людей контролю над своєю особистою інформацією в Інтернеті. На особистому рівні кібератаки та порушення безпеки можуть мати різноманітні неприємні та небезпечні наслідки, наприклад, викрадення особистих даних для фінансових та майнових маніпуляцій або вимагання сімейних фотографій [80].

Кібербезпека також є ключовим аспектом забезпечення належного функціонування критичної інфраструктури (електростанції, лікарні, банки тощо) та державного адміністративного апарату. Сьогодні робота всього військово-промислового комплексу можлива лише за умови технічної підтримки та підтримки інфраструктури кіберзахисту. Зі зростанням ролі ідей і концепцій у сучасному світі захист інтелектуальної власності в кіберпросторі набуває особливого значення.

ІТ-індустрія та інформаційний простір розвиваються зі швидкістю сніжного кому, і ні звичайні громадяни, ні бізнес-корпорації, ні правова система не встигають за швидким реагуванням на виклики та загрози, які звідси виникають. Кіберзлочинці, озброєні технічним обладнанням і навичками та використовуючи недосконаліть правового регулювання у віртуальному світі, активно спричиняють проблеми.

Очевидно, що посиляться дії щодо обмеження суспільного стеження за допомогою нових адміністративно-правових заходів. Споживачі платитимуть більше за послуги, які гарантують конфіденційність, а ринок технологій захисту конфіденційності буде рости. У квітні 1999 р. журнал «The Economist» опублікував статтю під назвою «Кінець приватності», в якій говорилося про неможливість стримати хвилю електронного вторгнення в конфіденційність і приватність, що стало однією з найбільших соціальних змін сучасності [110].

З огляду на те, що цифрова інформація, ймовірно, може зберігатися нескінченно довго, потрібно розглянуті детальні заходи щодо адміністративно-правового забезпечення вирішення проблеми конфіденційності та віртуальної безпеки. Звичайно, це не дасть 100% гарантії практичної реалізації таких прав і свобод. Однак це принаймні створить необхідну законодавчу основу для певного цивілізованого контролю над віртуальним простором та його використанням [80]. Окрім законодавчого регулювання кібербезпеки та конфіденційності в Інтернеті, неодмінними умовами розвитку стабільного суспільства є складові монетарної та фіскальної політики. Серед них особливої уваги заслуговують гарантована законом вільна конкуренція, лояльна торгівля та рух капіталу. Політична стабільність і поступальний розвиток також є критичними факторами [67]. Також для всебічного висвітлення теми дослідження необхідний постійний моніторинг та порівняльний аналіз отриманих даних. Це стосується насамперед країн з розвиненою економічною системою [81].

Кібербезпека та захист конфіденційності у віртуальному просторі як складові сфери послуг є актуальними складовими сучасної економіки. Особливо це стосується таких країн, як Сполучені Штати Америки, Федеративна

Республіка Німеччина та Китайська Народна Республіка [82]. Якщо говорити про розвиток бізнесу, то необхідною умовою для його функціонування є кібербезпека, її правові аспекти та практична реалізація. Серед своїх функцій управління підприємством також включає моніторинг і діагностику системи кібербезпеки [83]. Зокрема, загроза кібератак є найбільшою небезпекою для бізнес-компаній. Їх лідери вважають кібератаки небезпечнішими за втрату репутації бренду, правове регулювання та економічну невизначеність [84].

Країни світу нарощують свою кіберпотужність і зміцнюють свої кіберкордони. Для України це стало особливо актуальним після повномасштабного вторгнення росії 24 лютого 2022 року. Велика увага, особливо у сфері державного управління, приділяється кібергігієні [85]. Крім того, децентралізація є надзвичайно важливою в умовах нашої країни. Ця реформа надала можливість громадам самостійно вирішувати пріоритетність та актуальність питань, які потребують вирішення. Важливо, що прийняття бюджету та його розподіл залишаються на місцевому рівні [86]. Іншими словами, фінансова свобода повинна сприяти ефективній реалізації кібербезпеки та захисту конфіденційності на місцевому рівні. Незважаючи на те, що правова система, особливо в міжнародному форматі, є неймовірно забюрократизованою та негнучкою, правове регулювання кібербезпеки та обігу персональних даних у кіберпросторі є динамічною нормотворчою діяльністю, яка потребує постійного моніторингу та пошуку ефективних стратегій протидії віртуальним загрози безпеці громадян і держави.

Формування правових засад кібербезпеки та конфіденційності у віртуальному просторі є невід’ємною частиною законодавчого процесу. Сюди також входить його практична реалізація та інкорпорація в законодавство різних країн, міжнародні угоди, договори тощо.

Тому для виконання даного наукового дослідження необхідно звернути увагу на наукові праці, в яких у цілому розглядаються правові механізми держав та міжурядових об’єднань. Зокрема, у своїх наукових працях науковець Брацук І. З. охарактеризував теоретико-правову взаємодію права Європейського

Союзу та національного права держав-членів. Надзвичайно цінним є те, що автор також дослідив механізми та конституційно-правові особливості імплементації норм права Європейського Союзу в національне законодавство держав-членів [87].

Дослідник Шемчук В. В. зосереджується на досліджені теоретичних і практичних проблем інформаційної безпеки як однієї з основоположних функцій держави в сучасному світі [88]. Ковач Л. зосереджується на аналізі стратегій кібербезпеки країн ЄС та НАТО [89]. Клименко Н. розглянула трактування безпеки в працях юристів, соціологів, філософів від античності до сьогодення [90]. В низці досліджень, опублікованих в [84], показано сучасний стан кібербезпеки, основні тренди віртуальних технологій, протистояння зовнішній кіберагресії та технічні аспекти кібербезпеки.

Науковець Пазюк А. В. досліджує розвиток міжнародного інформаційного права на різних етапах. Зокрема, особливу дослідницьку увагу зосереджено на впливі Інтернету на формування законодавчих ініціатив. Останнє пов’язане з появою кіберпростору та його всебічним проникненням в усі сфери життєдіяльності громадян, суспільства та держави [91]. Войціховський А. розглядає концептуальні підходи до кібербезпеки в європейському правовому полі, правових та організаційних основах ЄС та подальші перспективи їх розвитку [92].

Враховуючи євроінтеграційні прагнення України та практичні кроки щодо реалізації цих прагнень, дослідження нормативно-правової бази Європейського Союзу та особливостей її імплементації в національне законодавство є надзвичайно актуальними. Включаючи як дослідження в галузі кібербезпеки, так і науково-аналітичні праці з адміністративно-правових аспектів забезпечення кібербезпеки.

Науковець Пазюк А. розглядав питання приватності в Інтернеті через призму правової конкретики. Зокрема, автор зазначив, що незважаючи на швидку цифровізацію, питання, пов’язані з кібербезпекою, все одно будуть вирішуватися [93]. Булавіна С. і Давидова Т. займаються вивченням наслідків

порушення прав на приватність. Вони аналізують міжнародну практику для впровадження кращого досвіду в правове поле України [94].

Як найбільша небезпека для будь-якої організації, кібербезпека та кібератаки розглядаються в праці Бакалінської О. [95]. Крім того, Бакалінська О. проводить наукове дослідження щодо вдосконалення законодавства з кібербезпеки в Україні. Автор розглядає сучасні тенденції в країнах Європейського Союзу та НАТО, а також вплив повномасштабної війни на кібернетичне середовище в Україні та необхідність адміністративно-правового регулювання на міжнародному рівні в українському контексті [96].

Наразі питання забезпечення адміністративно-правового регулювання кібербезпеки та конфіденційності в Інтернеті постало надзвичайно актуальним. Воно є предметом наукового та практичного інтересу як дослідників, так і юристів, медіаекспертів, економістів, соціологів, державних службовців.

Враховуючи зростаючу роль кібербезпеки в житті людей і в міжнародному масштабі, а також зростаючі проблеми із захистом конфіденційності у віртуальному світі, очевидні переваги віртуалізації в усіх аспектах нашого повсякденного життя мають зворотний бік. Загрози національній безпеці через кіберзлочинність, як на рівні країни, так і в усьому світі будуть лише зростати. В умовах повномасштабної війни в Україні фактор віртуалізації життя набув специфічних ознак. Війна поширюється на всі простори, включаючи віртуальну сферу. Тому для з метою забезпечення національної безпеки нашої країни одним з пріоритетів є законодавче гарантування кібербезпеки.

Сучасний розвиток людської цивілізації значною мірою залежить від розвитку віртуального середовища. Наприклад, термін «диджиталізація (оцифрування)» став одним із найпопулярніших в онлайн-середовищі України у 2019 році [94]. Слово «диджиталізація» є одним з результатів глобальної цифрової революції. Це неологізм, що позначає зміни в суспільному житті, викликані появою, розповсюдженням і широким використанням цифрових технологій.

На сьогоднішній день віртуальний світ багато в чому повторює взаємодії у фізичній сфері. Це також стосується правовідносин у цифровому форматі. Зокрема, сформувалася система правовідносин між споживачами та інтернет-провайдерами, електронні платежі, зв'язок, надання адміністративних послуг через цифрові додатки, електронне управління та правоохоронні функції. Закони країн і міжнародні угоди все це певною мірою регламентують. Водночас існує мережевий етикет (поняття виникло у 1980-х роках – від англійського «net» і французького «etiquette») – культура віртуального спілкування, яка передбачає дотримання кількох основних категорій:

емоційний контакт (смайли, емодзі, форми звернення на «ти» або «ви», ігнорування агресивних інцидентів, усталені форми вітання та прощання в офіційних листування тощо);

технічні особливості віртуального спілкування (правила цитування, форма, розмір і колір шрифту, особливості форматування тексту, оформлення презентацій тощо);

адміністративні (дозволеність чи недоречність флейму (емоційного утвердження своєї позиції), реклами чи її заборони, тематика групи тощо).

До порушень мережевого етикету належать особисті нападки, словесні та візуальні образи, відхилення від теми розмови, надмірна самореклама, плагіат, аморальні висловлювання тощо.

При формуванні та вдосконаленні правової культури, пов'язаної з цифровізацією суспільства, Україні слід звернути увагу на відповідні досягнення в країнах Європейського Союзу. Враховуючи війну, яка триває, країна також повинна враховувати внутрішнє становище та потреби.

Ще з давніх часів і аж до XVI століття розуміння безпеки пов'язувалося з фізичним захистом від різних загроз. Державі відводилася роль гаранта такого захисту. В тих конкретних історичних умовах співпраця та спільнота були вирішальними для виживання. Самотність зазвичай прирівнювалася до смерті та різко знижувала шанси на фізичне виживання. Християнські філософи вважали безпеку пов'язаною з Божим захистом, благодаттю або гнівом небесних сил.

В епоху Відродження виховували усвідомлення безпеки як доброзичливості мудрого правителя (монарха). У XVII і XVIII століттях сильна держава мала виступати гарантом природного права громадян на безпеку. У XIX столітті виникли принципово інші розуміння забезпечення цього права. Тепер сама держава може становити загрозу для громадян, як і вони для держави. Все більшого значення набували правові аспекти розподілу гілок влади, охорони території держави, міжнародні угоди.

У XX столітті, незважаючи на дві світові війни, низку революцій, репресій, геноцидів та ідеологій ненависті, поняття «безпека» додало усвідомлення її стосовно людини, суспільства та держави. Добре сформований інститут держави зобов'язаний захищати всі права і свободи громадян. Це має гарантувати вільний і стабільний поступальний розвиток, прогрес і процвітання. Актуальними стали поняття суверенітету та територіальної цілісності. У наш час до існуючих інтерпретацій і розуміння безпеки додалися гуманітарні компоненти. Релігія, мова, традиції та ідентичність є частиною сучасної концепції безпеки людської цивілізації. Йдеться насамперед про внутрішню (національну) безпеку. Проте в умовах поглиблення глобалізації та зростання ролі віртуального світу в усіх міжнародних процесах, значна увага починає приділятися глобальній безпеці [90].

У країнах західного культурного кола широко поширене переконання, що успішне, справедливе та ефективне виконання судових рішень, як щодо осіб, які здійснюють економічні операції, так і щодо державних органів чи посадових осіб, має вирішальне значення для розвитку норм правової культури та незалежність суддів. Водночас ми спостерігаємо збільшення обсягу різноманітних документів і матеріалів міжнародної юриспруденції. Це, серед іншого, потребує продуманих підходів до ухвалення максимально об'єктивних судових рішень [97].

Освіта має важливе значення для забезпечення сталого розвитку, який включає, серед іншого, кібербезпеку та конфіденційність у цифрову епоху. Водночас освіта спрямована на підвищення інтелектуального рівня людства.

Люди повинні навчитися розпізнавати небезпечну поведінку та вміти її коригувати або запобігати таким проявам. Ефективні зміни мають відбуватися як на рівні особистості, так і на рівні суспільства. Активна реалізація свого потенціалу сприятиме суспільному благополуччю та розкриттю кращих перспектив [98].

Кібербезпека та конфіденційність у віртуальному просторі є ключовими питаннями економічної, політичної та військової безпеки. Проте наразі вони є найбільш вразливими щодо захисту (в тому числі правового), розуміння загроз і перспектив, векторів розвитку, можливостей впливу в різних сферах діяльності суспільства. Слід зазначити, що держави вже мають політику як у фізичному, так і в цифровому світі. Іноді вони навіть суперечитимуть один одному в майбутньому, як би парадоксально це не звучало [80]. Стратегія кібербезпеки є інструментом для досягнення цілей національної безпеки. Поряд з технологічним розвитком, технічною підтримкою та підготовкою кваліфікованого персоналу частиною цієї стратегії є правове регулювання [89].

Кіберпростір має свою специфіку, яка визначається миттєвим поширенням інформації, її доступністю та відсутністю кордонів (або майже їх відсутністю, залежно від політики існуючих сьогодні держав) [91]. Це значно ускладнює його регулювання та реагування на виклики і небезпеки.

Першим кроком у забезпеченні безпеки критичної інфраструктури вважається створення в 1996 р. Президентом Сполучених Штатів Америки Комісії із захисту критичної інфраструктури. Вона була спрямована на розробку національної стратегії захисту критичної інфраструктури від фізичних та кіберзагроз [99].

У більшості країн світу подібні стратегії включають:

транспортну мережу та енергетику;

логістику;

засоби масової інформації, комунікації;

міжбанківські розрахунки;

об’єкти функціонування органів державної влади;

підприємства загальнодержавного значення;

аварійні служби;

систему життєзабезпечення мегаполісів [100, 101].

Як влучно зазначає дослідниця Бакалінська О., кіберпростір став могутнім тунелем для виникнення, поширення та трансформації інформації. Водночас він бере на себе функції «серця» економіки та її «двигуна». Це також платформа для нових соціальних зав'язків, комунікацій і спільнот. Вже зараз можна говорити про появу нового типу держави – віртуальної [95].

У Декларації Комітету Міністрів Ради Європи про принципи управління Інтернетом, прийнятій 21 вересня 2011 року, сформульовано 10 основних принципів:

1. Верховенство права та розвиток демократії;

2. Багатостороннє управління;

3. Обов'язки держав;

4. Допомога споживачам цифрового контенту;

5. Універсальність Інтернету;

6. Цілісність Інтернету (цей принцип включає безпеку, стабільність, надійність і стійкість Інтернету, а також його здатність розвиватися, мають бути ключовими цілями управління Інтернетом);

7. Децентралізоване управління (органи, відповідальні за технічні та управлінські аспекти Інтернету, а також приватний сектор, повинні зберігати свою провідну роль у технічних та операційних питаннях, забезпечуючи при цьому прозорість. Крім того, вони повинні нести відповідальність перед світовою спільнотою за дії, що впливають на державну політику);

8. Архітектурні принципи (безбар'єрність Інтернету);

9. Відкрита мережа;

10. Культурне та мовне різноманіття, сприяння розвитку місцевого контенту [102].

В Європейському Союзі є низка організацій, які прагнуть розвивати культуру кібербезпеки, зокрема через правові норми та гарантії, що містяться в нормативних документах, які стосуються:

безпеки мережі та інформації;

боротьба з кіберзлочинністю;

методів, інструментів та засобів регулювання [92].

Стратегія Ради Європи щодо управління Інтернетом, прийнята 30 березня 2016 року, є продовженням нормативно-правового регулювання діяльності та розвитку віртуального простору. Зокрема, в ній виділяються моменти, які зосереджуються на кібербезпеці та захисті конфіденційності користувачів Інтернету. Це питання спільної відповідальності, консолідації та концентрації зусиль для боротьби з екстремізмом, радикалізацією, кіберзлочинністю, експлуатацією, переслідуванням і залякуванням людей за допомогою віртуальних технологій. Особлива увага приділяється захисту від сексуального насильства, експлуатації дітей в Інтернеті, протидії торгівлі органами та людьми, а також продажу підроблених ліків і препаратів. Рада Європи зосереджується на сприянні приєднанню країн до низки міжнародних законодавчих ініціатив у цій сфері, щоб забезпечити ефективне виконання цих пріоритетів. Подальші кроки також включають встановлення спільної політики та принципів управління Інтернетом, особливо в сфері інформаційної та мережевої безпеки. Проблеми перехоплення даних, захисту персональних даних, прав людини у віртуальному просторі також залишаються актуальними [103].

У прийнятій 16 грудня 2020 року Генеральною Асамблеєю ООН Резолюції A/RES/75/176 «Право на приватність у цифрову епоху» узагальнено попередні розробки міжнародного права в сфері кібербезпеки та конфіденційності у віртуальному світі. Резолюція також зосереджена на штучному інтелекті [105]. Як зазначалося вище, людству ще належить усвідомити і відчути на практиці переваги і небезпеки віртуального світу.

Як зазначають чимало дослідників, вплив штучного інтелекту на захист прав людини, трансформацію державного управління та соціальних відносин

може мати далекосяжні, непередбачувані наслідки, не в останню чергу пов’язані з приватністю. Це пов’язано насамперед з відсутністю відповідних гарантій, коли штучний інтелект, який швидко навчається, може впливати на прийняття рішень, які вплинуть на економічні, соціальні та культурні права людини. Це також впливає на принцип недискримінації.

Особлива небезпека таких непередбачуваних результатів полягає в:

обробці персональних та біометричних даних;

незаконний або несвідомий збір даних, перехоплення та несанкціонований доступ до персональних даних;

незаконне використання біометричних технологій.

Усі ці загрози та виклики можуть призвести до порушення права на приватне життя, свободу вираження поглядів, свободу поглядів і переконань, свободу мирних зібрань і об’єднань, а також права на релігійну свободу. Більш того, це суперечить фундаментальним демократичним засадам суспільства.

У Резолюції наголошується, що всі права, якими люди володіють у повсякденному житті, включаючи право на приватність, мають поширюватися і на віртуальний простір. Ще одним занепокоєнням є поширення дезінформації та неправдивої інформації, особливо в соціальних мережах. Така дезінформація спрямована на поширення расизму, ксенофобії, негативних стереотипів і стигматизації. Вона також містить заклики до насильства, дискримінації, ненависті та ворожнечі у всіх її проявах. Держави та комерційні організації несуть відповідальність за дотримання норм міжнародного права та національного законодавства. Їх закликають поважати прийняті норми та тлумачення конфіденційності, здоров’я людини, захисту даних тощо. Резолюція підтверджує численні правила та закони щодо конфіденційності та захисту даних, які вже були ухвалені. Особливо це стосується захисту прав дітей. Необхідно гармонізувати міжнародну та національну законодавчу базу та регулярно контролювати та вдосконалювати практики, процедури та законодавство для забезпечення права на приватність у віртуальному світі. Це вимагатиме використання наявних і розроблених ресурсів і механізмів, а також

створення нових, неупереджених, неупереджених та ефективних судів, парламентський нагляд та прозоре звітування щодо збору, розповсюдження та зберігання персональних даних.

У Резолюції йдеться про необхідність подальшого розвитку ефективного законодавства як на міжнародному, так і на національному рівнях, що стосується приватності у віртуальному просторі. Враховуючи стрімкий розвиток віртуальних технологій, штучного інтелекту та їх вплив на життя людей, суспільства та держави, Резолюція зазначає необхідність подальшого розвитку правової бази, пов'язаної з кібербезпекою та захистом приватності у віртуальному просторі [104].

9 березня 2021 року Європейська Комісія опублікувала Повідомлення «Цифровий компас 2030: європейський шлях до цифрового десятиліття» [106], в якому визначено цілі та завдання розвитку Європи до 2030 року в сфері цифрових технологій, а також у формуванні сталої економіки замкнутого циклу. Крім того, Цифровий компас 2030 враховує зміну клімату, зосереджуючись на добробуті та процвітанні людини в контексті розвитку цифрової культури в глобальному масштабі [96].

На сьогодні Україною прийнято (ратифіковано) на законодавчому рівні низку рішень щодо правового регулювання кібербезпеки та конфіденційності у віртуальному просторі в Україні. Зокрема, 7 вересня 2005 року Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність від 23 листопада 2001 року. Зокрема, цим документом визначено заходи, які належать до компетенції національного законодавства:

встановлення кримінальної відповідальності за навмисний доступ до цілої комп'ютерної системи або її частини без права на це;

встановлення кримінальної відповідальності за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування;

встановлення кримінальної відповідальності за навмисне пошкодження, знищення, погіршення, зміну або приховування комп’ютерної інформації без права на це;

встановлення кримінальної відповідальності за навмисне серйозне перешкоджання функціонуванню комп’ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп’ютерних даних без права на це;

встановлення кримінальної відповідальності за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними;

встановлення кримінальної відповідальності за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

a. будь-якого введення, зміни, знищення чи приховування комп’ютерних даних,

b. будь-якого втручання у функціонування комп’ютерної системи,

з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи;

встановлення кримінальної відповідальності за навмисне вчинення, без права на це, наступних дій:

a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп’ютерних систем;

b. пропонування або надання доступу до дитячої порнографії за допомогою комп’ютерних систем;

c. розповсюдження або передача дитячої порнографії за допомогою комп’ютерних систем;

d. здобуття дитячої порнографії за допомогою комп’ютерних систем для себе чи іншої особи;

e. володіння дитячою порнографією у комп’ютерній системі чи на комп’ютерному носії інформації;

встановлення кримінальної відповідальності за порушення авторських прав;

встановлення кримінальної відповідальності за порушення суміжних прав.

Конвенція також визначає корпоративну відповідальність, співучасть, санкції та заходи, пов’язані з недотриманням положень Конвенції [107].

Фундаментальною основою кібербезпеки України є Конституція України [108] та низка законів і підзаконних нормативно-правових актів.

У Статті 17 Конституції України сказано, що захист інформаційної безпеки є однією з найважливіших функцій держави і справою всього Українського народу [108].

Стаття 18 Конституції України вимагає, щоб зовнішньополітична діяльність України була спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права [108].

Згідно зі статтями 106 та 107 Конституції України, Президент відіграє важливу роль у забезпеченні національної безпеки, до якої відноситься й кібербезпека, зокрема як Голова Ради національної безпеки і оборони, той, хто відповідає за національну безпеку і оборону і хто вносить до Парламенту подання про призначення на посаду та звільнення з посади Голови Служби безпеки України [108]. Рада національної безпеки і оборони є координаційним органом з питань національної безпеки і оборони при Президентові України. Президент особисто формує персональний склад Ради національної безпеки і оборони. Діяльність Ради національної безпеки і оборони України визначається Законом про Раду національної безпеки і оборони, який уповноважує її розглядати питання, визначені Стратегією національної безпеки України [108].

Указом Президента України від 28 грудня 2021 року № 685 затверджено Стратегію інформаційної безпеки, схвалену Рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року. Згідно з цим документом,

завдання, визначені Стратегією, мають бути реалізовані до 2025 року [109]. Їх практичне вирішення потребує:

консолідації роботи з вдосконалення відповідної нормативно-правової бази, техніко-технологічних розробок, кадрових рішень, системної медіаграмотності на всіх рівнях освіти;

стабільної системної взаємодії з іноземними партнерами з урахуванням теоретичного та практичного досвіду міжнародної спільноти.

Практична реалізація цієї мети потребує вдосконалення відповідного законодавства та моніторингу виконання завдань Стратегії інформаційної безпеки.

Нова редакція Стратегії кібербезпеки України, схвалена Рішенням Ради національної безпеки та оборони України від 14 травня 2021 року та затверджена Указом Президента України від 26 серпня 2021 року № 447, для формування нової якості національної системи кібербезпеки визначає такі цілі:

1. Дієва кібероборона - Україна створить та забезпечить розвиток (у тому числі кадрово та технологічно) підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформує належну правову, організаційну, технологічну модель їх функціонування та застосування, забезпечить ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності;

2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму – Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян;

3. Ефективна протидія кіберзлочинності – Україна забезпечить набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів;

4. Розвиток асиметричних інструментів стримування – Україна створить необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу приватного сектору;

5. Національна кіберготовність та надійний кіберзахист – Україна запровадить і реалізує чіткі та зрозумілі для всіх заінтересованих сторін заходи щодо національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України. Україна посилить кіберготовність, що полягатиме у здатності всіх заінтересованих сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури. Україна створить національну систему управління інцидентами;

6. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки – Україна проведе докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, а також здійснить заходи щодо збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створення національних інформаційних систем, платформ і продуктів. Вітчизняний науково-технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Цифрові навички, кіберобізнаність

щодо сучасних кіберзагроз та протидії ним стануть невід'ємними елементами освіти кожного громадянина України;

7. Безпечні цифрові послуги – Україна забезпечить досягнення балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійність та безпеку цифрових послуг протягом усього їхнього життєвого циклу;

8. Зміцнення системи координації – Україна створить умови для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів, скоординує діяльність усіх заінтересованих сторін задля подолання надзвичайних (кризових) ситуацій у кіберпросторі;

9. Формування нової моделі відносин у сфері кібербезпеки – Україна запровадить сервісну модель державної участі у заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки;

10. Прагматичне міжнародне співробітництво – Україна спрямує відносини з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками. Україна забезпечить активну участь у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Забезпечення координації з міжнародними партнерами здійснюватиметься Міністерством закордонних справ України [4].

Формування та розвиток законодавчої бази, пов’язаної з кібербезпекою та конфіденційністю у віртуальному просторі в Україні, випливає з євроінтеграції нашої країни та реалій російсько-української війни. Важливо усвідомлювати, що

для ефективного правового регулювання кіберпростору недостатньо лише законодавчих рішень. В умовах дедалі більшої атомізації суспільства свідомість громадян та рівень їх медіаграмотності відіграють суттєву роль у формуванні розуміння кіберзагроз та протидії їм.

Висновки до розділу 1

Показано, що термін «кібербезпека» набуває все більшого поширення в останні часи, водночас, використання цього терміну та визначення його контексту в різних наукових працях і нормативно-правових документах значно різняться між собою.

У результаті теоретичного та правового аналізу наукової літератури та законодавства, проаналізовані нормативно правові джерела та праці вчених, узагальнено науковий матеріал щодо визначень терміну «кібербезпека», які наведені в різних законодавчих та нормативно-правових актах, а також науковій літературі. Встановлено, як ключові, такі його аспекти:

використання комп’ютерних систем і телекомунікаційних мереж;

нейтралізація негативних інформаційних впливів на технологічному рівні;

захист основоположних прав і життєво важливих інтересів людини і громадянина, суспільства і держави в кібернетичному середовищі, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем;

нейтралізація загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах;

спрямованість на досягнення і утримання потенційними протиборчими сторонами переваги в протидії новим загрозам безпеці для власних об’єктів критично важливої інформаційної і кіберінфраструктури.

Проведено наукове дослідження організаційно-адміністративних засад системи забезпечення кібербезпеки та кіберзахисту з урахуванням сучасної нормативної бази в цій сфері.

Показано, що кібербезпека являє собою правовий інститут, тобто цілу систему юридичних норм, у вигляді правового об’єкта якого розглядають регулювання безпечного стану обробки інформації у кіберпросторі. Тоді, як під кіберзахистом слід розуміти систему (механізм) засобів різного характеру (правового, організаційного, ресурсно-фінансового, програмно-технічного та іншого характеру), за допомогою яких здійснюється діяльність у кіберпросторі з охорони певних його об’єктів від протиправних посягань (наприклад, кіберзлочинів) і створення перешкод у реалізації загроз кримінального характеру.

Виходячи із зазначеного визначено основні суб’єкти та об’єкти кібербезпеки та кіберзахисту.

Важливо зазначити, що правове регулювання кібербезпеки та конфіденційності у віртуальному просторі може буде ефективним у тому випадку, якщо цей процес буде динамічним та різноспрямованим.

В Україні також триває процес правового забезпечення кібербезпеки та конфіденційності в Інтернеті. Україна ратифікувала низку міжнародних документів з цього питання та має власну законодавчу базу. Законодавчий процес у цій сфері потребує подальшого вдосконалення визначень термінів «кібербезпека», «кіберзлочинність», «приватність у віртуальному просторі», методології правового регулювання віртуального світу.

Крім того, необхідно пам’ятати про безпрецедентний розвиток віртуальних технологій, штучного інтелекту, цифрової культури, зростання рівня кіберзлочинності та вплив віртуального світу на всі без винятку сфери життя людини, суспільства та держави.

Законотворчий процес має враховувати існуючі норми міжнародного права та чинне національне законодавство, а також актуальні виклики та

прогнозувати перспективи позитивних та негативних наслідків віртуального впливу на реальне життя.

Юридичне забезпечення кібербезпеки та конфіденційності у віртуальному просторі є важливим чинником розвитку інтернет-економіки. Цей сектор економічного зростання (насамперед віртуальна торгівля) набув значного розвитку під час тривалого карантину, а в Україні – також і через повномасштабне вторгнення росії. Тому цей напрямок законотворчої діяльності є перспективним за актуальністю та швидкістю реагування на виклики часу.

Явище кібербулінгу (кібернасильства) як один з наслідків недотримання права на приватність потребує подальшого вивчення, аналізу та розвитку законодавчої бази. Наразі дослідженням проблеми кібербулінгом, окрім юристів, займаються також психологи, соціологи, лікарі та педагоги. Іншими словами, це міждисциплінарна проблема, яка потребує постійного моніторингу та взаємодії між фахівцями різних галузей.

Сьогодні віртуальний світ відтворює відносини у фізичному житті. Те саме стосується правовідносин у цифровому форматі. Зокрема, сформовано систему правовідносин між споживачами та постачальниками послуг Інтернету, електронних платежів, зв’язку, надання адміністративних послуг через цифрові додатки, електронного урядування, правоохоронних функцій. Ці сфери так чи інакше регулюються національними законами та міжнародними договорами. Водночас існує мережевий етикет (поняття, що виникло у 1980-х роках – англ. «net» і фр. «etiquette») – культура віртуального спілкування, яка передбачає дотримання наступних категорій:

емоційний контакт (емотикони, емодзі, форми звернення на «ти» або «ви», ігнорування агресивних випадів, усталених форм вітання та прощання в офіційному листуванні, тощо);

технічні особливості віртуального спілкування (правила цитування, форма, розмір і колір шрифту, особливості форматування тексту, оформлення презентації тощо);

адміністративні (допустимість чи недоречність флейму (емоційного доказу своєї позиції), реклами або її заборона, тематика груп тощо).

До порушень мережевого етикету належать:

персоналізація;

словесні та візуальні образи;

відхилення від теми спілкування;

надмірна самореклама;

плагіат;

аморальні висловлювання тощо.

Отже, можна твердо стверджувати, що нові технологічні реалії, міжнародні відносини та геополітична ситуація стали серйозними викликами для системи правових відносин у сучасному світі. Міжнародні правові норми та національне законодавство відіграють наздоганяючу роль у системах кібербезпеки та конфіденційності віртуального простору. Це ще більше посилює загрозу кіберзлочинності. Нормативно-правова база віртуальної сфери, як в Україні, так і в усьому світі, має встигати за розвитком технологій.

Проте самого правового регулювання недостатньо для вирішення цих проблем. Іншим важливим фактором кібербезпеки та конфіденційності у віртуальному світі є кібергігієна, медіаграмотність і кібердетоксикація. Усе це повинно стати частиною нашого життя з дитинства.

РОЗДІЛ 2. ЗМІСТ ТА ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЩОДО ПРОТИДІЇ ОКРЕМИМ ВИДАМ КІБЕРЗАГРОЗ У СУЧАСНОМУ СВІТІ

2.1. Визначення правового статусу кібератак та кібервійськових операцій

Станом на теперішній час, значно почастішали кібератаки як в Україні, так і в інших державах. Розвиток впорядкування суспільних відносин у напрямку цифровізації є притаманним для багатьох розвинутих країн світу. Однак, для українського суспільства процес нормативної та інституціональної форми трансформації триває в умовах російсько-української війни, яка однозначно встановила єдиний напрямок суспільних інтересів та консолідацію українського суспільства.

В умовах формування державних інститутів кібербезпеки та становлення норм права, щодо стабілізації політичних процесів, формується система поглядів на позитивні та негативні стилі поведінки учасників політичного процесу в кіберпросторі, можливі допустимі межі їх активності та створення інформаційної публічної бази, яка не шкодить інтересам країни.

Для створення комплексного уявлення про забезпечення кібербезпеки, заслуговують на увагу праці щодо інформаційної безпеки, таких вчених, як: Д. В. Дубов, В. О. Жадько, Ю. В. Завгородня, Л. І. Кормич, О. І. Харитоненко, Ю. С. Полтавець та інших. Міжнародний досвід щодо реакції на кіберконфлікти, кібератаки досліджується й у працях зарубіжних вчених, а саме: Ю. Тор, Р. Горва, М. Смеетс, Т. Рід, Д. Пуйвельде, А. Брантлі тощо. Водночас, попри значну кількість таких наукових праць і накопиченого на даний час теоретичного матеріалу, слід визнати, що питання визначення правового статусу кібератак та кібервійськових операцій до сих пір досліджено лише фрагментарно. Отже, існує потреба в проведені відповідного комплексного наукового дослідження.

Відомий науковець М. Шмітт надає таке визначення кібератаки – це кібероперація, будь то наступальна чи оборонна, яка, як обґрунтовано очікується, спричинить поранення чи смерть людей або пошкодження чи руйнування об’єктів [227].

Основи адміністративно-правового регулювання протидії кіберзагрозам містяться у:

Законі України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР [5];

Доктрині інформаційної безпеки України, схваленої Рішенням Ради національної безпеки та оборони України від 29 грудня 2016 року та затвердженої Указом Президента України від 25 лютого 2017 року № 47 [1];

Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [2];

Законі України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII [3];

Стратегії кібербезпеки України, схваленої Рішенням Ради національної безпеки та оборони України від 14 травня 2021 року та затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4],

що стали підґрунтям для сприйняття кібернетичної площини, як повноцінної сфери, яка потребує захисту.

Окрім цього, даним законодавством надано нормативне визначення поняттям «кіберзлочину», «кібератаки», «критичної інформаційної інфраструктури» та ін. Тобто, визначено, на нормативному рівні, конкретні форми впливу небезпеки в кібернетичній площині.

Зокрема, відповідно до пункту 4 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення

конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [2].

Згідно з пунктом 8 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

Ціннісними формами побудови кіберсистеми є уповноваження державних інституцій, які будуть регулятивною та безпековою основою розвитку цифровізованого суспільства. У сфері системи виконавчої влади такою конструктивною основою є:

Міністерство культури та стратегічних комунікацій України,

Міністерство закордонних справ України,

Національна рада України з питань телебачення і радіомовлення,

Державне агентство України з питань кіно,

Державний комітет телебачення і радіомовлення України,

які створюють умови для реалізації політичних цілей та завдань в країні [6].

Окрім того, координацію діяльності органів виконавчої влади з метою реалізації Доктрини інформаційної безпеки України, схваленої Рішенням Ради національної безпеки та оборони України від 29 грудня 2016 року та затвердженої Указом Президента України від 25 лютого 2017 року № 47, [1] та гарантування національної безпеки в інформаційній сфері здійснює Рада національної безпеки та оборони України.

Державною службою спеціального зв'язку та захисту інформації України оприлюднено статистику кібератак на українську критичну інформаційну інфраструктуру. Відповідно до якої протягом 15 - 22 березня 2022 р. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зафіксувала 60 кібератак. З них:

уряд та місцеві органи влади – 11,

фінансовий сектор – 6,

телеком та програмне забезпечення – 4,

сектор безпеки та оборони – 8,

комерційний сектор – 6,

енергетика – 2,

інше – 22 [7].

Основними характерними ознаками кіберконфліктів, які відмежовують їх від інших загроз є:

просторові межі,

можливість глобального розвитку в найкоротші терміни,

відсутність суб'єктної прив'язки до конкретних дій в кіберпросторі (як правило кібератаками займаються компетентні особи з відповідного розпорядження суб'єктів протиборства).

Сучасна політика держави зосереджена на спрощенні бюрократичної системи, економії часу для будь-яких реєстраційних процесів, ефективного користування соціальними гарантіями. Окрім позитивних аспектів існує ряд загроз щодо кібератак для оприлюднення персональних даних, можливості їх використання та видалення з баз даних. Саме такі загрози стоять перед сучасним сектором інформаційної політики з метою захисту та збереження персональної інформації [8].

Оприлюднення персональних даних є однієї з головних небезпек, які можуть бути відкриті в кіберпросторі, оскільки сюди можуть відноситись:

данні про членів сім'ї політично-владних суб'єктів (дружина, діти, батьки);

данні про наявність рухомого та нерухомого майна в активного політичного діяча та його членів сім'ї;

дані про економічні транзакції, які мають сумнівно-незаконний характер, та суми, які перевищують офіційні доходи особи,

та інші відомості, які можуть нашкодити діяльності політичного діяча.

Адже, можливість створювати безлад в системі інформації, заводить суспільство в панівні настрої, а тому є тим негативним чинником, якого прагнуть сторони протидії, тобто зміна свідомості відносно сприйняття політичної сили чи політичного лідера.

Окрім того, трансформація конфліктної активності в кіберпростір провокує швидку глобалізацію конфронтації з можливістю залучення міжнародних учасників, які мають вплив на міжнародні процеси. В сучасному світі, на думку Н. Ржевської, «найефективнішим інструментарієм інформаційно-психологічного впливу на потенційні об'єкти конфлікту є засоби масової інформації. Інформаційне середовище геополітичного конфлікту формується і підтримується діяльністю засобів масової інформації. Найчастіше саме засоби масової інформації є головною ланкою в інформаційному полі міжнародного конфлікту. Бурхливе зростання тимчасових електронних засобів масової інформації та прискорений розвиток інформаційних технологій наблизили до реальності проєкти створення комплексних інформаційних систем найвищого рівня» [9].

Звичайно, роль інформаційних каналів досить актуальна, оскільки сучасні міжнародні конфлікти переважно реалізуються в медійному просторі, у формі боротьби за усвідомлення національних та міжнародних політичних процесів. А тому, вагому роль відіграють нормативні процеси, що є механізмом реалізації публічної риторики політичних лідерів, демонстрація їх вектору політики та рівень відповідності слів і дій. Якщо конфлікт заходить у крайню фазу свого розвитку, військове протиборство, то Н. Ржевська вдало відзначає про роль комунікаційних ресурсів поряд з військовою технікою, яка є важливою для

сприйняття суспільством, тому військові дії підкріпляються інформаційними війнами [9].

Враховуючи особливості кіберпростору, кібератаки як форма політичного кіберконфлікту можуть призводити до міжнародних конфліктів, що охоплюють територіально визначені зони. З одного боку, прорахувати межі та наслідки таких атак в умовах глобальної взаємодії інформаційних інфраструктур окремих країн вкрай складно, а з іншого – складність ідентифікації джерела та висока ймовірність неправильної оцінки ситуації можуть призвести до непропорційних індивідуальних заходів з боку постраждалої сторони. Це може призвести до відкритого військового конфлікту із застосуванням звичайних озброєнь [10].

Окрім того, не варто виключати психологічні технології, які вдало діють в інформаційній площині. Коли в умовах повного інформаційного хаосу відбувається процес формування керованого переговорного стану. Інформаційні та психологічні технології можуть перетворити міжнародні конфлікти на мир [9].

Оскільки, в інформаційному суспільстві формується уявлення про кіберконфлікт, негативні наслідки його ескалації. У зв’язку з цим, можемо відзначити, що інформаційне протиборство здійснюється для впливу на масову свідомість, за допомогою спотворення реальності щодо наслідків конфронтації сторін. Результатом кіберконфлікту можуть бути політичні рішення глобального значення. Звичайно, результати кіберконфліктів мають вагомий вплив на процес прийняття найважливіших у світі політичних рішень. Політична еліта використовує результати конфронтації, як площину для легітимації персональних рішень та реалізації цілей геополітичного рівня.

Тому, трансформація у військових атак у кібервійськові є проявом осучаснення ведення військових дій та реалізації глобалізаційних змін. Тому, кібервійськові атаки стають невід’ємною формою існування демократичного устрою. У зв’язку з цим, виникає потреба у формуванні системи реагування органами управління, на небезпеку, яку вони можуть нести суспільству.

Протягом останніх років світ став свідком шквалу досить серйозних російських кібератак, спрямованих на українську інфраструктуру та цивільні

об’єкти, які розгортаються з невпинною швидкістю та становлять постійну загрозу для цивільних осіб та критичної інфраструктури в Україні. Оскільки росії не вдається досягти бажаних результатів на полі бою, кількість і серйозність кібератак продовжуватимуть зростати.

Відколи в 2014 році почалося вторгнення росії в Україну, росія здійснює багаторічне бомбардування кібератаками Україну, яких раніше не було в історії. Лише хакери Sandworm (групу хакерів, якою керує військова частина 74455, підрозділ кібервійни ГУ ГШ ЗС рф) тричі намагалися відключити електроенергію в Україні. Принаймні дві з них вдалося. Цілеспрямованими атаками знищено мережі засобів масової інформації, приватних компаній та державних установ. А в 2017 році було випущено деструктивне шкідливе програмне забезпечення NotPetya, що саморозповсюджується, яке вразило комп’ютерні мережі сотні організацій по всій Україні, а згодом і багато інших по всьому світу, завдавши рекордних збитків на суму 10 мільярдів доларів США.

З початком широкомасштабного вторгнення, яке росія розпочала 24 лютого 2022 р., хакери, які спонсоруються кремлем, розв’язали нову широку кампанію деструктивного злому проти сотень українських цілей, часто ретельно скоординовану з фізичною військовою тактикою. Цей новий шквал включав кібератаку, під час якої хакери ГРУ атакували супутникові системи Viasat, відключивши широкосмугове з’єднання в Україні та Європі, включно з підключенням тисяч вітрових турбін у Німеччині [217].

Наприкінці березня 2022 року група юристів-правозахисників і слідчих з Центру прав людини при Школі права Каліфорнійського університету в Берклі надіслала офіційний запит до Офісу прокурора Міжнародного кримінального суду в Гаазі. Він закликає Міжнародний кримінальний суд розглянути переслідування російських хакерів за військові злочини, а саме за їх кібератаки в Україні. Зокрема, група міжнародних кримінальних розслідувань Центру прав людини при Школі права Каліфорнійського університету в Берклі в своєму запиті вказує на Sandworm і на дві найбільш кричущі кібератаки Sandworm:

відключення електроенергії, які ці хакери спричинили, атакуючи електромережі в Західній Україні в грудні 2015 р. та в Києві в 2016 р., що вплинуло на сотні тисяч мирних жителів. Юристи виділили ці дві атаки з юридичних і практичних причин: вони вже були ретельно розслідувані та покладені на хакерів Sandworm через детективну роботу як у приватному секторі, так і в Уряді Сполучених Штатів Америки, зокрема в жовтні 2020 р. Міністерство юстиції США висунуло звинувачення шістьом хакерам цього угруповання [225]. Кібератаки сталися в перші роки війни росії в Україні, під час активних бойових дій у східному регіоні країни, що дозволяє стверджувати, що вони відбулися в контексті військового конфлікту і, таким чином, є військовим злочином. Вони мають чітку цивільну ціль, враховуючи, що на момент відключення електроенергії ні в Західній Україні, ні в Києві військові дії не велися. Вони мали чіткий і прямий фізичний результат, що робить їх еквівалентними фізичним нападам, які трибунали з військових злочинів висували в минулому [218].

Крім цього, в запиті вказується на серйозність атак Sandworm на цивільні електромережі. Зокрема, 23 грудня 2015 р. за допомогою троянської програми BlackEnergy3 російськими хакерами було відключено близько 30 підстанцій Прикарпаттяобленерго, в зв'язку з чим більш 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Під час інциденту 2016 року в Києві хакери використали зловмисне програмне забезпечення, відоме як Industroyer або Crash Override, щоб автоматично викликати це відключення електроенергії. Незважаючи на те, що відключення електроенергії в столиці України тривало лише близько години, аналіз показав, що компонент шкідливого програмного забезпечення, призначений для вимкнення систем безпеки, був розроблений для фізичного руйнування електрообладнання, і вийшов з ладу лише через неправильну конфігурацію шкідливого програмного забезпечення [218].

Документ групи юристів Каліфорнійського університету в Берклі надіслано відповідно до статті 15 Римського статуту [30], який наділяє

Міжнародний кримінальний суд повноваженнями, дозволяючи рекомендації від неурядових організацій. Він просить прокурора Міжнародного кримінального суду К. Хана «розширити сферу свого розслідування, щоб охопити кібердомен на додаток до традиційних сфер війни – наземної, повітряної, морської та космічної – з огляду на історію ворожої кіберактивності російської федерації в Україні». У запиті визнається, що звинувачення проти Sandworm будуть першим випадком «військових кіберзлочинів», коли-небудь висунутим Міжнародним кримінальним судом. В ньому стверджується, що прецедент допоміг би не тільки добитися справедливості для тих, хто постраждав від кібератак Sandworm, але й стримати майбутні, потенційно гірші кібератаки, які вплинуть на критично важливу цивільну інфраструктуру по всьому світу. Л. Фрімен, директор із технологій, права та політики Центру прав людини при Школі права Каліфорнійського університету в Берклі стверджує, що єдиний спосіб правильно розслідувати та зрозуміти цей конфлікт — це побачити не лише те, що відбувається у фізичному світі, а й те, що відбувається в кібернетичному та інформаційному просторах, і це те, на що слідчі військових злочинів ніколи не звертали уваги [218].

У березні 2023 р. Центр прав людини Школи права Каліфорнійського університету в Берклі подав друге звернення за статтею 15 Римського статуту [30] до Офісу прокурора Міжнародного кримінального суду щодо кібервійни в російсько-українському конфлікті, в якому представлено обвинувачення п’яти російських кібератак на критичну інфраструктуру України як військових злочинів через те, що вони були спрямовані на цивільні об’єкти або мали невибірковий характер [219].

Описані в цьому зверненні Центру кібератаки відповідають необхідному порогу прийнятності. Запропонована справа складається з п’яти інцидентів, пов’язаних з найнебезпечнішими кіберзагрозами, з якими стикається сьогодні світ: зловмисне програмне забезпечення, яке порушує роботу систем, що контролюють операційні технології; та зловмисне програмне забезпечення, яке за своєю конструкцією є невибірковим. Кібератаки, задокументовані Центром

прав людини при Школі права Каліфорнійського університету в Берклі, завдали значної шкоди критичній інфраструктурі, такій як електромережі, мережі супутникового зв’язку та комп’ютерні системи. Вони також вплинули на мільйони прямих і опосередкованих жертв як в Україні, так і за її межами. Ці факти демонструють, що кібервійна росії проти України відповідає порогу прийнятності Міжнародного кримінального суду [219].

До того ж, Міжнародний кримінальний суд у роз’ясненні «Елементи злочинів» уточнює, що військові злочини є особливо тяжкими, коли вони є «частиною великомасштабної кампанії» або вчинені «відповідно до плану чи політики» [220].

Відповідно до Політики відбору та пріоритетності справ Офісу прокурора Міжнародного кримінального суду від 15 вересня 2016 року встановлено принципи, згідно з якими Офіс прокурора здійснює свою дискрецію, враховуючи «масштаб, характер, спосіб вчинення та вплив злочинів» під час оцінки. Політика визначає тяжкість як «переважаючий критерій відбору справ» [221].

Отже, коли російські урядові хакери зруйнували електромережу Івано-Франківська взимку 2015 року, Київську енергомережу взимку 2016 року та третю енергомережу у 2022 році, це були не просто атаки на три електромережі, а атаки на кожну домівку, офіс, лікарню та критичну інфраструктуру, яка працює від цієї електроенергії. Як стверджується в заяві Центру прав людини при Школі права Каліфорнійського університету в Берклі: «це були напади на опалення, яке зігріває людей взимку; охолодження, яке не псує їжу; світлофори, що забезпечують громадську безпеку; фінансові послуги, які захищають засоби існування людей і підтримують обмін найважливішими товарами та послугами; медичні установи, на які люди покладаються для свого здоров'я; системи, які ізолюють небезпечні ядерні та хімічні об'єкти від міських центрів; а також транспорт, комунальні послуги та зв’язок, які з’єднують українську громаду одна з одною та зовнішнім світом». Таким чином, у справі проти російських кібервійськ йдеться про правовий захист цивільної критичної інфраструктури, яка підтримує повсякденне життя в епоху цифрових технологій [219].

Так, С. Кальтаджіроне роз'яснює, що сучасні суспільства щодня покладаються на промислові системи управління, які фактично є «прихованими комп'ютерами» та мережами, що лежать в основі сучасного життя. Ці системи підтримують виробництво електроенергії, «підтримуючи опалення та економіку», управляють обладнанням, що запобігає повеням, «захищають життя та підтримують мільйони акрів придатних для використання сільськогосподарських угідь», а також забезпечують безпечну та ефективну обробку їжі, «годуючи більше людей та запобігаючи хворобам». Без цих промислових систем мільйони чи більше людей можуть страждати від відсутності медичної допомоги, їжі, питної води, опалення взимку та охолодження влітку [222].

Н. Брубакер та інші детально описують, що зловмисне програмне забезпечення, націлене на промислові системи управління, представляє «виключно рідкісну та небезпечну здатність кібератак». Зловмисне програмне забезпечення, націлене на промислові системи управління, створено для атаки на системи, що керують операційними технологіями, на відміну від інформаційних технологій. З іншого боку, кібератаки на операційні технології можуть призвести до збоїв, саботажу та, що найважливіше, фізичного знищення [223].

На думку Л. Гізель і Л. Олейніка, кібератаки, спрямовані на фізичне знищення, є найбільш явним порушенням норм міжнародного гуманітарного права, якщо вони відбуваються в контексті збройного конфлікту і спрямовані проти цивільних об'єктів. Оскільки, спеціалізовані кібероперації проти промислових систем управління та інших операційних технологій можуть спричинити «навмисні чи ненавмисні фізичні ефекти (наприклад, руйнування чи вибухи), які можуть призвести до втрати людського життя (прямо чи опосередковано)» [224].

На сьогоднішній день розроблено лише кілька відомих можливостей шкідливого програмного забезпечення, націлених на промислові системи управління: Stuxnet, Triton, Havex, BlackEnergy3, Industroyer, Industroyer2 та Incontroller. Через необхідні технічні навички, час та фінансові ресурси,

необхідні для створення цієї рідкісної породи зловмисного програмного забезпечення, усі вони пов’язані з державними органами та установами. Окрім Stuxnet, яке використовувалося на іранських центрифугах для уповільнення збагачення урану і пов’язане зі Сполученими Штатами Америки та Ізраїлем, усі інші вважаються створеними російським урядом і державними кіберлабораторіями. Причому, останні чотири – BlackEnergy3, Industroyer, Industroyer2 та Incontroller – виникли під час війни в Україні. Крім того, за останні роки зловмисне програмне забезпечення, націлених на промислові системи управління, стало складнішим, вдосконаленим і простішим у використанні. Таким чином, цей тип зловмисного програмного забезпечення розвивається в небезпечному напрямку з кожною новою ітерацією, яка стає все більш складною [219].

Другою зростаючою загрозою є зловмисне програмне забезпечення, яке не може відрізнити цивільні об’єкти від військових цілей і яке не можливо контролювати після його розгортання, що аналогічно біологічній чи хімічній зброї, що переміщується по повітрю, або наземним мінам, закладеним у землю. Невибіркові кібератаки з використанням деструктивного зловмисного програмного забезпечення, яке саморозповсюджується, наприклад, NotPetya, або зловмисного програмного забезпечення, яке спричиняє надмірно широкі наслідки. Оскільки Інтернет складається з взаємопов’язаних мереж, невелика локалізована атака може перерости у всесвітню катастрофу, як це сталося з атакою NotPetya від Sandworm [219]. Як зазначено в Обвинувальному висновку Міністерства юстиції Сполучених Штатів Америки від 15 жовтня 2020 року в кримінальній справі № 20-316, під час кібератаки, яка стала найдорожчою в історії, код NotPetya скерував зловмисне програмне забезпечення поширюватися «автоматично, швидко та без розбору», досягаючи мереж у 65 країнах і виводячи з ладу комп’ютерні системи по всьому світу [225].

Таким чином, у випадку порушення прокурором Міжнародного кримінального суду справи за зазначеними зверненнями Центру прав людини при Школі права Каліфорнійського університету в Берклі буде створено

значний правовий прецедент і зроблено перший важливий крок до захисту цивільних осіб від сучасних загроз XXI століття під час збройних конфліктів.

Головний прокурор Міжнародного кримінального суду Карім А. А. Хан зазначає, що інструменти, які використовуються для вчинення серйозних міжнародних злочинів, постійно розвиваються – від куль і бомб до соціальних мереж, Інтернету і, можливо, тепер навіть штучного інтелекту. Оскільки держави та інші суб'єкти все частіше вдаються до операцій у кіберпросторі, цим новим і швидко розвиваючим засобом управління державою та ведення війни можна зловживати для здійснення або сприяння військовим злочинам, злочинам проти людяності, геноциду та навіть агресії однієї держави проти іншої [226].

На думку Каріма А. А. Хана, міжнародне кримінальне правосуддя може і повинно адаптуватися до цього нового ландшафту. Хоча жодне положення Римського статуту не стосується кіберзлочинів, така поведінка потенційно може відповідати елементам багатьох основних міжнародних злочинів, які уже визначено [226].

Карім А. А. Хан підкреслює, що кібервійна не розгортається абстрактно. Навпаки, це може мати глибокий вплив на життя людей. Спроби вплинути на критично важливу інфраструктуру, таку як медичні заклади чи системи керування виробництвом електроенергії, можуть призвести до негайних наслідків для багатьох, особливо для найбільш уразливих. Ми також пам'ятаємо про зловживання Інтернетом для поширення ненависті та дезінформації, що може сприяти або навіть безпосередньо призводити до скоєння злочинів [226].

Державна служба спеціального зв'язку та захисту інформації України підтверджує, що росія здійснює кібератаки в координації з кінетичними військовими атаками в рамках свого вторгнення в Україну. Отже, цифрова війна є частиною скоєних військових злочинів. Як приклад, атаки росії на ДТЕК, найбільшу приватну енергетичну компанію, в липні 2022 р., коли було обстріляно теплову електростанцію і одночасно атаковано корпоративну мережу ДТЕК . Це керована та спланована діяльність росіян, яку вони робили як у звичайній сфері, так і в кіберсфері. Подібну скоординовану діяльність бачимо і

в Одесі, Львові та Миколаєві, де обстріли «підкріплюються [кібератаками] на місцеву владу, веб-сайти або місцевих інтернет-провайдерів». Ці атаки мають «прямий вплив», порушуючи служби даних, ІТ-інфраструктуру, електромережі, телекомунікації та критичну інфраструктуру [229].

Міжнародне Товариство Червоного Хреста в листопаді 2019 р. висловило свою позицію таким чином: немає сумніву, що [міжнародне гуманітарне право] застосовується до кібероперацій під час збройного конфлікту, а отже обмежує їх [230].

Відомий науковець М. Шмітт зазначає, що кібероперації можуть вважатися військовими злочинами і, таким чином, призвести до індивідуальної кримінальної відповідальності згідно з міжнародним правом. Це не обмежує можливість того, що кібероперації також можуть вважатися злочином проти людяності, геноцидом або злочином агресії згідно з міжнародним правом [227].

В Звіті Ради радників із застосування Римського статуту Міжнародного кримінального суду до кібервійни, опублікованому в серпні 2021 року, міститься кілька важливих рекомендацій. По-перше, це припускає (відповідно до статті 52(2) Римського статуту [30]), що напад можна вважати таким, що мав місце, коли ціль просто «нейтралізована», а не знищена відразу. Таким чином, у контексті кіберпростору Рада стверджує, що «порушення або припинення функціонування критичної інфраструктури держави або створення перешкод військовим можливостям, навіть якщо критична інфраструктура або військова техніка фізично не знищено, може кваліфікуватися як напад відповідно до міжнародного гуманітарного права. Додане застереження є примітним, оскільки воно передбачає, що остаточна оцінка цього питання належатиме прокурору на його розсуд. По-друге, Звіт радить вважати «цивільні дані» «законним захищеним об’єктом». Таким чином, націлювання на таку інформацію може становити атаку. На підтримку цієї точки зору в Звіті наведено важливий приклад націлювання на особисті медичні дані пацієнтів, які зберігаються в цивільному чи військовому госпіталі, видалення яких серйозно підірвало б допомогу, яку можна надавати хворим і пораненим [231].

Ще одним важливим аспектом є сучасні актуальні функції е-демократії, які можна розглядати як модель електронного уряду, що гарантує двосторонню політичну комунікацію та участь недержавних суб'єктів у процесі прийняття рішень. Адже надзвичайно важливим є забезпечення правдивості та достовірності інформації, в умовах відсутності дієвої міри відповідальності, яка регламентована в праві з чіткою процедурою застосування. Водночас, виникає необхідність у цифровій трансформації, як діяльності направленій на пошук ефективних механізмів захисту інформаційного середовища.

Нова редакція Стратегії кібербезпеки України, схвалена Рішенням Ради національної безпеки та оборони України від 14 травня 2021 року та затверджена Указом Президента України від 26 серпня 2021 року № 447, визначає такі загрози кібербезпеці Україні:

гібридна агресія російської федерації проти України у кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки російської федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності;

кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими

речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо;

організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності. Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію;

використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності [4].

Сучасний міжнародний досвід щодо реакції на кібератаки, або окремі форми прояву кібероборотьби, зводиться до практики глобальних учасників, на внутрішньому та зовнішньому рівні щодо реалізації кібервпливу на політичні процеси.

Цікавим для вивчення з точки зору дієвості впливу є досвід Сполучених Штатів Америки та Китайської Народної Республіки, який продовжує розвиватись і на даний час. Їх діяльність трансформується в співпрацю з країнами-однодумцями та міжнародними організаціями, які переслідують принципи, щодо спільної боротьби та співпраці у галузі кіберзахисту.

Ще в 2003 році була опублікована Національна стратегія безпеки кіберпростору США (National Strategy to Secure Cyberspace) [11, 12]. Це час коли в Україні лише розпочинався процес використання комп’ютерів та ноутбуків в індивідуальній діяльності, а тому в будь-яких заходах захисту чи боротьби не було актуальної потреби. Однак, у США стратегія захисту кіберпростору стала частиною загальнонаціональної безпеки.

Національна стратегія безпеки кіберпростору США проголошує три стратегічні цілі, а саме:

1) захист від кібератак об’єктів критичної інфраструктури Сполучених Штатів Америки;

2) мінімізація збитків та часу відновлення від кібератак;

3) зменшення вразливості від кібератак в загальнонаціональному масштабі [12].

1 квітня 2015 р. в США був підписаний Указ «Про арешт власності осіб, причетних до серйозних протиправних дій у кіберпросторі», суть його в побудові системи відповідальності за протиправні дії в кіберпросторі. Сполучені Штати Америки розробили правові умови для застосування санкцій до компаній та фізичних осіб, причетних до кібератак, що порушують стабільне функціонування об’єктів критичної інфраструктури США та ключових комп’ютерних мереж і систем. Відповідні санкції також мають бути накладені на осіб і компанії, які за допомогою кібератак незаконно привласнили кошти або інші активи, включаючи комерційну таємницю, персональні дані або фінансову інформацію американських компаній і організацій, або свідомо використовують такі активи, викрадені третіми особами в ході кібератак. Саме прописані в цьому Указі механізми й лягли в основу прийнятих у грудні 2016 р. санкцій проти росії [11].

11 травня 2017 р. в США був підписаний Указ «Про посилення кібербезпеки федеральних мереж і критичної інфраструктури». В ньому визначено такі напрями роботи:

1) комплексна перевірка американської інформаційної інфраструктури на предмет критичних вразливостей (відповідальне відомство Міноборони щодо систем, які забезпечують національну безпеку та Міністерством внутрішньої безпеки – щодо цивільної інфраструктури, серед іншого систем федерального уряду і приватного сектора, а координація зазначених завдань покладається на директора нацрозвідки, помічника президента з питань нацбезпеки, а також помічника президента з питань внутрішньої безпеки та боротьби з тероризмом);

2) оцінювання потенційних супротивників США в кіберпросторі;

3) оцінювання можливостей США в кіберпросторі (мають здійснювати Міністерство оборони, Міністерство внутрішньої безпеки і Агентство національної безпеки для розроблення системи рекомендацій і практичних кроків для зміцнення захисту американської критичної інфраструктури);

4) дослідження і розробка заохочувальних заходів для зміцнення кібербезпеки приватного сектора (відповідальне Міністерство торгівлі) [13 - 15].

Окрім цього, процес розвитку захисту від будь-яких потенційних провокативних кібератак в Сполучених Штатах Америки досить уважно відслідковується.

Ще однією інформаційно прогресивною країною на глобальному рівні є Китай. В сучасному глобальному інформаційному просторі існує достатня свобода щодо світосприйняття та висловлювань в напрямку політичних процесів. В кіберпросторі Китайська Народна Республіка, за останнє десятиріччя, також формує власну систему дій щодо укріплення національного інформаційного суверенітету, що створює двозначну форму сприйняття у світі: з одного боку, це трактується як спроба руйнації цілісності мережі Інтернет, а з іншого, як захист державницьких інтересів з жорсткою системою реагування та санкціонування.

Ще однією важливою складовою є кількість користувачів мережі Інтернет, яка в Китаї досить велика. Так, до прикладу, в 2013 р. показники користувачів Інтернет у КНР та користувачів Інтернет в усьому ЄС перевищувались у рази [16]. Звичайно, одним з основних чинників, що пливають на цю ситуацію, є чисельність населення та прогресивний розвиток Китаю, який відбувається досить швидко. В свою чергу в Європі спостерігається старіння населення та значне зменшення чисельності молодих людей, які є рушієм прогресу та сприйняття новітніх розробок.

На думку дослідника Дубова Д. В. у Китаї умовно можливо виокремити два основні напрями контролю. Перший напрям, так званого, «низького рівня», а другий – «високого рівня». Перший рівень контролює не технологічні, а регуляційні та організаційні методики, котрі стосуються цензури, тобто

допустимості окремого контенту, його непорушності національних інтересів. Другий «високий рівень» здійснення контролю, передбачає обмеження поширення так званої небажаної інформації, яка пов’язана з інформаційно-кібернетичними технологіями, з метою контролю над внутрішнім станом суспільства, впливом на його свідомість. Сучасники називають це новим виміром для прояву домінування в просторі країни [17].

Україна в сучасних умовах війни з 2014 р. Досить часто відчувала вплив на систему захисту об’єктів критичної інфраструктури, що сформувало необхідність адміністративно-правого регулювання, розвитку кіберзахисту, формування відповідних інститутів державного регулювання питань безпеки в інформаційній сфері.

В умовах консолідації прогресивних, мирних країн світу формуються умови для спільної міждержавної боротьби з кібератаками. У серпні 2022 р. між Україною та Польщею підписано меморандум про співпрацю у сфері кіберзахисту [18].

З 2016 року НАТО визнає як сферу операцій, у якій НАТО має захищатися так само ефективно, як це робить у повітрі, на суші та на морі [228].

Також у червні 2022 р. на Мадридському саміті НАТО оголосило про нову програму швидкого реагування на кібератаки. Альянс взявся посилити кіберзахист України перед обличчям постійних російських атак. Адже, росія систематично здійснює кібератаки на енергетику, банківську систему та інші критичні для економіки України об’єкти.

Тут важливу роль відіграють нормативні акти НАТО, спрямовані на вирішення поточних питань у кіберпросторі і які відображають сучасні виклики інформаційних загроз. Наприклад, Комплексна політика НАТО з кіберзахисту, спрямована на забезпечення мирного і безпечного кіберпростору [19].

«Кіберзагрози безпеці Альянсу мають комплексний, руйнівний характер. Вони стають все більш частими. Це підтверджується нещодавніми інцидентами з використанням програм-вимагачів та іншою зловмисною кіберактивністю, націленою на нашу важливу інфраструктуру та демократичні інститути», -

йдеться в комюніке за підсумками Брюссельського саміту НАТО. Зазначається, що НАТО «просуватиме вільний, відкритий, мирний і безпечний кіберпростір», а також продовжить докладати зусиль «щодо підвищення стабільності й зниження ризику конфліктів, підтримуючи міжнародне право та добровільні норми відповідальної поведінки держави в кіберпросторі» [19].

Альянсом проголошено, що кіберпростір належить до сфери відповідальності та діяльності НАТО, а кібероборона є основною в сучасному інформаційному світі [20].

Щодо співпраці України з НАТО у сфері запобігання та врегулювання конфліктів у кіберпросторі, зазначимо, що у 2018 р. Україна розпочала розбудову системи захисту кіберпростору за натовським зразком. Така трансформація є проявом необхідності в нинішньому становищі України. Однак у практичній реалізації поставлених завдань українські фахівці продемонстрували високу та розвинену спроможність реагувати на нові виклики [21].

Так, нова редакція Стратегії кібербезпеки України, схвалена Рішенням Ради національної безпеки та оборони України від 14 травня 2021 року та затверджена Указом Президента України від 26 серпня 2021 року № 447, регламентує вагомим елементом інтеграцію з системою кіберзахисту НАТО, бо боротьба України з кіберзагрозами стала досить актуальною в сучасному інформаційно-політичному просторі. Адже, ефективна політична система тоді, коли ефективні органи управління. Основними викликами у сфері кібербезпеки України є активне використання кіберінструментів у міжнародній конкуренції та вираження індивідуального впливу на глобальному рівні, а також конкурентний характер розвитку засобів кібербезпеки в умовах швидких змін в інформаційно-комунікаційних технологіях, зокрема хмарних та квантових обчислень, мереж 5G, великих даних, інтернету речей та штучного інтелекту [4].

Актуальною загрозою, яку виділено в Стратегії, і яка фактично реалізована країною агресором на території України – «мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі» [4].

Сучасна російсько-українська війна демонструє використання спецслужбами інформації, яку громадяни публікують публічно в соціальних мережах [22].

Окрім того, для політичних лідерів соціальні мережі стали майданчиком публічного спілкування з населенням в умовах війни та формою звіту про виконану та плановану роботу. А відеоролики, які з'являються в соціальних мережах, розцінюють, як прямі публічні звернення уповноважених осіб до суспільства. Тому, агресор використовує будь-яку інформацію, яка може допомогти.

Держава-агресор активно використовує кіберпростір. Основною формою цього є створення арсеналу наступальної кіберзброї, застосування якої є незворотнім і може мати незворотні деструктивні наслідки. Водночас інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури зазнають впливу, спрямованого на виведення їх з ладу (кібердиверсії), отримання негласного доступу та управління, ведення розвідувально-підривної діяльності.

Варто зазначити, що консолідація України у боротьбі з кіберзагрозами з окремими країнами чи міжнародними безпековими організаціями є шляхом обміну досвідом та практичними заняттями по боротьбі з агресорами. Кібератаки є інструментом впливу, який також активно виступає елементом спеціальних розвідувальних операцій для маніпулювання населенням та дискредитації України як держави. Також, вони використовувались під час виборчих компаній в країні та могли бути неправильно трактовані, як «чорний піар» та виборчі технології. Разом з тим, негативну складову кібероборотьби не варто виключати, бо шкода її для суспільства та держави є суттєвою та потребує значного часу для відновлення. Отже, робота по вдосконаленню системи органів швидкого реагування потребує вдосконалення, а відповідно адміністративно-правове забезпечення повинне відповідати викликам часу, що демонструє потребу у фахівцях інформаційного спрямування.

2.2. Адміністративно-правові засади забезпечення кібербезпеки в сфері боротьби з комп'ютерними злочинами й кібератакам

У сучасному світі, де все більше аспектів життя переходить в онлайн, кіберзлочинність та кібербезпека стають надзвичайно актуальними питаннями.

В Резолюції A/RES/57/239 Генеральної Асамблеї Організації Об'єднаних Націй «Створення глобальної культури кібербезпеки», ухваленій 20 грудня 2002 року, зазначається, що стрімкий розвиток інформаційної технології змінив те, як державні органи, підприємства, інші організації та індивідуальні користувачі, які розробляють ці інформаційні системи та мережі, мають, постачають їх, керують ними, обслуговують та використовують їх («учасники»), мають підходити до кібербезпеки [216].

Серед суб'єктів національної системи кібербезпеки надважливою є діяльність Державної служба спеціального зв'язку та захисту інформації України, на яку припадає близько 80 % навантаження в цій сфері, та яка відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»:

забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах;

координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту;

забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;

здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

інформує про кіберзагрози та відповідні методи захисту від них;

забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);

координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість;

забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (Computer response team of Ukraine), завданнями якої є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об’єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об’єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб’єктів національної системи кібербезпеки та власників об’єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп’ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об’єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам [2].

Згідно з даними Федерального бюро розслідувань Сполучених Штатів Америки, в 2022 р. зареєстровано 800 944 скарги на кіберзлочинність. Це означає, що щонайменше 422 мільйони людей постраждали від цього негативного явища. В 2023 р. зламано майже 33 мільярди облікових записів [23], вартість яких оцінено у 8 трильйонів доларів США.

Отже, на сьогодні, кіберзлочинність – це індустрія злочинців, яка коштує трильйони доларів США, і 43% атак спрямовані на малий і середній бізнес. Протягом періоду з 2001 по 2021 роки жертвами кіберзлочинності стало щонайменше 6,5 мільйонів осіб. За цей самий період сума заподіяних збитків склала майже 26 мільярдів доларів США.

Згідно з прогнозом авторитетного міжнародного видання Cybercrime Magazine у наступні п’ять років витрати від кіберзлочинності зростуть на 15 % і до 2025 р. досягнуть 10,5 трлн. доларів США на рік. Програми-вимагачі щороку коштують своїм жертвам близько 265 мільярдів доларів США [24].

Біля 80 % зареєстрованих кіберзлочинів зазвичай пов’язані з фішинговими атаками в технологічному секторі. Це значна проблема, яка потребує негайного вирішення, оскільки кіберзлочини, такі як шахрайство, крадіжка особистих даних, шпигунство та атаки на критичну інфраструктуру, можуть мати значні наслідки як для окремих осіб, так і для цілих організацій та держав.

Дослідник Доронін І. М. наголошує, що у сучасних умовах фактичної гібридної війни, яка ведеться проти України, питання забезпечення кібербезпеки у нашій державі має надзвичайно велике значення [215].

Виходячи з вищезазначеного, очевидно, що актуальним є проведення дослідження проблеми кіберзлочинності та кібербезпеки, а також напрацювання напрямків удосконалення адміністративно-правових засад забезпечення

кібербезпеки в Україні щодо боротьби з комп’ютерними злочинами й кібератаками.

Кіберзлочини часто складні для розслідування через брак кваліфікованих кадрів, необхідних інструментів та міжнародної співпраці. Кіберзлочинці часто ховаються за анонімністю, що ускладнює їх ідентифікацію та притягнення до відповідальності. Законодавство у сфері кіберзлочинності постійно еволюціонує, адже не завжди встигає за темпами розвитку нових технологій. Важливо зазначити, що кіберзлочинність є серйозною загрозою для суспільства, тому необхідні спільні зусилля держави, приватного сектору та громадян для її подолання.

Боротьба з кіберзлочинністю та забезпечення кібербезпеки – одна з найактуальніших проблем сьогодення. Це питання, яке потребує комплексного підходу, що містить як правові, так і технічні аспекти.

Важливою є та обставина, що кіберзлочинність постійно змінюється, постійно виникають нові типи злочинів та використовуються нові технології. Загалом цей процес можна поділити на кілька етапів розвитку.

На початку шістдесятих з’являються перші комп’ютерні мережі, що дає поштовх до розвитку кіберзлочинності. Саме тоді з’явилися і перші випадки крадіжки даних та комп’ютерних програм.

У вісімдесятих набули поширення персональні комп'ютери та Інтернет. І у цей період з’являються перші кіберзлочинні групи, які використовують кібершантаж та викрадення даних.

У 1990-ті відбулося стрімке зростання кіберзлочинності, перші масштабні кібератаки. З’являються нові типи кіберзлочинів [25].

На початку 2020-х спостерігається різке зростання кількості кібератак на державні органи та приватні компанії. Кібербезпека стає одним з пріоритетів національної безпеки. Кіберзлочинність стає все більш витонченою та складною. Зростає кількості кібератак на штучний інтелект та інші нові технології.

Перше покоління кіберзлочинів включає атаки, спрямовані на комп’ютери, комп’ютерні мережі та дані.

Друге покоління пов’язане з розвитком ІТ-мереж і атаками хакерів на їх цілісність і доступність.

Третє покоління пов’язане з помітним процесом автоматизації кіберзлочинності, що є, в тому числі результатом використання спеціального програмного забезпечення [26].

Нове покоління кіберзлочинів не вчиняється особисто та безпосередньо злочинцями, а є результатом автоматизованих атак з використанням програмного забезпечення, створеного для цієї мети.

Разом з тим, намагаючись постійно розв’язувати проблеми кібератак, фахівці розробили сучасні методи кіберзахисту, до яких відносять:

1. Запобігання кібератакам шляхом впровадження відповідних заходів безпеки.

2. Своєчасне виявлення кібератак для мінімізації їхніх наслідків.

3. Заходи для нейтралізації кібератак та відновлення роботи систем.

Серед інструментів кіберзахисту найчастіше використовують антивірусне програмне забезпечення, яке захищає комп’ютерні системи від вірусів, шпигунських програм та інших шкідливих програм [27]. Брандмауер – теж один з інструментів захисту, який блокує несанкціонований доступ до комп’ютерних систем.

Системи запобігання вторгненням блокують підозрілу активність у комп’ютерних мережах [27]. Метод шифрування захищає дані від несанкціонованого доступу через використання спеціальних шифрів та обмежує доступ до комп’ютерних систем та даних. Не варто забувати й про підвищення обізнаності користувачів щодо ризиків кіберзлочинності, які спрямовані на захист себе від них [27].

Відповідно до Резолюції A/RES/57/239 Генеральної Асамблеї Організації Об’єднаних Націй «Створення глобальної культури кібербезпеки» від 20 грудня 2002 року глобальна культура кібербезпеки вимагатиме, щоб усі учасники звернули увагу на такі дев’ять додаткових елементів:

a) Обізнаність. Учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що саме вони можуть здійснити для підвищення безпеки;

b) Відповідальність. Учасники відповідають за безпеку мереж відповідно до власної ролі. Вони повинні регулярно переглядати свою власну політику, практику, заходи та процедури та оцінювати, чи відповідають вони їхньому середовищу;

c) Реагування. Учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявлення та реагування на них. Вони повинні обмінюватися інформацією про загрози та вразливі місця, якщо це доцільно, і впроваджувати процедури швидкої та ефективної співпраці для запобігання, виявлення та реагування на інциденти безпеки. Це може включати транскордонний обмін інформацією та співпрацю;

d) Етика. Враховуючи поширеність інформаційних систем і мереж у сучасних суспільствах, учасники повинні поважати законні інтереси інших і визнавати, що їх дії чи бездіяльність можуть завдати шкоди іншим;

e) Демократія. Безпека повинна забезпечуватись таким чином, щоб це відповідало демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації; відкритість та гласність;

f) Оцінка ризиків. Усі учасники повинні проводити періодичні оцінки ризиків, які визначають загрози та вразливі місця; є достатньо широкими, щоб охопити ключові внутрішні та зовнішні фактори, такі як технології, фізичні та людські чинники, політики та сторонні послуги з наслідками для безпеки; дозволяють визначити допустимий рівень ризику; і допомагати у виборі відповідних засобів контролю для управління ризиком потенційної шкоди інформаційним системам і мережам у світлі характеру та важливості інформації, що підлягає захисту;

g) Проектування та впровадження засобів забезпечення безпеки. Учасники повинні включати безпеку як важливий елемент у плануванні та проектуванні, експлуатації та використанні інформаційних систем і мереж;

h) Управління безпекою. Учасники повинні прийняти комплексний підхід до управління безпекою, заснований на динамічній оцінці ризиків, яка охоплює всі рівні діяльності учасників і всі аспекти їх діяльності;

і) Переоцінка. Учасники повинні переглянути та переоцінити безпеку інформаційних систем і мереж, а також внести відповідні зміни в політику, практику, заходи та процедури безпеки, які включають усунення нових і мінливих загроз і вразливостей [216].

Крім того, в сенсі євроінтеграції для України важливими є відповідні норми європейського права.

Згідно з Регламентом Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), опрацювання персональних даних мірою, що є надзвичайно необхідною та пропорційною цілям забезпечення мережевої та інформаційної безпеки, тобто здатності мережі чи інформаційної системи чинити опір, на певному рівні довіри, випадковим подіям або незаконним чи зловмисним діям, що ставлять під загрозу наявність, автентичність, цілісність та конфіденційність збережених або переданих персональних даних, і безпеки пов'язаних послуг, які пропонують через такі мережі чи системи або надають за їхньою допомогою доступ органи публічної влади, групи з реагування на надзвичайні ситуації в комп’ютерній сфері (CERT), групи для реагування на інциденти в сфері комп’ютерної безпеки (CSIRT), провайдери електронних мереж і послуг зв'язку та провайдери технологій і послуг у сфері безпеки, становить законний інтерес відповідного контролера даних. Це, наприклад, може включати запобігання несанкціонованому доступу до електронних мереж зв'язку і розподіл шкідливого коду, припинення атак на

«відмову в обслуговуванні», а також пошкодження комп’ютера та систем електронного зв'язку [187].

Відповідно до Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу «безпека мережевих та інформаційних систем» означає здатність мережевих та інформаційних систем витримувати - на певному рівні впевненості - будь-яку дію, що загрожує доступності, справжності, цілісності або конфіденційності збережених або переданих чи опрацьованих даних або пов’язаних послуг, які пропонують такі мережеві та інформаційні системи або які доступні за допомогою таких систем:

держави-члени повинні бути належним чином оснащені, з огляду на технічні та організаційні спроможності, для запобігання, виявлення, реагування на інциденти та ризики мережевих та інформаційних систем та усунення їхніх наслідків. Отже, держави-члени повинні забезпечувати наявність у себе надійно функціонуючі CSIRT, також відомі як групи реагування на комп'ютерні надзвичайні ситуації («CERT»), що відповідають основним вимогам гарантування результативних та сумісних спроможностей для подолання наслідків таких інцидентів та ризиків і забезпечення ефективної співпраці на рівні Союзу. Для того, щоби всі типи операторів основних послуг та надавачів цифрових послуг користувалися перевагами таких спроможностей та співпраці, держави-члени повинні забезпечувати, щоби призначена CSIRT була передбачена для всіх типів. Враховуючи важливість міжнародної співпраці з питань кібербезпеки, CSIRT повинні мати можливість брати участь у мережах міжнародної співпраці окрім мережі CSIRT, заснованої цією Директивою;

інформація про інциденти дедалі стає важливішою для громадськості та суб’єктів господарської діяльності, особливо для малих та середніх підприємств. У деяких випадках, така інформація вже надається за допомогою веб-сайтів на національному рівні мовою конкретної країни, вона орієнтована головним чином на інциденти та події національного масштабу. З огляду на те, що суб’єкти господарської діяльності дедалі більше діяльності працюють через кордони і

громадяни використовують онлайн послуги, інформацію про інциденти необхідно надавати комплексно на рівні Союзу. Секретаріат мережі CSIRT заохочують підтримувати веб-сайт або розміщати виділену сторінку на існуючому веб-сайті, де оприлюднюють загальну інформацію про значні інциденти, які трапилися на території Союзу, з особливою увагою до інтересів та потреб суб'єктів господарської діяльності. CSIRT, які беруть участь у мережі CSIRT, заохочують добровільно надавати інформацію, що буде опублікована на такому веб-сайті, за винятком конфіденційної або чутливої інформації;

надавачі цифрових послуг повинні забезпечити рівень безпеки, співмірний з рівнем ризику, що виникає для безпеки цифрових послуг, які вони надають, враховуючи важливість інших послуг для операцій інших суб'єктів господарської діяльності в межах Союзу. На практиці, ступінь ризику для операторів основних послуг, які часто є істотними для підтримки важливої соціальної та економічної діяльності, є вищим ніж для надавачів цифрових послуг. Таким чином, вимоги до безпеки для надавачів цифрових послуг повинні бути менш суворими. Надавачі цифрових послуг повинні мати свободу вживати заходів, які вони вважають належними для управління ризиками, що виникають для безпеки їхніх мережевих та інформаційних систем. Через свій транскордонний характер, надавачі цифрових послуг повинні підлягати більш гармонізованому підходу на рівні Союзу. Імплементаційні акти повинні сприяти конкретизації та реалізації таких заходів;

інциденти можуть бути результатом злочинної діяльності, попередженню, розслідуванню та кримінальному переслідуванню яких сприяє координація та співпраця між операторами основних послуг, надавачами цифрових послуг, компетентними органами та правоохоронними органами. У разі підозри, що інцидент пов'язаний із серйозною злочинною діяльністю відповідно до національного законодавства або законодавства Союзу, держави-члени повинні заохочувати операторів основних послуг та надавачів цифрових послуг повідомляти відповідні правоохоронні органи про інциденти, щодо серйозного злочинного характеру яких виникає підозра. Якщо доречно, бажано, щоб

координації компетентних органів та правоохоронних органів різних держав-членів сприяли Європейський центр боротьби з кіберзлочинністю (ЕСЗ) та Європейського агентства з питань мережевої та інформаційної безпеки (ENISA) [233].

Отже, очевидним є висновок, що враховуючи загрози сьогодення важливо використовувати комплексний підхід до кіберзахисту, який поєднує різні методи та інструменти. Зважаючи на ряд актуальних проблем кібербезпеки можемо виділити наступне:

Кіберзлочинці постійно вдосконалюють свої методи, що робить кібератаки все більш складними для виявлення та нейтралізації [28].

Існує гостра нестача фахівців з кібербезпеки, що ускладнює захист організацій від кібератак.

Різні організації та країни мають різні підходи до кібербезпеки, що ускладнює міжнародну співпрацю [29].

Зростання залежності від Інтернету робить суспільство більш вразливим до кібератак.

Кіберзлочинність постійно еволюціонує, з’являються нові типи кіберзлочинів, що потребує постійного вдосконалення методів боротьби з ними [30].

Штучний інтелект може допомогти у виявленні та нейтралізації кібератак. Зростання обізнаності про кібербезпеку допоможе людям краще захищати себе від кіберзлочинності. Рухаючись у напрямі міжнародної співпраці кожна країна може допомогти собі в боротьбі з транснаціональною кіберзлочинністю. Вдосконалення законодавства сприятиме забезпеченню ефективного розслідування та переслідування злочинців [31].

Отже, підсумовуюче зазначене, можемо зробити висновки, що кібератаки стають все більш витонченими та складними, що робить кібербезпеку критично важливою. Ефективна боротьба з кіберзлочинністю потребує співпраці між державами, приватним сектором та громадянами. Необхідно постійно

вдосконалювати методи кібербезпеки, використовуючи нові технології та підвищуючи обізнаність.

Важливо розробити міжнародні стандарти та законодавство для боротьби з транснаціональною кіберзлочинністю.

Цілком очевидно, що майбутнє кібербезпеки залежить від здатності різних зацікавлених сторін працювати разом для захисту інформаційних систем та даних.

Варто підкреслити, що проаналізувавши теоретико-методичну джерельну базу, було б доречним запропонувати авторську методику впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України (табл. 2.1).

Таблиця 2.1

Методика впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України

Види об'єктів	**Об'єкти кіберзахисту**	**Механізми захисту**
Інформація	Персональні дані, конфіденційна корпоративна інформація, державні секрети	Шифрування, контроль доступу, резервне копіювання
Інформаційні системи	ERP, CRM, системи обліку та зберігання даних	Антивіруси, багатофакторна автентифікація, регулярні оновлення програмного забезпечення
Комп'ютерні мережі	Локальні мережі, хмарні сервіси, Інтернет-мережі	Мережеві екрани, VPN, IDS/IPS

Продовження таблиці 2.1

Види об’єктів	**Об’єкти кіберзахисту**	**Механізми захисту**
Фізичні пристрої	Сервери, робочі станції, мобільні пристрої	Захист паролем, контроль доступу, антивірусне програмне забезпечення
Програмне забезпечення	Операційні системи, додатки, антивірусне програмне забезпечення	Регулярні оновлення, використання ліцензійного програмного забезпечення
Комунікаційні засоби	Електронна пошта, месенджери, відеоконференції	Шифрування повідомлень, антифішингові заходи
Критична інформаційна інфраструктура	Енергетичні мережі, телекомунікації, банківські системи	Сегментація мережі, моніторинг в реальному часі
Людський фактор	Працівники, користувачі систем	Навчання, підвищення обізнаності, внутрішні політики
Процеси	Бізнес-процеси, технологічні процеси	Аудит безпеки, автоматизація
Репутація та імідж	Довіра клієнтів, позиція компанії на ринку	Моніторинг соціальних мереж, PR-кампанії
Правові та регуляторні аспекти	Дані, що підлягають захисту відповідно до законодавства	Відповідність GDPR, ISO 27001, локальним нормам

Продовження таблиці 2.1

Види об’єктів	**Об’єкти кіберзахисту**	**Механізми захисту**
Веб-ресурси	Корпоративні веб-сайти, інтернет-магазини	SSL-сертифікати, веб-фаєрволи
Облікові записи користувачів	Логіни, паролі, сесійні токени	MFA, менеджери паролів
Фінансові ресурси	Банківські рахунки, криптовалюти	Моніторинг транзакцій, безпечні платіжні шлюзи
Архіви даних	Резервні копії, архівні сервери	Шифрування резервів, фізична безпека
Критичні технології	Системи SCADA, ICS	Сегментація мережі, моніторинг і оновлення
Розумні системи	Розумні будинки, розумні міста	Шифрування, регулярне оновлення прошивки
Хмарні інфраструктури	PaaS, SaaS, IaaS	Контроль доступу, резервне копіювання
Медіа-контент	Відео, аудіо, графічні файли	Захист авторських прав, DRM
Алгоритми та моделі	Алгоритми шифрування, моделі штучного інтелекту	Контроль доступу, перевірка моделей
Канали зв’язку	Голосові дзвінки, VPN	Шифрування, брандмауери
Фізичне середовище	Центри обробки даних, контроль доступу до приміщень	Системи відеоспостереження, біометрія
Соціальні мережі	Корпоративні акаунти, сторінки бренду	Двофакторна автентифікація, моніторинг активності

Закінчення таблиці 2.1

Види об’єктів	**Об’єкти кіберзахисту**	**Механізми захисту**
Навчальні ресурси	Онлайн-курси, бази знань	Контроль доступу, регулярне оновлення даних
Мобільні додатки	Корпоративні та розважальні додатки	Шифрування, захист коду
Інфраструктура резервного відновлення	Дата-центри резервного відновлення	Тестування відновлення, плани аварійного реагування

Джерело: авторська розробка на основі теоретико-методичних матеріалів

Доречно зазначити, що авторська методика впровадження механізмів захисту об’єктів кіберзахисту в період воєнного стану та повоєнного відновлення України потребує подальшого вивчення та аналізу. Зазначений матеріал є актуальним сьогодні на глобальному рівні. В нашій державі зазначена авторська пропозиція потребує окремої уваги.

Вважаємо, що в період воєнного часу авторська методика впровадження механізмів захисту об’єктів кіберзахисту в період воєнного стану та повоєнного відновлення України є важливою та має бути впроваджена у вигляді відповідної програми з удосконалення обізнаності населення щодо існуючих механізмів захисту об’єктів кіберзахисту (табл. 2.1). Вона допоможе суспільству та поліпшить обізнаність щодо захисту своїх прав на конфіденційність інформації та об’єкти інтелектуальної власності тощо. Зазначена розробка є важливою та актуальною і надає гарантію захисту людських прав, під час воєнного вторгнення росії на територію України та на стадії відновлення.

Здійснивши дослідження та проаналізувавши наукові джерела, варто в майбутньому і надалі вивчати шляхи захисту відповідних об’єктів кіберзахисту.

Слушно підкреслити, що гарантії захисту свобод та людських прав реалізуються на державному рівні. Це надає змогу вирішити основні проблемні аспекти сьогодення, тому пропозицією є поліпшення обізнаності населення шляхом реалізації відповідної інформаційної політики Кабінетом Міністрів України як органу, який відповідно до частини третьої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю, через профільні центральні органи виконавчої влади: Міністерство цифрової трансформації України, Міністерство культури та стратегічних комунікацій України, Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України тощо.

Висновки до розділу 2

Станом на теперішній час, значно почастішали кібератаки як в Україні, так і в інших державах.

В розділі 2 дисертаційного дослідження проведено комплексне наукове дослідження визначення правового статусу кібератак та кібервійськових операцій, який до сих пір досліджено лише фрагментарно.

Трансформація конфліктної активності в кіберпростір провокує швидку глобалізацію конфронтації з можливістю залучення міжнародних учасників, які мають вплив на міжнародні процеси. Враховуючи особливості кіберпростору, кібератаки як форма політичного кіберконфлікту можуть призводити до міжнародних конфліктів, що охоплюють територіально визначені зони.

Визначено, що оскільки в інформаційному суспільстві формується уявлення про кіберконфлікт, негативні наслідки його ескалації, то інформаційне протиборство здійснюється для впливу на масову свідомість, за допомогою

спотворення реальності щодо наслідків конфронтації сторін. Результати кіберконфліктів мають вагомий вплив на процес прийняття найважливіших у світі політичних рішень та реалізації цілей геополітичного рівня.

Показано, що трансформація у військових атак у кібервійськові є проявом осучаснення ведення військових дій та реалізації глобалізаційних змін. Доведено, що кібервійськові атаки стають невід'ємною формою існування демократичного устрою. Визначено, що виникає потреба у формуванні системи реагування органами управління, на небезпеку, яку вони можуть нести суспільству, в тому числі, необхідність у цифровій трансформації, як діяльності направленій на пошук ефективних механізмів захисту інформаційного середовища.

На прикладі НАТО, Сполучених Штатів Америки та Китайської Народної Республіки досліджено сучасний міжнародний досвід щодо реакції на кібератаки, або окремі форми прояву кіберборотьби, який, на сьогодні, зводиться до практики глобальних учасників на внутрішньому та зовнішньому рівні щодо реалізації кібервпливу на політичні процеси.

Показано, що сучасна російсько-українська війна демонструє використання спецслужбами інформації, яку громадяни публікують публічно в соціальних мережах. Держава-агресор активно використовує кіберпростір. Основною формою цього є створення арсеналу наступальної кіберзброї, застосування якої є незворотнім і може мати незворотні деструктивні наслідки. Водночас інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури зазнають впливу, спрямованого на виведення їх з ладу (кібердиверсії), отримання негласного доступу та управління, ведення розвідувально-підривної діяльності.

Отже, об'єднання України у боротьбі з кіберзагрозами з окремими країнами чи міжнародними безпековими організаціями є шляхом обміну досвідом та практичними заняттями по боротьбі з агресорами. Кібератаки є інструментом впливу, який виступає елементом спеціальних розвідувальних

операцій для маніпулювання населенням та дискредитації України як держави. Також, вони використовувались під час виборчих компаній в країні.

Разом з тим, негативну складову кіберборотьби не варто виключати, оскільки шкода її для суспільства та держави є суттєвою та потребує значного часу для відновлення. А тому, робота по модернізації системи органів швидкого реагування потребує вдосконалення, а відповідно нормативна система повинна відповідати викликам часу.

Показано, що на даний час значною є проблема фішингових атак в технологічному секторі, яка потребує негайного вирішення, оскільки кіберзлочини, такі як шахрайство, крадіжка особистих даних, шпигунство та атаки на критичну інфраструктуру, можуть мати значні наслідки як для окремих осіб, так і для цілих організацій та держав.

Проведено дослідження проблеми кіберзлочинності та кібербезпеки, за результатами якого запропоновано напрямки удосконалення адміністративно-правових засад забезпечення кібербезпеки в Україні щодо боротьби з комп’ютерними злочинами й кібератаками.

Зазначено, що кіберзлочини часто складні для розслідування через брак кваліфікованих кадрів, необхідних інструментів та міжнародної співпраці. Кіберзлочинці часто ховаються за анонімністю, що ускладнює їх ідентифікацію та притягнення до відповідальності. Законодавство у сфері кіберзлочинності постійно еволюціонує, адже не завжди встигає за темпами розвитку нових технологій.

Наголошується, що кіберзлочинність є серйозною загрозою для суспільства. Боротьба з кіберзлочинністю та забезпечення кібербезпеки – одна з найактуальніших проблем сьогодення. Це питання, яке потребує комплексного підходу, що містить як правові, так і технічні аспекти.

Важливою є обставина, що кіберзлочинність постійно змінюється, постійно виникають нові типи злочинів та використовуються нові технології. Кібератаки стають все більш витонченими та складними, що робить кібербезпеку критично важливою.

Зроблено висновок, що враховуючи загрози сьогодення важливо використовувати комплексний підхід до кіберзахисту, який поєднує різні методи та інструменти.

Серед актуальних проблем кібербезпеки виділено такі:

кіберзлочинці постійно вдосконалюють свої методи, що робить кібератаки все більш складними для виявлення та нейтралізації;

існує гостра нестача фахівців з кібербезпеки, що ускладнює захист організацій від кібератак;

різні організації та країни мають різні підходи до кібербезпеки, що ускладнює міжнародну співпрацю;

зростання залежності від Інтернету робить суспільство більш вразливим до кібератак;

кіберзлочинність постійно еволюціонує, з'являються нові типи кіберзлочинів, що потребує постійного вдосконалення методів боротьби з ними.

Ефективна боротьба з кіберзлочинністю потребує співпраці між державами, приватним сектором та громадянами. Необхідно постійно вдосконалювати методи кібербезпеки, використовуючи нові технології та підвищуючи обізнаність. Важливо розробити міжнародні стандарти та законодавство для боротьби з транснаціональною кіберзлочинністю. Майбутнє кібербезпеки залежить від здатності різних зацікавлених сторін працювати разом для захисту інформаційних систем та даних.

Рухаючись у напрямі міжнародної співпраці кожна країна може допомогти собі в боротьбі з транснаціональною кіберзлочинністю. Вдосконалення законодавства сприятиме забезпеченню ефективного розслідування та переслідування злочинців.

Запропоновано авторську методику впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України. Зазначений матеріал є актуальним сьогодні на глобальному рівні. В нашій державі викладена авторська пропозиція потребує окремої уваги. Зазначається, що авторська методика впровадження механізмів захисту об'єктів

кіберзахисту в період воєнного стану та повоєнного відновлення України потребує подальшого вивчення та аналізу.

Вважаємо, що в період воєнного часу авторська методика впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України є важливою та має бути впроваджена у вигляді відповідної програми з удосконалення обізнаності населення щодо існуючих механізмів захисту об'єктів кіберзахисту. Вона допоможе суспільству та поліпшить обізнаність щодо захисту своїх прав на конфіденційність інформації та об'єкти інтелектуальної власності тощо. Зростання ж обізнаності про кібербезпеку допоможе людям краще захищати себе від кіберзлочинності. Зазначена розробка є важливою та актуальною і надає гарантію захисту людських прав, під час воєнного вторгнення росії на територію України та на стадії відновлення.

Вважаємо, що варто в майбутньому і надалі вивчати шляхи захисту відповідних об'єктів кіберзахисту. Слушно підкреслити, що гарантії захисту свобод та людських прав реалізуються на державному рівні. Це надає змогу вирішити основні проблемні аспекти сьогодення, тому пропозицією є поліпшення обізнаності населення шляхом реалізації відповідної інформаційної політики Кабінетом Міністрів України як органу, який відповідно до частини третьої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю, через профільні центральні органи виконавчої влади: Міністерство цифрової трансформації України, Міністерство культури та стратегічних комунікацій України, Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України тощо.

РОЗДІЛ 3. АКТУАЛЬНІ ПИТАННЯ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ ТА ПОВОЄННОЇ ВІДБУДОВИ УКРАЇНИ

3.1. Напрями вдосконалення адміністративно-правового забезпечення кібербезпеки в сфері захисту інформації та запобігання сучасним загрозам кіберзлочинності в секторі державної безпеки

Сучасні реалії показують, що за останні десятиліття в світі спостерігається значне зростання кількості кіберзлочинів. Змінюються як мотиви, так і цілі зловмисників, продовжує зростати рівень загрози від їх дій для держав та державних інституцій. Загострення цього питання потребує негайного та ефективного вирішення, враховуючи те, що кіберзлочинність стає все більш складною та витонченою, а ефективність розслідувань та протидії в кіберпросторі падає. Тема кібербезпеки є особливо актуальною на даний момент у світлі витрат на запобігання та розкриття кіберзлочинів у контексті безпеки держави.

Цікаво та влучно ситуацію описує М. Єрема: на початку XXI століття злодій – це не обов'язково холоднокровна озброєна людина. Інформаційна революція призвела до того, що злодієм може виявитися звичайний студент із ноутбуком та доступом до мережі. В умовах війни такий злодій стає бойовою одиницею, а його основний інструмент - кібератаки і злами. Крім того, під час воєнного стану атаки можливі не лише з боку ворога, який використовує інфопростір для завдання шкоди обороноздатності України, а й з боку тих, хто вирішив скористатися ситуацією, коли правоохоронні органи перевантажені, та поживитися коштами наших громадян [171].

М. Єрема констатує, що в наш час війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою [171].

Юридичні та фізичні особи прагнуть захистити себе заздалегідь, однак злочинці в кіберпросторі постійно вдосконалюють свої методи, що робить цю сферу важливою для постійного моніторингу та розробки нових рішень щодо вдосконалення адміністративно-правових засад запобігання сучасним загрозам кіберзлочинності та захисту інформації в сфері державної безпеки**.** Розширення можливостей інформаційних технологій, особливо Інтернету, призвело до підвищення інтересу з боку окремих осіб та організованих злочинних груп, які використовують ці технології в протиправних цілях. Доступність технологій, їх низька вартість та можливість отримання значних прибутків з мінімальними ризиками та високою анонімністю роблять запобігання сучасним загрозам і боротьбу з кіберзлочинністю одним з найактуальніших на даний час викликів світу [32]. Постійний розвиток інформаційних технологій і поява нових способів їх використання в злочинних цілях загрожують безпеці глобальних інформаційних мереж і держав загалом. Цим зумовлена актуальність проведення дослідження щодо визначення напрямків вдосконалення адміністративно-правових засад запобігання сучасним загрозам кіберзлочинності та захисту інформації**.**

Вважаємо, що в дисертаційному дослідженні варто розглянути поняття «злочинність у сфері комп’ютерної інформації», посилаючись як на наукові, так і на законодавчі визначення, щоб отримати краще розуміння цього явища, що набирає обертів. Терміни «кіберзлочинність» і «злочинність у сфері комп’ютерної інформації» часто вживаються як синоніми, хоча між ними є певні відмінності.

Наприклад, Д. Нікола в своєму дослідженні визначає злочини у сфері комп’ютерної інформації, не проводячи чіткого розмежування між цим терміном і поняттям «комп’ютерні злочини» [33].

У своїх наукових роботах [34] та [35] дослідники О. Вакулик та П. Ванг висвітлюють ідею, що термін «комп’ютерна злочинність» був введений для

опису як абсолютно нових типів злочинів, спрямованих проти комп'ютерів, мереж та їх користувачів, так і традиційних злочинів. вчинені з використанням комп'ютерної техніки.

Науковець В. Шаблистий разом з іншими визначили «комп'ютерні злочини» як категорію, яка має чітке визначення та включає як злочини у сфері комп'ютерної інформації, так і злочини, вчинені у сфері інформаційно-комунікаційних технологій, запропонувавши визначити їх як інформаційні злочини; злочини, в яких комп'ютери та мережі є інструментами для вчинення протиправних дій [36].

Дослідники Б. Коліер та К. Джордан трактують кіберзлочинність як концепцію, яка охоплює всі протиправні дії, які вчиняються чи здійснюються з використанням інформаційно-комунікаційних технологій [37, 38].

Термін «кіберзлочинність» означає дії, спрямовані на порушення конфіденційності, компрометацію цілісності або обмеження доступу до комп'ютерних даних чи систем, що є ядром концепції кіберзлочинності [39]. У ширшому розумінні це включає злочини, вчинені з використанням комп'ютерів для отримання особистої або фінансової вигоди чи шкоди, включаючи використання персональних даних та інформації, що зберігається в комп'ютерних системах [40].

Дехто з науковців, такі як В. Акото та Б. Дюпон, зазначають, що «кіберзлочинність» охоплює злочини, пов'язані як з використанням комп'ютерних технологій, так і з глобальними мережами. Водночас «комп'ютерна злочинність» більш конкретно стосується злочинів проти комп'ютерних систем або даних [41, 42].

Такі вчені як Н. Чаудгарі, І. Леукфілдт, А. Лаворгна, І. Кліманс і Т. Тропіна в своїх дослідженнях [43 – 45] показують, що злочини, скоєні у глобальних комп'ютерних мережах зазвичай мають такі ознаки:

1) висока конспірація під час вчинення злочинів;

2) транскордонний характер, коли злочинець, об'єкт злочину та жертва можуть перебувати в різних країнах;

3) спеціальну кваліфікацію злочинців та інтелектуальний характер їх дій;

4) можливість автоматизованих злочинів у кількох місцях одночасно;

5) труднощі попередження та припинення таких злочинів традиційними методами.

Загалом можна констатувати, що сьогодні кіберзлочинність включає широкий спектр протиправних дій, від несанкціонованого доступу до державних комп'ютерних мереж і крадіжки особистих даних до фінансового шпигунства та відмивання грошей.

А тому актуальним постає проведення наукового дослідження з ґрунтовним аналізом сучасного стану кіберзлочинності та її впливу на безпеку держави. Необхідно також дослідити та визначити ключові загрози, що виникають у цифровому просторі, розробити адміністративно-правові методи запобігання та протидії цим загрозам у контексті забезпечення безпеки держави.

Загрози кіберзлочинності в сфері безпеки держави постійно збільшуються та розвиваються в зв'язку з удосконаленням та появою нових ІТ-технологій, а також збільшенням кількості користувачів, залучених до інформаційних процесів. Це, зокрема, розширення кіберпростору за рахунок зростання кількості користувачів Інтернету та мобільних пристроїв, а також перехід на електронний документообіг в державних організаціях та установах.

Наразі Україна, поряд зі Сполученими Штатами Америки та Китаєм, є однією з країн-лідерів за кількістю кібератак. Злочини в цій сфері можна класифікувати за трьома основними категоріями:

1) незаконне завантаження або використання програмного забезпечення;

2) шахрайство та обман;

3) атаки, які використовують вразливі місця системи та несанкціонований доступ до цифрових даних та/або мереж державних установ та установ [46].

Обсяг таких злочинів значно зріс за останні два роки через зростання кількості сайтів і мереж, які надають доступ до інформації [47].

В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди [171].

Від початку війни стало відомо про велику кількість кібератак на Україну.

Варто згадати невдалу спробу атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти конфіденційну інформацію.

Нещодавно Держспецзв’язку повідомило про отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання хакерами повного контролю над вашим комп'ютером та загрожує крадіжкою та пошкодженням комп'ютерних даних.

Раніше, 4 квітня 2022 р., Держспецзв’язку попереджувало про розповсюдження електронних листів з назвою «Військові злочинці РФ.htm», відкриття яких призводить до того, що зловмисники отримують віддалений доступ до комп’ютера жертви.

Під прицілом знаходяться також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 р., під час якої хакери намагались проаналізувати, як влаштована IT-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії.

23 березня 2022 р. ворог намагався здійснити кібератаку на державні установи України з використанням шкідливої програми Cobalt Strike Beacon, яка уражає комп’ютер у випадку її відкриття.

Це приклади лише масованих атак [171].

Кібертехнології та шахрайські схеми використовують вразливі місця в державних системах безпеки, використовуючи різні типи атак соціальної інженерії та недостатню обізнаність кінцевих користувачів про необхідні заходи безпеки для захисту від онлайн-загроз.

Атака соціальної інженерії – це атака на кібербезпеку, яка ґрунтується на психологічних маніпуляціях людською поведінкою, щоб розкрити конфіденційні дані, отримати облікові дані чи доступ до персонального пристрою або іншим чином порушити цифрову безпеку [50].

Атаки соціальної інженерії становлять велику загрозу кібербезпеці, оскільки багато атак починаються на особистому рівні та покладаються на людську помилку для просування шляху атаки. Викликаючи співчуття, страх і невідкладність у жертви, зловмисники часто можуть отримати доступ до особистої чи конфіденційної інформації. Якщо пристрій підключено до корпоративної мережі або містить облікові дані для корпоративних облікових записів, це також може надати зловмисникам шлях до атак вже на рівні підприємства.

Найпоширенішими типами атак соціальної інженерії є:

1. Фішинг (phishing) – це кібератака, яка використовує електронну пошту, телефон, SMS, соціальні мережі чи іншу форму особистого спілкування, щоб спонукати користувачів натиснути зловмисне посилання, завантажити заражені файли або розкрити особисту інформацію, таку як паролі чи номери облікових записів. Найвідоміші фішингові атаки зазвичай пов’язані з дивовижними претензіями. У багатьох випадках кіберзлочинець може маскуватися під роздрібних продавців, постачальників послуг або державні установи, щоб отримати особисту інформацію, яка може здаватися нешкідливою, наприклад адреси електронної пошти, номери телефонів, дату народження користувача або імена членів сім’ї. Фішинг є одним з найпоширеніших видів кібератак, і його поширеність продовжує зростати з року в рік. Через поширення епідемії COVID-19 різко збільшила кібератаки всіх видів, у тому числі фішингові. В період карантину люди зазвичай проводили більше часу в Інтернеті, а також відчували загострення емоцій. Так, наприклад, за даними Федерального бюро розслідувань Сполучених Штатів Америки, фішинг був найпоширенішою формою кіберзлочинності в 2020 році, кількість інцидентів збільшилася майже вдвічі порівняно з 2019 роком.

2. Китобійна атака – це різновид фішингової атаки, яка також використовує особисте спілкування для отримання доступу до пристрою або особистої інформації користувача. Різниця між фішингом і китобійством пов’язана з рівнем персоналізації. В той час як фішингові атаки не персоналізовані та можуть бути відтворені для мільйонів користувачів, китобійні атаки спрямовані на одну особу, як правило, на керівника високого рівня. Цей тип атаки вимагає значного обсягу досліджень щодо цієї особи, що зазвичай робиться шляхом перегляду її активності в соціальних мережах та іншої публічної поведінки. Хоча китобійні атаки вимагають більшого планування та зусиль, вони часто приносять величезні прибутки, оскільки цілі (жертви) цих атак мають доступ до цінних даних або фінансових ресурсів.

3. Переманювання – це тип атаки соціальної інженерії, коли шахраї дають користувачам помилкові обіцянки, щоб спонукати їх розкрити особисту інформацію або встановити шкідливе програмне забезпечення в системі. Таке шахрайство може здійснюватися у формі спокусливої реклами чи онлайн-реклами, як-от безкоштовне завантаження ігор чи фільмів, потокове передавання музики чи оновлення телефону. Зловмисник сподівається, що пароль, який ціль використовує, щоб отримати пропозицію, є тим, який він також використовував на інших сайтах, що може дозволити хакеру отримати доступ до даних жертви або продати інформацію іншим злочинцям у темній мережі. Приманка також може здійснюватися у фізичній формі, найчастіше через заражену шкідливим програмним забезпеченням флешку. Зловмисник залишить заражену флешку в місці, де жертва, швидше за все, побачить її. Це спонукало б жертву вставити флешку в комп’ютер, щоб дізнатися, кому вона належить. Тим часом зловмисне програмне забезпечення встановлюється автоматично.

4. Диверсійна крадіжка – це кібератака, яка виникла офлайн. Під час цієї атаки злодій переконує кур’єра забрати або залишити пакунок не в тому місці, доставити не той пакунок або доставити пакунок не тому одержувачу. Проте, на сьогодні, диверсійна крадіжка вже адаптована і як онлайн-схема. Зловмисник викрадає конфіденційну інформацію, обманом змушуючи користувача надіслати

її не тому одержувачу. Цей тип атаки часто включає спуфінг, який є технікою, яку використовують кіберзлочинці, щоб замаскувати себе під відоме або надійне джерело. Спуфінг може приймати різні форми, наприклад спуфінг електронної пошти, спуфінг IP-адреси, спуфінг DNS, спуфінг GPS, спуфінг веб-сайту та спуфінг дзвінків.

5. Компроміс корпоративної пошти – це тип атаки соціальної інженерії, коли зловмисник видає себе за надійного керівника, уповноваженого вирішувати фінансові питання в організації. В цьому сценарії атаки шахрай уважно стежить за поведінкою керівника та використовує підробку, щоб створити підроблений обліковий запис електронної пошти. Видаючи себе за іншу особу, зловмисник надсилає електронного листа своїм підлеглим з проханням здійснювати банківські перекази, змінювати банківські реквізити та виконувати інші завдання, пов’язані з грошима. Така кібератака може призвести до великих фінансових втрат для компаній. На відміну від інших кібершахрайств, ці атаки не покладаються на шкідливі URL-адреси чи зловмисне програмне забезпечення, які можуть бути виявлені інструментами кібербезпеки, такими як брандмауери або системи виявлення та реагування на кінцеві точки.

6. Смішинг (SMS-фішинг) — це атака соціальної інженерії, яка здійснюється спеціально за допомогою SMS-повідомлень. У цій атаці шахраї намагаються спонукати користувача натиснути посилання, яке спрямовує його на шкідливий сайт. Опинившись на сайті, жертві пропонується завантажити шкідливе програмне забезпечення та вміст. Смішінг-атаки стали популярними серед злочинців, оскільки люди проводять більше часу за мобільними пристроями. І хоча вцілому користувачі стали більш уважнішими щодо виявлення фішингу електронної пошти, багато людей набагато менше усвідомлюють ризики, пов’язані з текстовими повідомленнями. Смішинг-атака вимагає невеликих зусиль від зловмисників і часто здійснюється шляхом простого придбання підробленого номера та встановлення шкідливого посилання.

7. Атака «quid pro quo» передбачає, що зловмисник запитує конфіденційну інформацію від жертви в обмін на бажану послугу. Наприклад, зловмисник може видати себе за фахівця з IT-підтримки та зателефонувати користувачеві комп'ютера, щоб вирішити поширену IT-проблему, таку як низька швидкість мережі або виправлення системи для отримання облікових даних користувача. Після обміну обліковими даними ця інформація використовується для отримання доступу до інших конфіденційних даних, що зберігаються на пристрої та його програмах, або продається в темній мережі.

8. Перетекстування – це тип атаки соціальної інженерії, яка передбачає складання правдоподібних сценаріїв або приводів, які ймовірно переконають жертв поділитися цінними та конфіденційними даними. Претекстори можуть видати себе за когось з представників владних повноважень, як-от співробітника правоохоронних органів чи податкового службовця, або за зацікавлену особу, як-от організатор тоталізаторів. Після пояснення контексту зловмисник ставить жертві запитання, щоб отримати особисту та конфіденційну інформацію, яку потім міг би використовувати для розвитку інших сценаріїв атаки або доступу до особистих облікових записів.

9. Атака медової пастки — це тип атаки соціальної інженерії, спрямований спеціально на людей, які шукають кохання на веб-сайтах знайомств або в соціальних мережах. Злочинець здружується з жертвою, створивши вигадану персону та фальшивий профіль в Інтернеті. Згодом злочинець користується стосунками й обманом змушує жертву дати їй гроші, надати особисту інформацію або встановити шкідливе програмне забезпечення.

10. Хвіст, також відомий як контрейлерство, — зловмисник отримує доступ до фізичного об'єкта, наприклад, попросивши особу, яка входить попереду, притримати двері. Зловмисник може видати себе за водія-доставника або іншу правдоподібну особу. Потрапивши всередину закладу, злочинець може використати свій час для проведення розвідки, викрадення пристроїв, які залишені без нагляду, або доступу до конфіденційних файлів. Зловживання також може включати дозвіл неавторизованій особі позичити ноутбук або інший

пристрій співробітника, щоб користувач міг встановити зловмисне програмне забезпечення [50].

Хоча неможливо запобігти атакам соціальної інженерії, громадяни та організації можуть захистити себе пильністю, відповідальною поведінкою та базовими знаннями основ кібербезпеки.

Зловмисний неавторизований доступ здійснюється, коли злочинець використовує різні методи, такі як віруси чи хробаки, щоб контролювати чиюсь систему без дозволу власника.

В табл. 3.1 приведено цілі (об’єкти) та відповідні їм види кіберзагроз, а протиправні дії можуть здійснюватися у формах атак, розглянутих вище.

Таблиця 3.1

Об’єкти та види кіберзагроз

Об’єкт кіберзагроз	**Види кіберзагроз**
Громадянське суспільство	Маніпулювання особистістю через збір персональних даних та атаки на комп’ютери державних службовців. Видалення та розголошення конфіденційної інформації або даних, призначених для обмеженого кола користувачів. Фінансові махінації. Поширення шкідливого контенту.
Бізнес середовище	Негативний вплив на системи Інтернет-безпеки державних органів. Порушення роботи інформаційної інфраструктури. Паралізує онлайн-системи документообігу та геоінформаційні системи. Хакерські атаки на сайти державних та приватних підприємств і установ.

Закінчення таблиці 3.1

Об'єкт кіберзагроз	**Види кіберзагроз**
Державний устрій	Атаки на важливі системи державного управління (електронний уряд, офіційні сайти державних установ). Економічні обмеження (масштабне призупинення роботи платіжних систем, казначейств, національного банку). Фізичні атаки на персональні комп'ютери та критичну інфраструктуру державних підприємств та установ.

Джерело: складено автором на основі [48, 49].

Безсумнівно, унікальність інформаційних систем, особливо Інтернету, «вимагає об'єднання зусиль різних суб'єктів, як державних, так і приватних», у вирішенні питань кібербезпеки держави. Проте ключову роль у цьому процесі має відігравати держава, яка має значні можливості для ефективної протидії кіберзлочинності та створення умов для захисту найбільш вразливих суб'єктів, дозволяючи їм розвиватися, створюючи надійні системи державної кібербезпеки [51]. Залежно від цілей, завдань і ресурсів суб'єктів кіберпростору можна виділити три основні рівні загроз інформаційній безпеці держави та відповідні їм види загроз, як показано на рис. 3.1.

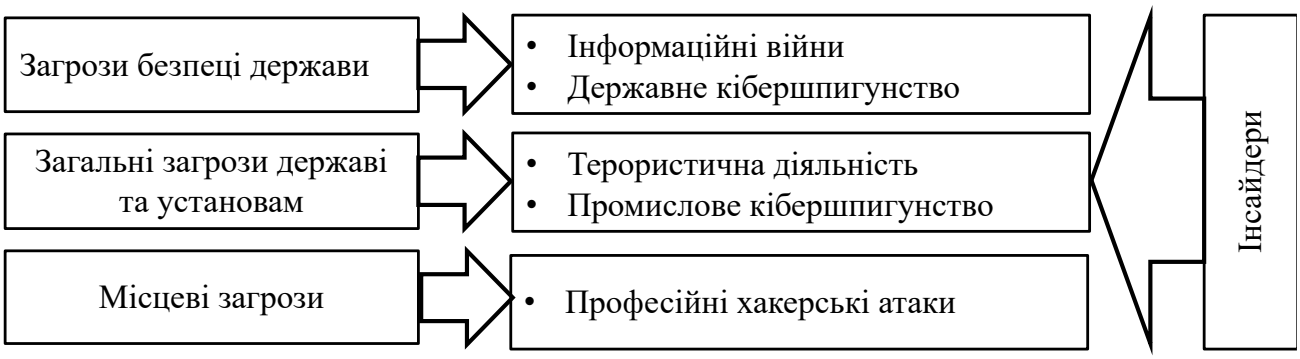

Рис. 3.1. Рівні загроз інформаційній безпеці держави

Джерело: складено автором на основі [52].

Такий підхід вказує на особливу небезпеку для системи державного управління, яку можуть становити такі деструктивні дії в кіберпросторі, як інформаційна війна та кібершпигунство. В свою чергу, зловживання інформаційно-комунікаційними технологіями в злочинних і терористичних цілях становить серйозну загрозу як для державного, так і для приватного секторів. Хакерство є значною локальною загрозою, яка впливає на як на окремих користувачів так і локальні мережі. В зв'язку з цим ризик деструктивних дій інсайдерів залишається актуальним на всіх рівнях. Модель управління кібербезпекою державних установ наведена на рис. 3.2.

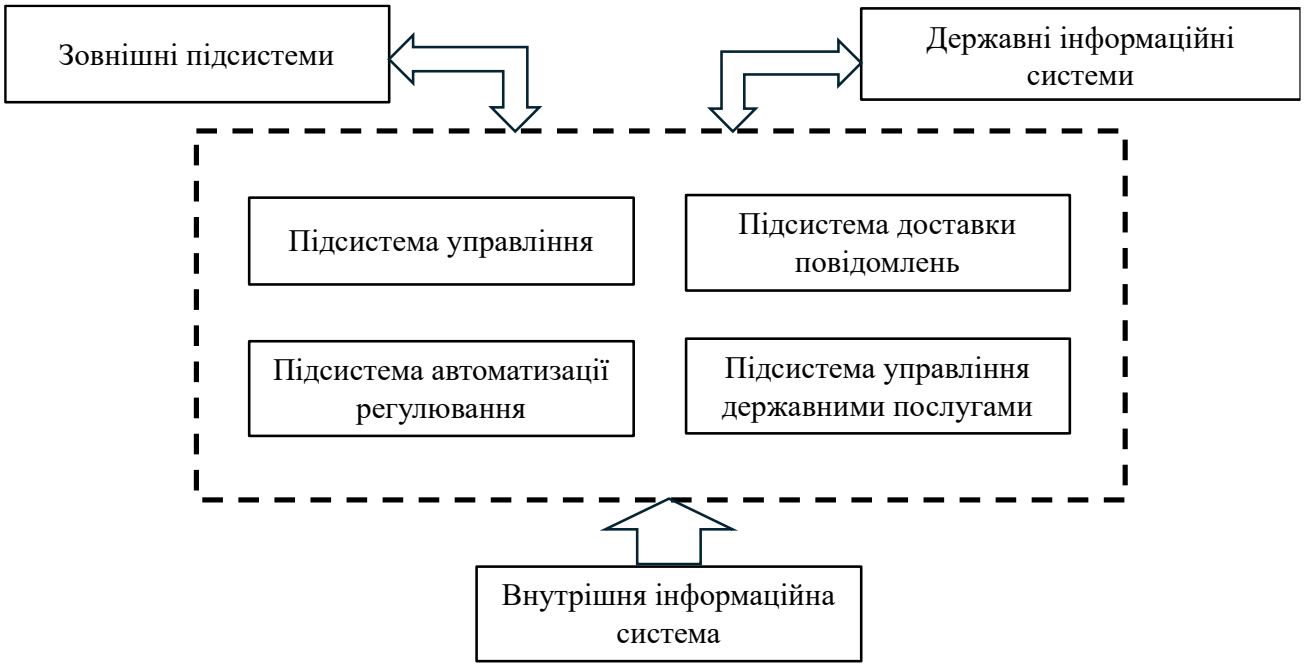

Рис. 3.2. Управління кібербезпекою на рівні органів державної влади

Джерело: складено автором.

Інтеграція процесів захисту інформації в сфері державної безпеки передбачає застосування узгоджених процедур, у яких на певних етапах використовуються спеціальні додатки. Обробка інформації на цих етапах здійснюється за допомогою додатків, а функції процесу виконуються через спеціалізовану підсистему. Цей метод інтеграції базується на технології

«WorkFlow» [53]. Пропонується використовувати модель двофакторної автентифікації державних службовців у розбудові системи кібербезпеки держави (рис. 3.3).

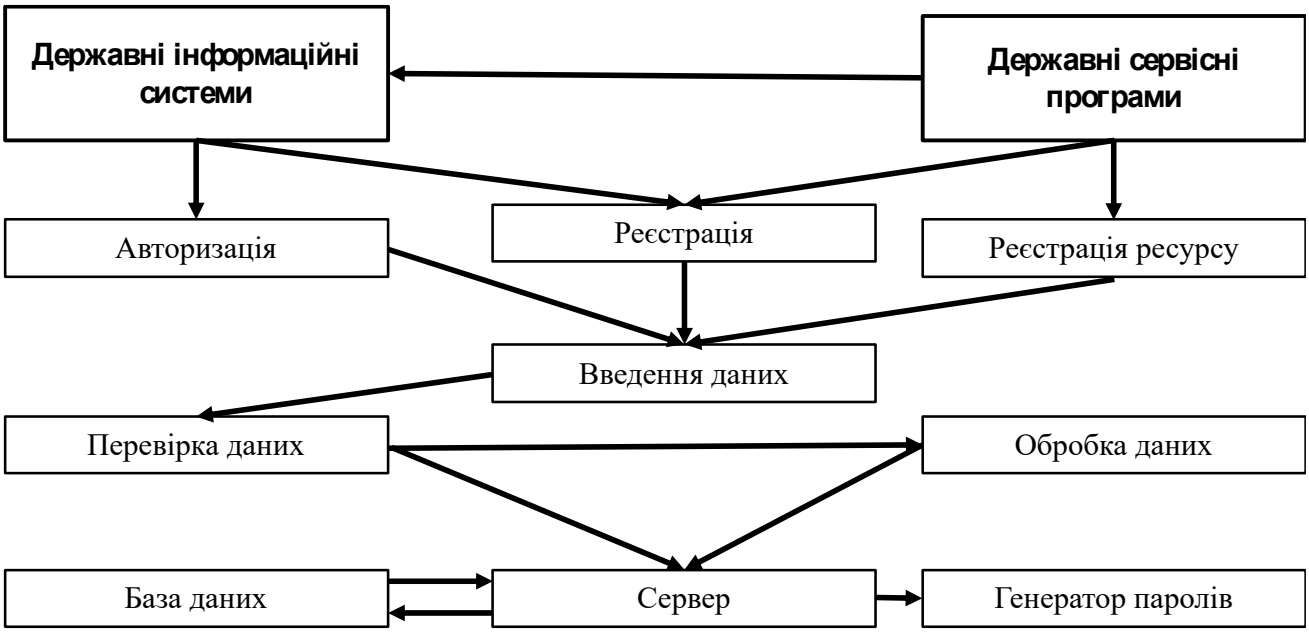

Рис. 3.3. Модель запропонованої двофакторної автентифікації державних службовців

Джерело: складено автором.

Запропонована модель базується на двох типах двофакторної автентифікації: автентифікатор у додатку та перевірка входу через мобільні додатки. Представлена модель і алгоритм захисту інформації в системі моніторингу засновані на поєднанні двох факторів: статичного і тимчасового пароля. Статичний пароль (перший фактор) встановлюється користувачем і використовується для створення облікового запису. Одноразові паролі, які виступають додатковим фактором, генеруються на сервері за описаним алгоритмом і діють протягом обмеженого часу, який становить двадцять секунд для кожного сеансу автентифікації. Повторне використання паролів заборонено, що є перешкодою для зловмисника, який намагається їх перехопити. Слід зазначити, що довжина пароля становить 6 символів і змінюється кожні

10 секунд. Враховуючи це, злом такого пароля в межах відведеного час є серйозною проблемою, оскільки потрібно знайти понад 1 мільйон комбінацій [54].

Програми, що працюють на середньому рівні, інтегрують ключові програмні компоненти. Провідні компанії активно розробляють комплексні рішення для корпоративних інформаційних систем. Ці рішення включають, наприклад, Oracle 10g, Microsoft BizTalk Server, IBM WebSphere і SAP Netweaver. Наприклад, Microsoft BizTalk Server, який реалізує функції обробки та передачі в системі електронного документообігу.

Мовний формат відіграє ключову роль у забезпеченні державної кібербезпеки процесів у технологічному аспекті. Мови програмування, які використовуються в інтегрованих інформаційних системах, стандартизовані. Ці стандарти включають Express зі STEP, мову розмітки XML і формат обміну даними EDIFACT. Мова метаданих RDFS і Мова представлення онтології OWL використовується для підтримки узгодженості в базах даних [55].

Підсумовуючи, можна констатувати, що кібербезпека на органи державного управління досягається шляхом уніфікації методів обміну даними, для чого використовуються транспортні протоколи. Протокол HTTP широко використовується в Інтернеті для організації взаємодії між клієнтом і сервером. Для пошуку потрібного сервера і встановлення зв'язку в мережевому середовищі застосовуються протоколи WSDL, SOAP і UDDI. У цьому контексті протокол HTTP є транспортним засобом для повідомлень SOAP [56].

Дослідження питань інформаційного протистояння, у тому числі визначення можливостей планування дій щодо впливу чи протидії інформаційним впливам, потребує детального аналізу основних напрямів кіберзахисту. Крім суто цивільного кіберзахисту, сучасна держава повинна мати можливість активно протидіяти кіберзагрозам, розвиваючи активні протидії. Ці події мають неабияку актуальність і значення для сучасної України [57]. В дисертаційному досліджені визначено наступні ключові напрямки:

1. Стратегія кіберінформаційної протидії системам управління. Ця стратегія сприймається як військова тактика, спрямована на ліквідацію систем контролю та ізоляцію керівних структур противника з метою зриву його військового керівництва. Таке протистояння може бути досягнуто шляхом прямого знищення вузлів управління або через порушення телекомунікаційних мереж координації управління. Спосіб протидії обирається відповідно до визначених тактичних і стратегічних завдань. Значущість кіберінформаційних операцій проти систем управління полягає в їх потенційній ефективності на початкових етапах конфлікту, створюючи основу для безкровної перемоги над ворогом. Однак такі переваги можуть бути зменшені ворогом завдяки децентралізації систем моніторингу та так званій «мережевій війні» [58]. Ці операції можна розглядати як еволюцію традиційної оперативної розвідки, хоча вони мають суттєві відмінності в тому, що зібрана інформація безпосередньо передається учасникам операції, тоді як інформація військової розвідки надходить до командних центрів, де вона аналізується і перетворюється на накази для виконання. Це передбачає адаптацію оперативної розвідки до децентралізованих систем військового управління та бойових дій, що потребує суттєвих змін у зборі, обробці та розповсюдженні розвідувальної інформації.

2. Електронне протистояння. Він відрізняється від першого напряму, який передбачає боротьбу за допомогою інформаційних систем або через них. Метою радіоелектронного протистояння є зниження інформаційних можливостей противника. Це включає боротьбу з комунікаційними мережами противника, електронну та криптографічну війну.

3. Психологічне кіберпротистояння. Цей напрям полягає у впливі на розум і психіку людини, а не на інформаційні системи. Психологічна боротьба включає маніпулювання суспільною свідомістю та поглядами різних соціальних груп. У країнах НАТО в рамках психологічної війни виділяють такі основні типи дій: деморалізація військовослужбовців, операції проти військового командування і, навіть, дії, спрямовані на управління [59].

4. Хакерська війна означає використання комп’ютерних технологій для незаконного доступу або порушення роботи ворожих систем. Хакерська боротьба здебільшого зосереджена проти компонентів комп’ютерних мереж та інформаційних ресурсів. Процеси злому характеризуються програмною природою, на відміну від апаратних атак. Багато західних експертів стверджують, що нинішнє інформаційне протистояння здебільшого зумовлене хакерською війною. Найпоширенішими інструментами хакерської війни є комп’ютерні хробаки, віруси, трояни, шкідливі програми для постійного пристрою та логічні бомби, які можна розглядати як приклади інформаційної зброї.

5. Кібернетичні та мережеві війни, які, незважаючи на свої технічні назви, мало пов’язані з інформаційними технологіями та охоплюють широкий спектр питань інформаційної війни, включаючи організаційні, тактичні, доктринальні, технічні та стратегічні аспекти. Кібервійна відіграє важливу роль у сучасному захисті державного кіберпростору, особливо в конфліктах високої інтенсивності та із застосуванням новітніх технологій [60].

6. Економічна кіберінформаційна війна, де основним форматом є інформаційна блокада. В умовах глобалізації та цифрової економіки інформаційна блокада може забезпечити прихований вплив на ворога. Це відрізняється від традиційних економічних санкцій, оскільки їх можна маскувати під випадкові хакерські атаки або збої в інформаційних системах, хоча це не виключає можливості явного державного впливу [61].

Отже, за результатами проведеного наукового дослідження, можемо зробити висновок щодо необхідності посилення державної кібербезпеки на всіх рівнях, від окремого користувача до національних державних органів. В дисертаційній роботі запропоновані конкретні рекомендації щодо захисту від кіберзагроз.

Останнім часом спостерігається суттєва зміна комплексу факторів, що визначають комп’ютерну злочинність на державному рівні. Крім традиційних соціальних, економічних, правових, кадрових, організаційних і технічних

аспектів все більшого значення набувають політичні фактори. До них належать геополітичні аспекти, зокрема військово-політичні, глобальні економічні та міжнародні політичні елементи, а також політичні та спостережні фактори, пов'язані з недостатнім соціальним і державним контролем над кіберпростором. Інші важливі чинники включають політико-кримінальний (включаючи кібертероризм, кіберекстремізм і хактивізм), політико-інформаційний (кібершпигунство) та політико-інституційний (зловживання ІТ-технологіями). Ключовим моментом еволюції кіберзлочинності, що перетворює її на технотронний злочин, є її самовизначення. Цей процес означає здатність комп'ютерної злочинності до автономного регенерування, тобто до самостійного відтворення злочинів у соціальному середовищі. Ці прояви визначають перспективи подальших досліджень сучасних кіберзагроз та заходів щодо їх запобігання.

3.2. Напрями вдосконалення адміністративно-правових засад кібербезпеки в сфері забезпечення стійкості функціонування фінансових установ під впливом кіберзагроз

Сучасний розвиток цифрових технологій, електронних комерційних операцій та автоматизації діяльності фінансових установ надає низку переваг для ефективного управління та зручності користувачів фінансовими послугами. Проте актуальною проблемою залишається забезпечення кібербезпеки, оскільки цифрове середовище залишається вразливим у сучасному технологічному світі.

Варто зазначити, що кібератаки загрожують різним секторам, зокрема енергетичним компаніям, промисловим виробникам, логістичним підприємствам, телекомунікаційним компаніям та розробникам програмного забезпечення [172].

Однак останнім часом найсерйозніші атаки спрямовані на фінансовий сектор України, зокрема великі банки, які істотно впливають на фінансову систему країни. Банки надають базові фінансові послуги населенню та зберігають чимало конфіденційної інформації, що робить їх привабливою мішенню для кіберзлочинців. Необхідно пам’ятати, що кіберзагрози не обмежуються великими компаніями, навіть невеликі підприємства можуть стати жертвами кібератак, зазнаючи серйозних фінансових та репутаційних втрат [173].

За останнє десятиліття зросла кількість зловмисних атак на фінансові установи, біржі криптовалют і різноманітних постачальників фінансових послуг. Тому пошук ефективних технологічних рішень і покращення функціонування фінансових установ є вирішальним завданням для їх подальшого розвитку.

До найпопулярніших технологічних рішень можна віднести:

змінні цифрові системи зберігання, подібні до хмарних систем;

використання аналітики великих даних;

впровадження систем резервного копіювання даних;

шифрування даних криптографічними методами.

Однак, незважаючи на масштабні заходи, спрямовані на захист цілісності фінансових процесів і безпеки даних, ключовим фактором є поєднання всіх аспектів безпеки. Він включає пом’якшення та зменшення ризиків, мінімізацію ризиків людської помилки, використання правової бази для кібербезпеки, підключення до глобальних фінансових мереж і децентралізацію внутрішньої серверної системи.

Впровадження безпеки програмного забезпечення на найнижчому архітектурному рівні є найефективнішим засобом забезпечення стабільності роботи фінансових установ. Він передбачає створення технологічних рішень цифрового захисту на апаратному рівні. Конфлікт в Україні викликав глобальну конкуренцію між різними світовими державами. Це призвело до необхідності посилення кібербезпеки та розробки ефективних механізмів і моделей управління для фінансових установ.

Отже, актуальним є розгляд впливу кібербезпеки на функціонування фінансових установ та розроблення пропозицій щодо напрямків удосконалення адміністративно-правових засад його забезпечення. Зокрема, адміністративно-правове забезпечення впливу кібербезпеки на стабільність фінансових установ має передбачати використання та впровадження різноманітних цифрових технологій, включаючи апаратне та програмне забезпечення.

Наприклад, такий вчений як А. Хакім зазначає, що поточна політика кібербезпеки є головним пріоритетом у всьому світі. Це пов'язано зі стрімкою реструктуризацією традиційної економіки в цифрову. Це призводить до неадекватного стану безпеки зберігання даних, документації та життєзабезпечення системи фінансової установи [62].

На думку дослідника М. Ходули, кібербезпека є глобальним викликом для всього світу. Він повинен використовувати децентралізовані системи зберігання даних і впроваджувати низку криптографічних методів у своїй бізнес-діяльності для забезпечення стабільності подальших операцій [63].

С. Левицька зазначає, що ключовим фактором кібербезпеки є протидія кібератакам на веб-ресурси, мобільні додатки та клієнтів фінансової установи. Це передбачає налаштування програмного забезпечення та технологій для веб-сайтів [64].

Ш. Дулей в свойому дослідженні [65] показує, що впровадження ефективної безпеки серверів і центрів обробки даних не може гарантувати повну безпеку. З цієї причини дослідниця пропонує використовувати хмарне сховище для більш надійного управління персональними даними та фінансовими транзакціями.

Більшість інформаційних гігантів сучасного світу, як зазначає Г. Бучак, використовують власну цифрову інфраструктуру для надання послуг для підвищення якості безпеки фінансових установ [66].

Проте в контексті появи інноваційних технологій і швидкого розвитку технічних засобів забезпечення повного захисту персональних даних є складним завданням [62].

За даними Ю. Ніконенко, найпопулярнішим засобом забезпечення захисту персональних даних є використання систем шифрування та єдиної системи блокчейн [67].

Д. Мельник погоджується з цим аргументом і вважає, що встановлення блокчейну для глобальної фінансової мережі та його використання для усунення можливості викрадення або фальсифікації даних фінансових установ є інноваційним рішенням для забезпечення стабільності фінансових установ [68].

А. Котідіс та С. Шрефт вважають, що практика розробки та інтеграції блокчейнів стає все більш популярною та може бути застосована до державного управління, ключових державних установ та фінансового сектора, які будуть надійно захищені від зовнішнього впливу [69].

В. Церасі погоджується з цією думкою та зазначає, що практика впровадження постійно розвиватиметься та охоплюватиме нові сектори фінансового середовища [70].

А. Сумець стверджує, що важливим фактором кібербезпеки фінансових установ є проведення спеціалізованого навчання персоналу цифровій грамотності та роботі з інформаційними технологіями. Хоча автоматизація популяризується, більшість кібератак є успішними завдяки людському фактору [71].

А. Новак досліджуючи це питання, стверджує, що створення інструкцій для роботи у фінансовій установі та проведення навчальних заходів є не менш важливим, ніж використання сучасних технологій цифрової безпеки [72].

Отже, серед науковців питання впливу кібербезпеки на стабільність діяльності фінансових установ та вдосконалення її адміністративно-правового забезпечення вбачається важливим та актуальним і потребує подальшого дослідження.

Тому актуальним є проведення дослідження, спрямованого на аналіз сучасних тенденцій у кібербезпеці, її впливу на стабільність фінансових установ та вдосконалення відповідного адміністративно-правового забезпечення. Очевидно необхідно також вивчити підтримку життєво важливих функцій

кібербезпеки в контексті зростання цифрових загроз. Важливим є дослідження практичного досвіду великих фінансових установ у формуванні власної стратегії кібербезпеки та визначення особливостей адміністративно-правових засад для підтримки цих інструментів. Важливим напрямком аналізу є визначення сучасних тенденцій у цифрових технологічних рішеннях фінансових установ, спрямованих на забезпечення власної безпеки в цифровому просторі та її подальшу підтримку шляхом впровадження ефективних цифрових та інноваційних рішень. Для цього необхідно проаналізувати теоретичні, методологічні та практичні підходи до кіберзахисту та цифрових інструментів, які допомагають підтримувати стабільність фінансових установ, та запропонувати шляхи вдосконалення адміністративно-правових засад щодо їх ефективного функціонування.

Вважаємо, що концепція кібербезпеки, запропонована Д. Ацтажею разом з іншими дослідниками, є ефективним засобом для мінімізації ризиків у цифровому середовищі. Вона охоплює набір дій і технологічних засобів для забезпечення ефективності роботи веб-ресурсу з доступом до мережі Інтернет. Сучасний розвиток цифрових технологій спонукає до пошуку ефективних та ефективних рішень для підвищення конфіденційності персональних даних та захисту організаційних та комерційних бізнес-процесів установи, організації чи будь-якої структури від зовнішнього втручання. Передача даних за допомогою мережевих протоколів OSI є фундаментальним чинником у створенні кібербезпеки. Вона має сім рівнів, що відповідають за з’єднання між різними цифровими носіями. Крім того, фінансові установи чи інші організації можуть працювати в своїх локальних мережах, для яких не потрібні додаткові підключення до мережі Інтернет. Проте в таких умовах кібербезпека пов’язана з надійністю налаштування апаратного та програмного забезпечення для потоку даних та структурування інформаційного середовища [73].

Сучасний технологічний розвиток фінансового ринку призвів до значного зростання кількості електронних комерційних послуг, що, безумовно, покращує якість обслуговування населення та юридичних осіб за допомогою електронних

транзакцій. Тим не менш, забезпечення ефективності управління даними, перевірка легітимності транзакцій з даними, захист від зовнішнього втручання є головними пріоритетами для фінансових установ, а також для держави. Останній містить набір електронних реєстрів, які можна використовувати як інструменти для управління цифровою безпекою.

Концепція впливу кібербезпеки на стабільність фінансових установ має першочергове значення, оскільки визначає правила їх функціонування в цілому. На думку І. Сейлана, діяльність фінансової установи можлива лише за умови попереднього планування правового характеру її діяльності та захисту персональних даних відповідно до вимог регуляторних та наглядових органів. Наприклад, при плануванні фінансової установи як комерційної організації визначається низка цифрових рішень для подальшої діяльності у фінансовому середовищі. По-перше, планується створення автоматизованих систем обліку, перевірки та функціональності фінансових операцій з валютою, дорогоцінними металами та іншими фінансовими активами. По-друге, таким організаціям необхідно створити існуючу цифрову інфраструктуру, яка може використовувати такі хмарні технології, як Oracle, Dropbox та різні інші альтернативні технологічні рішення [74].

Суттєвим фактором забезпечення планування діяльності фінансової установи є мінімізація та запобігання ризикам, створення відповідного структурного підрозділу, відповідального за вирішення цих питань [75, 76]. Відповідно до цього підходу, вплив кібербезпеки на стабільність функціонування фінансової установи є вирішальним і вимагає високоякісних технологічних рішень.

У табл. 3.2 наведено детальну інформацію стосовно впливу кібербезпеки на стабільність функціонування фінансової установи та запропоновано заходи щодо запобігання відповідним ризикам.

Таблиця 3.2

Вплив кібербезпеки на стабільність функціонування фінансових установ, аналіз і заходи щодо запобігання ризикам

Параметр	**Вплив на стабільність функціонування фінансових установ**	**Заходи щодо підвищення кібербезпеки**
Кібератаки	Підвищений ризик фінансових втрат, втрати репутації та ймовірність фінансового краху	Регулярні аудити безпеки, навчання персоналу, розробка плану відновлення
Законодавство та нормативні акти	Регулювання кібербезпеки як вимога до фінансових установ, вплив на операції	Дотримання вимог і створення політик безпеки
Внутрішня безпека	Посилення заходів безпеки та контролю для запобігання кібератакам	Моніторинг та вдосконалення систем безпеки
Технологічні ризики	Вплив інноваційних технологій на підвищення/зменшення ризику	Оцінка ризиків, вдосконалення процедур, застосування передових технологій
Взаємозв’язок установ	Співпраця та обмін інформацією між фінансовими установами для колективного захисту	Розробка стандартів і співпраця для кібербезпеки
Моніторинг і відновлення	Системи моніторингу та відновлення резервних копій для виявлення та усунення кіберзагроз	Постійний моніторинг і плани відновлення після нападу

Джерело: складено автором.

Заходи, наведені в табл. 3.2, широко використовуються глобальними платіжними системами та різними фінансовими установами, які надають фінансові послуги та виконують розрахункові функції. Однак, залежно від їх розташування та регіонів діяльності, на них поширюються норми, що регулюють цифрову безпеку їх власної інфраструктури та фінансових операцій. Зокрема, Міжнародна організація зі стандартизації (ISO) має набір вимог до якості стандартів кібербезпеки та ключових рішень. Вони включають шифрування даних, щоквартальні оновлення та сервісне обслуговування, моніторинг їх центрів обробки даних та використання різноманітних антивірусних програм для забезпечення безперебійної роботи фінансових установ тощо. Федеральне агентство з кібербезпеки та безпеки інфраструктури США (Certified Information Systems Auditor, CISA) було створено для розслідування найбільш серйозних кібератак у сучасному цифровому світі. Крім того, CISA прагне покращити загальне цифрове середовище шляхом розробки відповідного програмного забезпечення та посилення кіберзахисту фінансових установ.

Вплив кібербезпеки на стабільну діяльність фінансових установ важко переоцінити, оскільки від неї залежить безперервне функціонування всієї структури. Водночас, вона має відповідати стандартам як на внутрішньому рівні – правове середовище країни, так і на глобальному рівні – міжнародні організації, які створюють відповідні нормативи.

Технологія блокчейн стала інноваційним засобом забезпечення стабільності функціонування фінансових установ і була широко інтегрована на всіх рівнях управління. Використання такої системи у фінансових установах значно знижує ризик зовнішнього впливу та зловмисних цифрових дій. У Китаї, Сполучених Штатах Америки, Німеччині та Швейцарії системи блокчейн зазвичай застосовуються до більшості корпоративних організацій і фінансових установ для забезпечення їх стабільної діяльності.

Конфлікт в Україні створив низку глобальних викликів для цифрової безпеки. Українські банки, як одні з найбільших фінансових установ країни, несуть відповідальність за захист персональних даних клієнтів і забезпечення

стабільності своїх пропозицій послуг. Однак, вони також є об’єктом національної стратегічної безпеки у фінансовому контексті. Тому своєчасне прийняття оперативних і технічних рішень, а також планування кібербезпеки забезпечили стабільність фінансової системи України під час світових економічних і політичних криз.

Ключовими факторами впливу на кібербезпеку стали управлінські рішення, спрямовані на диверсифікацію ризиків та їх уникнення, використання хмарних сервісів і технологій автентифікації, а також посилення фінансового моніторингу.

Крім того, під час війни кожен великий український банк провів серію тренінгів з цифрової грамотності та навичок цифрової безпеки. Основні заходи, вжиті найбільшими банківськими установами під час війни в Україні у 2022-2023 роках, наведено в табл. 3.3.

Таблиця 3.3

Заходи та технічні рішення, вжиті українськими банками для посилення кібербезпеки під час війни

Назва банку	Заходи із забезпечення кібербезпеки	Технічні рішення
Приватбанк	Встановлення криптографічного з'єднання для безпечного обміну даними між відділеннями та центральним сервером банку	Розташування власних дата-центрів у Європі забезпечує сховища з надійним шифруванням даних

Закінчення таблиці 3.3

Назва банку	Заходи із забезпечення кібербезпеки	Технічні рішення
Монобанк	Впровадження мережевих брандмауерів та систем перехоплення вторгнень для виявлення та блокування несанкціонованого доступу до систем банку	Застосування багаторівневої ідентифікації користувачів та створення децентралізованих систем баз даних, що працюють у хмарному сховищі
Універсальний банк	Підвищення безпеки мережі шляхом регулярного моніторингу мережі та виявлення незвичайної активності	Використання системи резервного копіювання даних і автоматичного відновлення в разі кібератаки
Ощадбанк	Удосконалення процедур автентифікації та авторизації персоналу	Забезпечення фізичної безпеки серверних кімнат та проведення інформаційних кампаній серед користувачів для захисту їхніх даних та покращення якості їх використання
Укргазбанк	Шифрування даних під час транзакцій та їх зберігання на серверах з обмеженим доступом	Перенесення дата-центрів до країн із суворішими стандартами кібербезпеки як ще один рівень захисту

Джерело: складено автором.

Заходи, вжиті українськими банками під час війни в Україні, стали вирішальним фактором у забезпеченні фінансової стабільності та функціонування установ.

Особливо вагомим є досвід ПриватБанку. З 2019 по 2020 рік банк реалізував низку цифрових рішень, включаючи зміни в розміщенні центрів обробки даних та інтеграцію різноманітних хмарних технологій для забезпечення безперервності своїх операцій. У 2022 році банк зміг забезпечити резервне копіювання та шифрування даних за допомогою криптографії. Він використовував кілька протоколів передачі даних низького рівня та зашифрував конфіденційну інформацію. Досвід найбільшого державного банку України може слугувати реальним прикладом функціонування фінансової установи в найбільш кризових ситуаціях.

Антикризовий менеджмент, спрямований на забезпечення цифрового захисту, є життєво важливим управлінським фактором для стабільності роботи фінансової установи. В сучасному світі автоматизація має менше недоліків, але ефективність організаційного та адміністративного середовища залишається важливою проблемою. Це передбачає підвищення компетентності співробітників шляхом навчання та інструктажів у різних кризах.

Комплексне управління кібербезпекою, як на технологічному, так і на управлінському рівнях у сучасних фінансових установах, відіграє ключову роль з точки зору національної безпеки, клієнтів і корпоративних аспектів. З цієї причини це особливо важливо в контексті прискореного розвитку технологій шифрування даних, таких як TDEA. Такі технології шифрування даних передбачають симетричне шифрування. Цей метод спрямований на приховування ключа, який використовується як для шифрування, так і для дешифрування.

Однак у 2023 році з розвитком штучного інтелекту цей метод був вдосконалений шляхом впровадження додаткових технічних засобів. Останній включає шифрування AES, інноваційний захист внутрішнього доступу до файлів. Цей метод використовується урядом Сполучених Штатів Америки та

кількома фінансовими установами для посилення цифрового захисту важливої інформації.

Таким чином, сучасний вплив кібербезпеки на стабільність функціонування фінансових установ відіграє ключову роль, оскільки визначає їх планову та операційну діяльність. Методи шифрування даних і складні алгоритми, які можна побудувати в системах блокчейн, сприяють вдосконаленню сучасного цифрового захисту.

Українські фінансові установи продемонстрували ефективне управління технологічними рішеннями для мінімізації ризиків від існуючих кібератак.

Однак, незважаючи на ефективність поточних заходів кібербезпеки у фінансових установах, ця сфера потребує постійного оновлення через швидкий розвиток цифрових технологій, штучного інтелекту та технологій баз даних [77].

Отже, на основі проведеного наукового дослідження можна стверджувати, що практика використання технічних засобів кібербезпеки є ключовим засобом забезпечення стабільності функціонування фінансових установ. Ці інструменти включають криптографію, шифрування, ефективну конфігурацію сервера, переміщення центру обробки даних, покращення якості автентифікації та інші методи. В умовах сучасного технологічного розвитку питання ефективного використання цифрових інструментів і збереження цілісності даних є першочерговим для будь-якої країни, оскільки це питання національної та стратегічної безпеки.

Д. Хукс разом з іншими дослідниками прогнозують, що майбутні перспективи захисту даних все більше зміщуватимуться в бік блокчейн-систем. Останній може ефективно зберігати інформацію як про клієнтів фінустанови, так і про низку внутрішньоорганізаційних документів. За його словами, практика посилення кібербезпеки фінустанов повинна бути інтегрована в глобальну фінансову мережу. Блокчейн стане основою цієї мережі [78].

Крім того, з розвитком технологій аналізу великих даних впровадження захисту даних стає більш простим завданням для сучасного світу, що вимагає подальших аналітичних і технічних досліджень. Досвід розвинутих країн

показує, що впровадження систем блокчейну як у фінансових установах, так і в управлінні державними організаціями є ефективним методом уникнення корупції та кібератак. Вони служать найкращим способом забезпечення безпеки цифрових даних.

Критичні аспекти впливу кібербезпеки на стабільність фінансових установ включають:

- управління зашифрованими протоколами;
- використання ряду SSL- сертифікатів;
- можливість формування передачі даних на всіх рівнях моделі OSI з відповідним шифруванням.

Ф. Янг зазначає, що для ефективної передачі даних необхідно використовувати приватні сервери та мати доступ до центрів обробки даних з додатковим захистом у вигляді хмарного сховища, що може включати такі заходи:

- експертиза хмарних систем зберігання, інтегрованих безпосередньо в діяльність фінансових установ;
- аналіз характеристик обладнання;
- порівняльна оцінка провідних продуктів інформаційної індустрії, таких як Oracle, Dropbox або будь-яких інших, доступних у фінансових установах.

Війна в Україні значно загострила геополітичну боротьбу в світі, де кіберпростір став окремим полем битви. Проведений у дисертаційній роботі аналіз практичних і технічних рішень українських фінансових установ (банків) для забезпечення ефективності кібербезпеки може слугувати моделлю для вдосконалення політики фінансових установ у всьому світі.

О. Бородіна та низка інших вчених вважають, що сучасні фінансові установи повинні посилити свою цифрову інфраструктуру. Вони повинні мати кілька рівнів захисту як персональних даних клієнтів, так і власних систем [79]. Досвід країн Європейського Союзу може бути цікавим для вивчення наявності локальної фінансової мережі європейського типу з резервними дата-центрами, серверами та рядом цифрових рішень для ефективної роботи. Тому аналіз

можливостей систем резервного копіювання, додаткових джерел живлення та визначення основних характеристик цієї інфраструктури на апаратному рівні може мати технічне значення для фінансових установ у всьому світі.

3.3. Перспективні напрями вдосконалення нормативно-правового регулювання адміністративно-правових засад забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України

В Загальному огляді і аналізі правової бази української кібербезпеки, підготовленому Міжнародною фундацією виборчих систем (IFES) за підтримки Агентства США з міжнародного розвитку (USAID), Міністерства міжнародних справ Канади та британської допомоги (UK aid), вказується на слабкість існуючих правових норм, пов’язаних з регулюванням кібербезпеки, які можна значною мірою пояснити відсутністю всеосяжної правової бази та існуванням ряду прогалин і неоднозначностей у законодавстві [214].

Поведений в дисертаційному дослідженні аналіз наукової літератури, аналітичних публікацій широкого кола експертів і чинної нормативно-правової бази надали можливість сформулювати наступні основні проблеми та актуальні виклики сьогодення в сфері забезпечення кібербезпеки та кіберзахисту, протидії кіберзагрозам, таким як кібератаки та кіберзлочинність, в умовах воєнного стану та повоєнної відбудови України. На підставі вивчення передового закордонного досвіду запропонувати шляхи їх вирішення та створення на майбутнє сучасної ефективної системи забезпечення кібербезпеки та кіберзахисту, що на даний час є вкрай актуальним питанням для нашої держави.

Недостатній рівень кіберзахисту критичної інфраструктури, який зумовлений такими факторами:

багато об’єктів критичної інфраструктури (енергетика, транспорт, банківська система) не мають належного рівня кіберзахисту;

відсутність регулярних аудитів кібербезпеки;

використання морально застарілого обладнання та програмного забезпечення;

вплив геополітичних факторів (використання кібератак як інструменту гібридної війни та постійні атаки з боку країни-агресора, спрямовані на дестабілізацію внутрішньої ситуації).

Так, у Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447, зазначається, що загрозами кібербезпеці України, поміж іншого є гібридна агресія російської федерації проти України у кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки російської федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності [4].

М. Делембовський, В. Ткаченко та Д. Мельник показують, що з 2017 по 2022 рік кількість значущих кібератак на критичну інфраструктуру України постійно зростає. Відсоткове збільшення варіюється, але загальна тенденція вказує на постійний ріст, що підкреслює необхідність посилення заходів з кібербезпеки та модернізації захисних систем. [146].

Вказану проблему ґрунтовно досліджує та чітко формулює Мануілов Я. С.: за наслідками повномасштабного вторгнення рф в Україну у 2022 року кількість кібератак із боку рф збільшилася вдвічі, а перед річницею воєнної агресії – у шість разів. Тобто у зв’язку зі збільшенням кількості та масштабів кібернападів як одного із проявів агресії російської федерації проти України набуває актуальності потреба вдосконалення нормативного забезпечення питань кіберзахисту інформаційних, електронних, комунікаційних й інформаційно-комунікаційних систем та об'єктів критичної інформаційної інфраструктури для

здійснення ефективного стримування та протидії агресії проти України в кіберпросторі [145].

О. Янковський переконує: необхідність змін підтверджена атаками на об'єкти критичної інфраструктури, сумнозвісним NotPetya та багатьма іншими інцидентами, які протягом останніх років створили Україні сумнівну репутацію одного з головних кіберполігонів [147].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

доповнити Закон України «Про основні засади забезпечення кібербезпеки України» [2] нормами щодо:

обов'язку для суб'єктів критичної інфраструктури впроваджувати системи управління кіберризиками. Наприклад, шляхом внесення до частини другої статті 8 зазначеного Закону нових абзаців такого змісту:

«Державні установи зобов'язані використовувати лише сертифіковане програмне та апаратне забезпечення, яке відповідає вимогам національної безпеки. Використання продуктів, розроблених у країнах, що представляють геополітичну загрозу, забороняється.

Суб'єкти критичної інфраструктури зобов'язані впроваджувати системи управління кіберризиками відповідно до стандартів ISO/IEC 27001 та забезпечувати щорічний аудит ефективності цих систем.»;

поширення завдань та функцій CERT-UA на здійснення моніторингу стану кібербезпеки критичної інфраструктури. Наприклад, шляхом внесення до частини першої статті 9 зазначеного Закону нового підпункту 10 такого змісту:

«10) здійснення постійного моніторингу стану кібербезпеки об'єктів критичної інфраструктури та надає обов'язкові рекомендації для усунення виявлених недоліків.»;

доповнити Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [5] нормою, що зобов'язує власників критичної інфраструктури використовувати багатофакторну автентифікацію для доступу до інформаційних систем, з обов'язковим використанням біометричної

автентифікації для запобігання несанкціонованому проникненню. Наприклад, шляхом внесення до статті 9 зазначеного Закону нової частини такого змісту:

«Суб'єкти критичної інфраструктури зобов'язані застосовувати багатофакторну автентифікацію, що включає комбінацію пароля та біометричних даних, для доступу до інформаційно-телекомунікаційних систем, які забезпечують функціонування таких об'єктів.»;

передбачити державне фінансування для модернізації систем кіберзахисту на об'єктах критичної інфраструктури. Наприклад, шляхом внесення змін до Бюджетного кодексу України, що передбачали б щорічне фінансування з державного бюджету для реалізації програм модернізації кіберзахисту критичної інфраструктури, зокрема на оновлення програмного забезпечення та обладнання;

розробити державну програму реагування на кіберзагрози в умовах геополітичних конфліктів. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«Розробити та подати Кабінету Міністрів України на затвердження державну програму реагування на кіберзагрози в умовах геополітичних конфліктів, що передбачатиме:

плани реагування на кібератаки з боку іноземних держав;

підготовку спеціалізованих команд для моніторингу та реагування на кібератаки;

організацію взаємодії з міжнародними організаціями для оперативного обміну інформацією про кіберзагрози;

участь у спільних навчаннях та тренінгах з кіберзахисту з НАТО, ЄС та в рамках заходів ООН;

розробку спільних з НАТО та ЄС стратегій протидії геополітичним кіберзагрозам»;

встановити вимогу обов'язкової сертифікації об'єктів критичної інфраструктури за міжнародними стандартами кібербезпеки. Наприклад, шляхом доповнення пункту 4 Порядку віднесення об'єктів до критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384), [148] новим абазом другим такого змісту:

«Кожен об'єкт критичної інфраструктури підлягає сертифікації відповідно до міжнародних стандартів кібербезпеки. Сертифікація повинна оновлюватися кожні два роки.»;

передбачити створення спеціалізованих команд реагування на інциденти кібербезпеки (CSIRT) для кожної галузі критичної інфраструктури. Наприклад, доповнивши завдання 5 Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури, затвердженого розпорядженням Кабінету Міністрів України від 19 вересня 2023 р. № 825, [149] новим заходом 4 такого змісту:

«Кожна галузь критичної інфраструктури повинна створити спеціалізовані команди реагування на кіберінциденти (CSIRT) для оперативного моніторингу та реагування на загрози.».

Недостатнє фінансування кібербезпеки, і як наслідок:

низький рівень бюджетного фінансування програм кібербезпеки;

відсутність належного фінансування для оновлення ІТ-інфраструктури;

відсутність інвестицій у модернізацію систем захисту та навчання персоналу.

Так, Віце-прем'єр-міністр України з інновацій, розвитку освіти, науки та технологій – Міністр цифрової трансформації Михайло Федоров, вказує, що фінансування цифрового сектору (включно з кібербезпекою) критично мале: у той час як витрати в Естонії, Данії, Норвегії коливаються на рівні від 1% до 4% держбюджету, в Україні в 2021 році вони склали 0,15% [150].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

у Законі України про Державний бюджет України запровадити окрему статтю видатків для фінансування державних програм кібербезпеки, зокрема модернізації інфраструктури, навчання персоналу, впровадження систем раннього реагування та моніторингу;

встановити обов'язок щорічного фінансування кібербезпеки державних установ. Наприклад, доповнивши статтю 13 Законі України «Про основні засади забезпечення кібербезпеки України» [2] новою частиною такого змісту:

«Держава зобов'язана забезпечувати фінансування заходів з кібербезпеки для захисту державних установ, критичної інфраструктури та державних інформаційних ресурсів.»;

передбачити спрощену процедуру закупівель у сфері кібербезпеки. Наприклад, виклавши абзац п'ятий підпункту 5 частини другої статті 4 Закону України «Про публічні закупівлі» [151] у такій новій редакції:

«спрощена закупівля – для замовників, визначених у пункті 4 частини першої статті 2 цього Закону*, а також для всіх замовників коли закупівлі, пов'язані з модернізацією систем кібербезпеки*, якщо вартість предмета закупівлі товару (товарів), послуги (послуг) менше ніж 1 мільйон гривень, а робіт - 5 мільйонів гривень;»;

сприяти державно-приватному партнерству для фінансування проектів з кібербезпеки. Для цього необхідно розширити перелік сфер, у яких застосовується державно-приватне партнерство, включивши до нього кібербезпеку. Пропонуємо в Законі України «Про державно-приватне партнерство» [152]:

частину першу статті 4 доповнити новим абзацом такого змісту:

«кібербезпека;»;

частину першу статті 18 доповнити новим абзацом такого змісту:

«Проекти з кібербезпеки можуть фінансуватися на умовах державно-приватного партнерства з можливістю податкових пільг для приватного сектора.».

Дефіцит кваліфікованих спеціалістів у сфері кібербезпеки в Україні, зокрема:

недостатня кількість кіберфахівців для роботи в державних та приватних структурах;

відсутня обов'язкової сертифікації для працівників у сфері кібербезпеки.

В. Грезєв, констатує: в Україні спостерігається дефіцит спеціалістів у вузькоспеціалізованих галузях, особливо у сфері комунікацій, діджиталу, маркетингу та інженерії для оборонного комплексу [153].

Згідно з даними компанії ISC2, у 2024 р. глобальне зростання спеціалістів в кібербезпеці вперше за шість років (відколи компанія почала оцінювати чисельність робочої сили з 2018 р.) сповільнилося, тоді як кіберзагрози продовжують зростати [154].

Вже зараз дефіцит кіберпрофі у світі перевищує 3,4 млн людей згідно з оцінками компанії ISC2 [156].

24 січня 2024 р. старший технічний радник CISA (Cybersecurity and Infrastructure Security Agency, Агентство з кібербезпеки та безпеки інфраструктури США) Д. Кейбл у своєму дописі на сайті CISA підкреслив, що шлях покладання кібербезпеки лише на кібербезпекових фахівців ніколи не дасть потрібного безпекового ефекту. На його думку, ключова зміна, яка має відбутись в освіті – при навчанні програмістів кібербезпека має перестати бути факультативною, не обов'язковою дисципліною. Він вказує на декілька проблем, чому така ситуація зберігається:

• безпека є вибірковим предметом;

• університети мають обмежені ресурси;

• викладачі не мають відповідного досвіду;

• галузь не висуває потреби в таких знаннях [201].

Дефіцит фахівців у сфері кібербезпеки – критична проблема в усьому світі, й, на жаль, Україна не виняток. Проблема в галузі кібербезпеки набагато серйозніша, ніж нам здається. За даними Technology Review Массачусетського технологічного інституту, лише один з чотирьох кандидатів, які подають заявки

на вакансії фахівців з кібербезпеки, – кваліфіковані. Підготовка кадрів не встигає за запитом ринку, тому необхідні позиції заповнюються людьми із недостатнім рівнем підготовки», – зазначив І. Легкодимов [155].

Як пояснив Ігор Легкодимов, за останні два роки ситуація змінилася не в кращий бік. З одного боку, із початком повномасштабної агресії росії проти України збільшилась кількість атак та інцидентів у кіберсфері, роль фахівців у кібербезпеці зросла (зокрема через страх власників компаній стати жертвою злочинців та певних вимог до держкомпаній). Цей практичний досвід дав певний ріст якості спеціалістів. Але з другого боку, багато спеціалістів приєдналися до лав ЗСУ, де здобувають інший досвід захисту; багато хто виїхав з України та змінив роботу на новому місці, і часто це не віддалена робота в українських компаніях, а робота у іноземних компаніях. Також непоодинокі випадки, коли один спеціаліст працює в декількох компаній на півставки, закриваючи «гарячі» питання, точніше займається «гасінням пожеж», що не веде до підвищення якості роботи та кількості спеціалістів [155].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

запровадити надання державних стимулів для перепідготовки працівників у сфері кібербезпеки. Наприклад, доповнивши статтю 15 Закону України «Про зайнятість населення» [157] новою частиною такого змісту:

«2. Держава компенсує витрати роботодавців на перепідготовку працівників у сфері кібербезпеки в рамках державних програм зайнятості.»;

запровадити державну програму підготовки та перепідготовки кадрів у сфері кібербезпеки. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити такі завдання:

«Створення безкоштовних освітніх курсів і тренінгів для студентів і фахівців»;

«Розробка програм підвищення кваліфікації у партнерстві з міжнародними організаціями (CISCO, Microsoft)»;

«Запровадження грантової підтримки для викладачів, які працюють у сфері кібербезпеки»;

«Запровадження підготовки фахівців у сфері кібербезпеки через створення навчальних центрів за підтримки приватних компаній».

Високий рівень кіберзагроз, зокрема:

часті DDoS-атаки, спрямовані на державні та приватні установи;

використання фішингу, соціальної інженерії (використання хакерами психологічних методів для отримання доступу до даних), вірусів-шифрувальників для крадіжки даних;

атаки на об'єкти критичної інфраструктури з боку іноземних хакерів.

Так, згідно зі Статистичним звітом за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року, протягом 2022 року було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році [159].

Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA, яка діє при Держспецзв’язку, в 2024 році опрацювала 4315 кіберінцидентів. Це на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз [160].

У Звіті PE 733.549 «Війна Росії проти України: хронологія кібератак», підготовленому Дослідницькою службою Європейського парламенту в жовтні 2022 р., надається детальний огляд російських кібератак проти України, підкреслюючи їх інтенсивність та вплив на критичну інфраструктуру країни [161].

З метою створення умов для подолання зазначеної проблеми пропонуємо:

розширити перелік обов’язків державних органів щодо моніторингу та реагування на кіберзагрози. Для цього статтю 11 Закону України «Про основні засади забезпечення кібербезпеки України» [2] доповнити новою частиною такого змісту:

«Державні органи, що відповідають за забезпечення кібербезпеки, повинні здійснювати постійний моніторинг кіберзагроз та вживати заходів для запобігання кіберінцидентам. Це включає використання технологій штучного інтелекту для виявлення та запобігання атакам у режимі реального часу.»;

встановити обов'язковість проведення тестування на проникнення (penetration testing) для об'єктів критичної інфраструктури. Для цього частину четверту статті 21 Закону України «Про критичну інфраструктуру» [137] доповнити новим підпунктом такого змісту:

«3^1) щороку проводити тестування на проникнення, що має підтверджувати захищеність інформаційних систем від актуальних кіберзагроз;»;

посилити відповідальність за організацію та здійснення кіберзлочинів. Наприклад, доповнивши Примітку до статті 361 Кримінального кодексу України [162] новою частиною такого змісту:

«2. Значною шкодою у статтях 361-363^1 вважається шкода, незалежно від її розміру, яка завдана об'єкту критичної інфраструктури або державній установі.»;

запровадити державну програму із захисту від DDoS-атак. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«Забезпечення державних установ системами для автоматичного виявлення та блокування DDoS-атак»;

встановити обов'язковість використання багатофакторної автентифікації для доступу до державних інформаційних систем. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було

затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«Усі державні установи зобов'язані впровадити багатофакторну автентифікацію для доступу до інформаційних систем, що обробляють персональні або державні дані».

Низький рівень обізнаності громадян, зокрема:

більшість громадян не дотримується основ кібергігієни (використання слабких паролів, ігнорування оновлень);

відсутність освітніх програм з кібербезпеки у школах і університетах;

недостатня кількість тренінгів щодо навичок з готовності до кібератак (організації рідко проводять тренінги або симуляції для перевірки готовності до кіберінцидентів, працівники часто не знають, як діяти у випадку кібератаки).

Так, згідно з результатами опитування, проведеного компанією Info Sapiens у 2023 р., лише 29 % молоді віком від 18 до 25 років вважають себе обізнаними з питань кібербезпеки, тоді як серед осіб старше 60 років цей показник становить лише 7% [163].

У Звіті про проміжне дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки, проведеного за підтримки Офісу Координатора допомоги США Європі та Євразії Державного департаменту Сполучених Штатів Америки зазначається, що знання правил кібергігієни за самооцінкою зросло в усіх аудиторіях, проте найменша частка обізнаних зафіксована серед аудиторії старше 60 років (42 %) [164].

За інформацією Ради національної безпеки і оборони України:

- одними з найвразливіших є підлітки (11 - 17 років) – вони користуються всіма технологіями значно впевненіше за більшість дорослих, але мають менше життєвого досвіду і критичного мислення, через що легше потрапляють на гачки шахраїв;
- дорослі (18 - 59 років) користуються технологічними новинками більш вибірково, але не вважають себе цікавими для кіберзлочинців, а тому продовжують нехтувати правилами безпеки;

- люди похилого віку (60+), адже з початком повномасштабного вторгнення вони все більше користуються онлайн-інструментами для отримання новин і зв’язку з рідними, а значить – також потребують підтримки і пояснення правил кібергігієни [165].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

встановити обов’язковість інформування громадян про методи захисту їхніх даних. Наприклад, доповнивши статтю 6 Закону України «Про захист персональних даних» [166] новою частиною такого змісту:

«11. Суб’єкти, що обробляють персональні дані, зобов’язані надавати користувачам рекомендації з кібергігієни, які сприяють захисту персональної інформації.»;

встановити обов’язок інтернет-провайдерів інформувати клієнтів про базові правила безпеки в інтернеті. Наприклад, доповнивши частину першу статті 6 Закону України «Про інформацію» [167] новим абзацом шостим такого змісту:

«обов’язком Інтернет-провайдерів розміщувати рекомендації щодо безпечного користування інтернетом на своїх веб-сайтах, а також надсилати клієнтам електронні листи з порадами з кібербезпеки;»**;**

встановити обов’язковість інформування клієнтів мобільних операторів про кіберзагрози. Наприклад, доповнивши статтю 31 Закону України «Про електронні комунікації» [168] новою частиною третьою такого змісту:

«3. Мобільні оператори зобов’язані надавати клієнтам SMS-сповіщення про актуальні кіберзагрози та рекомендації щодо їх уникнення.»;

запровадити обов’язкові курси з основ кібергігієни в школах. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«заклади загальної середньої освіти повинні включити в навчальні програми з дисципліни «Основи інформатики» курс з кібергігієни для учнів старших класів, що охоплює правила користування цифровими пристроями, захист даних та розпізнавання кіберзагроз»;

здійснити інтеграцію курсів з кібергігієни в навчальні програми в закладах вищої освіти. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«навчальні програми в закладах вищої освіти повинні включати обов'язкові курси з кібергігієни, який охоплює:

безпечне користування інтернетом;

розпізнавання шахрайства та фішингу;

захист персональних даних»;

створити онлайн-платформу для безкоштовного навчання кібергігієні. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«створити онлайн-платформу для безкоштовного навчання населення кібергігієні, що міститиме:

онлайн-курси для різних вікових груп;

сертифікати про проходження навчання;

доступ до тестових симуляторів кібератак для навчальних цілей»;

створити національну програму просвітництва у сфері кібербезпеки. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року

№ 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«розробити та подати на затвердження Кабінетові Міністрів України національну програму просвітництва у сфері кібербезпеки, яка б передбачала:

регулярні інформаційні кампанії через засоби масової інформації та соціальні мережі про важливість дотримання кібергігієни;

створення серії відповідних освітніх відео програм для громадян та розміщення їх на платформі YouTube;

надання безкоштовного доступу до онлайн-курсів з кібергігієни для всіх бажаючих».

Слабка координація між органами влади, а саме:

недостатні обмін інформацією про кіберзагрози та співпраця у питанні протидії кібератакам між державними органами та приватним сектором;

відсутність централізованої системи обміну інформацією про кіберзагрози та кіберінциденти (на даний час немає єдиної бази даних, де реєструвалися б та аналізувалися б кіберінциденти в державному та приватному секторах, що в свою чергу створює надзвичайно обмежені можливості для аналізу трендів і прогнозування кіберзагроз).

Національний інститут стратегічних досліджень звертає увагу, що відсутність належної координації між державними органами у сфері кібербезпеки є однією з ключових проблем, що потребує вирішення [169].

На посилені координації діяльності та взаємодії між ключовими стейкхолдерами, такими як Держспецзв'язку, Мінцифри, РНБО та Комітет Верховної Ради України з питань цифрової трансформації наголошує і С. Кутор. Крім того, вона висловлює думку, з якою ми, безумовно погоджуємося, що така співпраця – це рушійна сила для розробки необхідного законодавства, покращення щоденної координації, підвищення кваліфікації фахівців та залучення приватного бізнесу задля посилення спроможностей у сфері кібербезпеки України [170].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

створити єдину платформу для обміну інформацією про кіберзагрози між державними органами. Для цього статтю 8 Закону України «Про основні засади забезпечення кібербезпеки України» [2] доповнити новою частиною такого змісту:

«7. Єдина державна платформа для обміну інформацією про кіберзагрози забезпечує:

1) реєстрацію всіх кіберінцидентів державного рівня;

2) оперативне сповіщення про нові загрози;

3) інтеграцію з приватними ініціативами у сфері кібербезпеки.»;

надати функції щодо координування дій всіх державних заходів у випадку масштабних кібератак Національному координаційному центру кібербезпеки. Для цього пункт 3 Положення про Національний координаційний центр кібербезпеки, затвердженого Указом Президента України від 7 червня 2016 року № 242, [175] доповнити новими підпунктами такого змісту:

2) збирання даних про кіберінциденти в режимі реального часу;

3) координація дій державних органів у випадку кібератаки;

4) забезпечення безперебійного обміну інформацією з міжнародними партнерами;»;

Встановити обов’язковість участі критичних об’єктів інфраструктури у спільних навчаннях із кібербезпеки. Для цього статтю 22 Закону України «Про критичну інфраструктуру» [137] доповнити новою частиною такого змісту:

«8. Об’єкти критичної інформаційної інфраструктури зобов’язані щорічно брати участь у навчаннях, організованих Національним координаційним центром кібербезпеки, для перевірки готовності до реагування на кібератаки.».

Відсутність кіберстрахування. Станом на даний час в Україні практично не розвинений механізм кіберстрахування для захисту від фінансових втрат через кібератаки.

Попович Д. В., Бундз Н. Б. та Іванків В. О. зазначають, що в Україні відсутні чіткі стандарти та правила стосовно страхування кіберризиків, що

ускладнює розвиток цього виду страхування [176]. Водночас, науковці стверджують, що розвиток страхування кіберризиків є важливим фактором для забезпечення безпеки та стабільності в інформаційній сфері [176].

Приказюк Н. В. цілком слушно констатує, що відповідно до активного росту успішності кібер-атак виникає необхідність розвитку спеціалізованого виду страхування від кібер-ризиків. На сьогоднішній день у світі даний сегмент страхування є одним з найбільш перспективних та ключових напрямків у стратегіях розвитку економік країн-лідерів страхової сфери, а також організацій, що займаються захистом персональних даних. Оскільки в Україні кібер-страхування поки знаходиться на етапі зародження, з одного боку, страхові компанії не готові гарантувати захист від кібер-ризиків, а з іншого боку, споживачі не розуміють повний перелік переваг, які вони отримають за умови страхування, та методику оцінки втрат від таких ризиків [177].

Приказюк Н. В. вказує, що впровадження кібер-страхування в Україні має підвищити рівень захищеності інформації в умовах масового переходу бізнес-процесів у дистанційний формат [177].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

ввести кіберстрахування як окремий вид страхових послуг. Для цього частину першу статті 4 Закону України «Про страхування» [178] доповнити новим підпунктом такого змісту:

«9^1) клас 9.1 – кіберстрахування, що покриває збитки від кіберзагроз, включаючи витрати на відновлення даних, забезпечення безперервності бізнесу та компенсацію витрат клієнтам;»;

передбачити обов’язкове кіберстрахування для об’єктів критичної інфраструктури. Для цього статтю 22 Закону України «Про критичну інфраструктуру» [137] доповнити новою частиною такого змісту:

«9. Об’єкти критичної інфраструктури зобов’язані укладати договори кіберстрахування з акредитованими страховиками для покриття таких можливих ризиків кібератак:

1) використання шкідливого програмного забезпечення;

2) DDoS-атаки;

3) заподіяння збитків через витік конфіденційної інформації.»

зобов’язати інтернет-магазини укладати кіберстрахові поліси. Для цього статтю 14 Закону України «Про електронну комерцію» [179] доповнити новою частиною такого змісту:

«5. Інтернет-магазини зобов’язані забезпечувати страхування ризиків, пов’язаних із витоком даних клієнтів, шляхом укладання договорів кіберстрахування.»;

гарантувати споживачам компенсацію збитків через кіберстрахування. Для цього статтю 17 Закону України «Про захист прав споживачів» [180] доповнити новою частиною такого змісту:

«6. Кожен споживач має право на компенсацію збитків, спричинених витоком персональних даних або шахрайством, за рахунок кіберстрахового полісу відповідного суб’єкта господарювання.»;

передбачити обов’язковість кіберстрахування для постачальників державних замовлень. Для цього статтю 4 Закону України «Про публічні закупівлі» [151] доповнити новою частиною такого змісту:

«5. Усі постачальники, які беруть участь у державних закупівлях, повинні мати діючий кіберстраховий поліс, що покриває ризики, пов’язані з обробкою державних даних.».

Низька кіберкультура в бізнесі, зокрема:

малий і середній бізнес часто не розглядає кібербезпеку як важливий елемент своєї діяльності;

відсутність політик безпеки та регулярних перевірок у приватних компаніях;

відсутність чітких зобов’язань для приватних компаній у сфері захисту персональних даних своїх клієнтів.

активна диджиталізація агросектору створює нові ризики, але питання кібербезпеки тут майже не розглядаються.

Міжнародний консультант з кібербезпеки М. Чайкін відзначає, що слід окремо оцінювати ситуацію у приватному й державному секторах [181]. За оцінками експертів, рівень кібербезпеки українського бізнесу – це п’ятірка за десятибальною шкалою [181]. За словами експерта, менеджмент великих компаній, холдингів, корпорацій розуміє, чому кібербезпека важлива і вкладає туди кошти. Але малий та середній бізнес ще не усвідомлює всіх ризиків. До спеціалістів зазвичай звертаються вже після хакерських атак. Хоча вигідніше вкласти кошти у попередній захист, аніж потім рахувати збитки [181].

Основну проблему експерти вбачають саме в законодавстві. М. Чайкін зазначає, що українське законодавство з інформаційної безпеки має дуже застарілі вимоги [181]. На думку експерта, це має бути запровадження відповідальності за невиконання вимог законодавства [181].

«Кіберзлочинці постійно пристосовуються до сучасного цифрового ландшафту, ставлячи перед фахівцями з кібербезпеки нові виклики. Приводом може служити як небажання бачити компанію на ринку, так і політичні мотиви. Тому кіберзагрози можуть стосуватися будь якої сфери бізнесу», – зазначають фахівці [182].

За офіційними даними, з січня 2022 р. по жовтень 2023 р. російські хакери атакували українські приватні підприємства та державні установи майже 4000 разів. Український бізнес, який працює нині в умовах війни, мусить адаптуватися і бути готовим до атак росії не лише фізичних, але й цифрових. Так само, як компанії облаштовують підземні сховища для співробітників та за потреби займаються їх релокацією, вони мусять піклуватися про захист своїх цифрових систем [183].

Зазначена проблема посилюється через слабкість законодавчого регулювання щодо збирання та обігу персональних даних. Отже, механізми захисту законних прав та інтересів фізичних осіб, в контексті захисту персональних даних, просто не працюють [184]. Найпростішим прикладом, коли від особи беруть згоду обробку на персональних даних, є реєстрація на сайті. Текст згоди на обробку персональних даних завжди однотипний, не передбачає

внесення змін та має лише одну опцію – погодитися. Не підписання такої згоди призводить до неможливості отримати необхідні послуги. [185]. Велика Палата Верховного Суду в Постанові від 19 вересня 2018 року в справі № 806/3265/17 (Пз/9901/2/18) звертає увагу, що законодавством не врегульовано питання щодо наслідків відмови особи від обробки її персональних даних, тобто фактично відсутня будь-яка альтернатива такого вибору, що в свою чергу обумовлює неякість закону та порушення конституційних прав такої особи [186]. В ЄС у 2016 р. був прийнятий Загальний регламент захисту даних (General Data Protection Regulation, GDPR) [187], яким встановлюються суворі вимоги до опрацювання персональних даних. Вони полягають в тому, що персональні дані мають збиратися законно, правомірно, прозоро та відповідно до цільового обмеження. Окрім того, їх зберігання обмежується строком, необхідним для опрацювання, яке має відбуватися під захистом від несанкціонованого впливу. Найважливіше, що встановлюється значна відповідальність юридичних осіб за порушення вимог Регламенту щодо захисту персональних даних [185]. Експерти зазначають, що текст Закону України «Про захист персональних даних» [166] є достатньо не поганим, однак, чи не найважливішою проблемою залишається той факт, що він не дієвий. Деякі статті закону навіть відображують в собі норми General Data Protection Regulation (GDPR) [187]. Однак, не маючи дієвого державного механізму контролю за виконанням цього закону, він приречений на своє ігнорування. Це, зокрема, можна спостерігати в сфері надання послуг, коли, наприклад, веб-сайт збирає про персональні дані користувачів та використовує ці дані для подальшої розсилки комерційних повідомлень. При цьому, користувач зазвичай не проінформований, куди та як він може подати скаргу на такий веб-сайт та і сам механізм оскарження є доволі незрозумілий [184].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

встановити обов’язковість розробки та впровадження політик кібербезпеки для підприємств. Для цього статтю 8 Закону України «Про основні засади забезпечення кібербезпеки України» [2] доповнити новою частиною такого змісту:

«8. Суб’єкти господарювання зобов’язані розробляти, затверджувати та впроваджувати політики кібербезпеки, що включають заходи з протидії кібератакам, навчання співробітників основам кібергігієни та впровадження сучасних засобів захисту інформації.»;

запровадити грантові програми для підвищення рівня кіберкультури у бізнесі. Для цього частину другу статті 16 Закону України «Про розвиток та державну підтримку малого і середнього підприємництва в Україні» [188] доповнити новим підпунктом такого змісту:

«9) надання грантів для проведення аудитів кібербезпеки, навчання співробітників та впровадження інноваційних технологій захисту даних.»;

зобов’язати бізнес впроваджувати багатофакторну автентифікацію для захисту даних клієнтів. Наприклад, доповнивши статтю 6 Закону України «Про захист персональних даних» [166] новою частиною такого змісту:

«12. Суб’єкти господарювання, що обробляють персональні дані, зобов’язані застосовувати багатофакторну автентифікацію для користувачів і адміністраторів всіх інформаційних систем, які використовуються для обробки та зберігання даних клієнтів.»;

посилити відповідальність підприємств за витоки персональних даних та встановити обов’язкові штрафи. Наприклад, доповнивши статтю 28 Закону України «Про захист персональних даних» [166] новою частиною такого змісту:

«2. У разі витоку персональних даних підприємства зобов’язані:

повідомити постраждалих осіб протягом 72 годин після виявлення витоку;

сплатити штраф у розмірі 5 % від річного доходу компанії або до 5 мільйонів гривень (залежно від того, яка сума більша).»;

зобов’язати компанії звітувати про всі інциденти, пов’язані з витоками даних. Наприклад, доповнивши статтю 28 Закону України «Про захист персональних даних» [166] новою частиною такого змісту:

«3. Компанії зобов’язані повідомляти про інциденти витоку даних до державного органу кібербезпеки протягом 24 годин після їх виявлення.

За невиконання цієї вимоги накладається штраф у розмірі до 1 мільйона гривень.»;

встановити вимогу проведення регулярних аудитів кібербезпеки для платформ електронної комерції, які обробляють персональні дані. Для цього статтю 14 Закону України «Про електронну комерцію» [179] доповнити новою частиною такого змісту:

«6. Власники платформ електронної комерції зобов'язані проводити регулярний аудит кібербезпеки не рідше одного разу на рік, який поміж іншого має включати перевірку відповідності стандартам захисту даних ISO 27001, для забезпечення захисту даних клієнтів і безперебійної роботи платформ.»;

визнати інформаційні системи сільського господарства частиною критичної інфраструктури та додати сільське господарство до переліку галузей, що потребують особливого захисту в сфері кібербезпеки. Для цього статтю 6 Закону України «Про основні засади забезпечення кібербезпеки України» [2] доповнити новою частиною такого змісту:

«6. Об'єкти аграрного сектору, що використовують інформаційні технології для управління виробництвом, зберігання даних та логістики, вважаються критично важливими для національної безпеки та підлягають обов'язковому кіберзахисту.

Інформаційні системи, які використовуються в агротехнологіях, управлінні агропідприємствами та логістиці продукції, підлягають обов'язковій сертифікації та кіберзахисту.

Центральний орган виконавчої влади, що забезпечує формування та реалізує державну аграрну політику, державну політику у сферах сільського господарства та з питань продовольчої безпеки держави здійснює оцінку ризиків кіберзагроз та розробку рекомендацій для впровадження сучасних кіберзахисних технологій у сільськогосподарському секторі.»;

включити витрати на кібербезпеку до переліку витрат, що підлягають державній компенсації. Наприклад, доповнивши статтю 2^1 Закону України «Про

державну підтримку сільського господарства України» [189] новою частиною такого змісту:

«2^1.7. Державна підтримка сільського господарства включає компенсацію витрат на впровадження кіберзахисних технологій, проведення аудитів кібербезпеки та навчання персоналу.».

Відсутність ефективних механізмів кібергігієни, зокрема:

громадяни та організації не дотримуються основних правил кібергігієни, таких як оновлення програмного забезпечення, використання складних паролів, багатофакторної автентифікації;

використання загальних облікових записів у державних і приватних установах;

відсутність чітких правил ідентифікації та автентифікації користувачів;

використання нелегального або несертифікованого програмного забезпечення у багатьох установах;

відсутність централізованих процедур перевірки безпеки стороннього програмного забезпечення;

збільшення використання хмарних технологій супроводжується недостатнім рівнем їх захисту;

неправильна конфігурація хмарних сервісів часто стає причиною витоків даних;

багато установ не мають систематичного підходу до резервного копіювання даних;

відсутність відновлювальних планів у випадку кібератак (наприклад, вірусів-шифрувальників);

використання незахищених мобільних пристроїв у корпоративному середовищі;

відсутність політик управління мобільними пристроями;

пристрої Інтернету речей (Internet of Things, IoT), які активно впроваджуються, часто не мають належного рівня кіберзахисту, що містить в собі

високу ймовірність зламу пристроїв IoT для використання в ботнетах або кібератаках.

А. Нікітенко констатує, що кібергігієна залишається на периферії уваги пересічного громадянина України. Такий легковажний підхід до цього важливого поняття несе як індивідуальну загрозу для кожної окремої людини, так і для держави загалом [190].

Науковець Т. Бабич радить: щоб захистити себе від кіберзагроз, потрібно знати базові правила поведінки в мережі [191].

Спеціалісти ESET зазначають: знешкоджувати загрози важливо. Але ефективніше їх попереджувати. Вони роз'яснюють, що через недотримання елементарних правил безпеки користувачі стають жертвами кіберзлочинців, які отримують доступ до конфіденційних даних, таких як інформація про кредитні картки, рахунки та паролі [192].

Міністерство оборони України підкреслює, що мобільні телефони стали найпростішим джерелом добування розвідувальної інформації, особливо через недотримання правил безпеки та встановлення сумнівних додатків [193].

О. Янковський підсумовує: важливим є формування культури кібербезпеки у суспільстві. З правилами кібергігієни дітей потрібно знайомити ще за шкільною партою, як, наприклад, зараз це відбувається з правилами безпечної поведінки на дорозі [147].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

запровадити обов'язкове навчання кібергігієні для працівників державного сектору. Для цього частину п'яту статті 48 Закону України «Про державну службу» [194] доповнити новими абзацами такого змісту:

«Професійного навчання державного службовця має обов'язково включати навчання основ кібергігієни, щодо:

використання багатофакторної автентифікації;

розпізнавання фішингових атак;

безпечну роботу з конфіденційною інформацією.»;

встановити обов’язковість регулярних тренінгів з кібергігієни для компаній, що обробляють персональні дані. Для цього статтю 12 Закону України «Про захист персональних даних» [166] доповнити новою частиною такого змісту:

«3. Підприємства, що обробляють персональні дані, зобов’язані забезпечити проходження своїми працівниками щорічних тренінгів із кібергігієни.»;

ввести обов’язкові правила кібергігієни для всіх державних установ. Для цього Положення про організаційно-технічну модель кіберзахисту, затверджене постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426, [196] доповнити новим пунктом такого змісту:

«15. Державні установи зобов’язані впровадити внутрішні правила кібергігієни, що включають:

використання надійних паролів;

здійснення регулярного резервного копіювання даних;

контроль доступу до інформаційних систем.»;

зобов’язати провайдерів інтернет-послуг надавати рекомендації щодо кібергігієни своїм клієнтам. Для цього статтю 104 Закону України «Про електронні комунікації» [168] доповнити новою частиною такого змісту:

«10. Провайдери інтернет-послуг зобов’язані надавати користувачам рекомендації з кібергігієни, включаючи:

1) поради щодо налаштування захищених з’єднань;

2) попередження про актуальні кіберзагрози.»;

встановити обов’язкові вимоги щодо кібербезпеки для пристроїв Інтернету речей (IoT), що імпортуються або виробляються в Україні, та запровадити сертифікацію пристроїв Інтернету речей (IoT) на відповідність стандартам кібербезпеки. З цією метою:

статтю 16 Закону України «Про технічні регламенти та оцінку відповідності» [197] доповнити новою частиною такого змісту:

«3. Всі пристрої Інтернету речей (IoT), які виробляються або імпортуються в Україну, повинні відповідати вимогам кібербезпеки, включаючи:

1) наявність можливості змінювати паролі за замовчуванням;

2) підтримку багатофакторної автентифікації;

3) шифрування даних під час передачі.

Сертифікація пристроїв Інтернету речей (IoT) на відповідність міжнародним стандартам кібербезпеки, включаючи ISO/IEC 27001 та ETSI EN 303 645, є обов'язковою умовою для їх реалізації в Україні.

Державні установи можуть використовувати лише сертифіковані пристрої Інтернету речей (IoT), які відповідають стандартам кібербезпеки. Контроль за виконанням цієї вимоги покладається на Держспецзв'язку.»;

статтю 4 Закону України «Про публічні закупівлі» [151] доповнити новою частиною такого змісту:

«6. При здійсненні публічних закупівель пристроїв Інтернету речей (IoT) замовник зобов'язаний враховувати відповідність продукції стандартам кібербезпеки, підтвердженим сертифікатом відповідності.»;

статтю 22 Закону України «Про критичну інфраструктуру» [137] доповнити новою частиною такого змісту:

«10. Об'єкти критичної інфраструктури зобов'язані впроваджувати:

1) системи моніторингу стану пристроїв Інтернету речей (IoT);

2) захист від DDoS-атак через пристрої Інтернету речей (IoT);

3) регулярний аудит безпеки підключених пристроїв Інтернету речей (IoT).»;

статтю 15 Закону України «Про захист прав споживачів» [180] доповнити новою частиною такого змісту:

«10. Виробники зобов'язані надавати споживачам інформацію про:

1) можливі ризики використання пристроїв Інтернету речей (IoT);

2) необхідність регулярного оновлення програмного забезпечення пристроїв Інтернету речей (IoT);

3) рекомендовані налаштування щодо забезпечення кібербезпеки при використанні пристроїв Інтернету речей (IoT).»;

доповнити Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [5] нормою, що зобов'язує власників пристроїв Інтернету речей (IoT) регулярно оновлювати їх прошивку. Наприклад, шляхом внесення до статті 9 зазначеного Закону нової частини такого змісту:

«Користувачі пристроїв Інтернету речей (IoT) зобов'язані забезпечувати регулярне оновлення їх програмного забезпечення відповідно до рекомендацій виробника для усунення вразливостей.»;

встановити обов'язкові вимоги до захисту даних у хмарних сервісах та запровадити обов'язкову сертифікацію хмарних сервісів для використання в державних установах. Для цього:

статтю 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [5] доповнити новими частинами такого змісту:

«Провайдери хмарних послуг зобов'язані:

1) використовувати системи шифрування даних під час їх зберігання та передачі;

2) забезпечувати можливість багатофакторно автентифікації для доступу до даних;

3) проводити регулярний аудит щодо стану кібербезпеки.

Провайдери хмарних сервісів, що працюють з державними установами, повинні кожні два роки проходити сертифікацію на відповідність стандартам кібербезпеки (ISO/IEC 27017, ISO/IEC 27018).»;

статтю 22 Закону України «Про критичну інфраструктуру» [137] доповнити новою частиною такого змісту:

«11. Хмарні сервіси, що обробляють дані критичної інформаційної інфраструктури, підлягають обов'язковій сертифікації та моніторингу.»;

статтю 4 Закону України «Про публічні закупівлі» [151] доповнити новою частиною такого змісту:

«7. При здійсненні публічних закупівель послуг на користування сервісами хмарних послуг замовники зобов’язані враховувати рівень кіберзахисту даних. Провайдери повинні надати сертифікати відповідності міжнародним стандартам кібербезпеки.»;

статтю 24 Закону України «Про захист персональних даних» [166] доповнити новою частиною такого змісту**:**

«5. Провайдери хмарних сервісів зобов’язані повідомляти користувачів про витоки персональних даних не пізніше 48 годин після виявлення інциденту.»;

статтю 31 Закону України «Про електронні комунікації» [168] доповнити новою частиною такого змісту:

«4. Провайдери хмарних сервісів повинні здійснювати щорічний аудит кібербезпеки з поданням звіту до Держспецзв’язку.»;

запровадити гранти на впровадження сучасних хмарних технологій з підвищеним рівнем захисту. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«розробити систему надання державних грантів малим та середнім підприємствам для впровадження хмарних сервісів з сертифікацією кібербезпеки»;

забезпечити інтеграцію хмарних сервісів з національними центрами кіберзахисту. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

Забезпечити взаємодію провайдерів хмарних сервісів з національними центрами кіберзахисту для моніторингу інцидентів та реагування на загрози.»;

встановити обов'язковість резервного копіювання даних для державних установ та критичної інфраструктури. Для цього:

статтю 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [5] доповнити новими частинами такого змісту:

«Усі державні установи та об'єкти критичної інфраструктури зобов'язані забезпечувати регулярне резервне копіювання даних на захищені сервери. Копії повинні зберігатися щонайменше на трьох фізично розподілених носіях.

Підприємства, які обробляють персональні або конфіденційні дані, зобов'язані використовувати сертифіковані системи резервного копіювання з можливістю шифрування даних.»;

статтю 4 Закону України «Про публічні закупівлі» [151] доповнити новою частиною такого змісту:

«8. При здійсненні публічних закупівель програмного забезпечення або послуг хмарних сервісів замовники зобов'язані вимагати наявність функціоналу резервного копіювання даних.»;

запровадити державну програму впровадження систем резервного копіювання. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«розробити та подати на затвердження Кабінетові Міністрів України державну програму впровадження систем резервного копіювання, яка поміж іншого має передбачати:

встановлення централізованих рішень для резервного копіювання у державному секторі;

організацію навчальних семінарів для співробітників державних установ;

фінансування впровадження резервного копіювання для малих державних установ.»;

вирішити проблему з контролем доступу до інформаційних систем і даних в Україні, шляхом встановлення в тендерних умовах закупівель вимоги щодо наявності системи контролю доступу в ІТ-продуктах. Для цього статтю 4 Закону України «Про публічні закупівлі» [151] доповнити новою частиною такого змісту:

«9. При здійсненні публічних закупівель програмного забезпечення замовники зобов’язані вимагати наявність функціоналу для управління правами доступу та ведення аудиту.»;

запровадити обов’язкову перевірку програмного забезпечення, що використовується в державних органах. З цією метою:

доповнити статтю 8 Закону України «Про основні засади забезпечення кібербезпеки України» [2] новою частиною такого змісту:

«9. Програмне забезпечення, що використовується державними органами, підлягає обов’язковій періодичній перевірці на відповідність вимогам кібербезпеки, включаючи аналіз коду на наявність вразливостей та шкідливого функціоналу.»;

до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«створення системи моніторингу безпеки програмного забезпечення, що забезпечуватиме регулярне сканування програмного забезпечення, яке використовується в державному секторі, для виявлення потенційних вразливостей, прихованих загроз або шкідливого коду»;

встановити обов’язковість використання лише перевіреного програмного забезпечення операторами електронних комунікацій. Наприклад, доповнивши

статтю 31 Закону України «Про електронні комунікації» [168] новою частиною такого змісту:

«5. Оператори електронних комунікаційних мереж повинні використовувати лише програмне забезпечення, яке пройшло сертифікацію на відповідність вимогам кібербезпеки.»;

вирішити проблему мобільної безпеки**,** шляхом встановлення обов'язкових вимог до мобільних додатків, які обробляють персональні дані. Наприклад, доповнивши статтю 6 Закону України «Про захист персональних даних» [166] новою частиною такого змісту:

«13. Мобільні додатки, що обробляють персональні дані користувачів, зобов'язані:

1) забезпечувати шифрування даних;

2) застосовувати механізми багатофакторної автентифікації;

3) регулярно проходити аудит кібербезпеки.

Державні установи можуть використовувати лише мобільні додатки, які пройшли перевірку на відповідність стандартам кібербезпеки, затвердженим Держспецзв'язку.»;

встановити вимогу до мобільних операторів впроваджувати засоби захисту мобільного зв'язку. Наприклад, доповнивши статтю 31 Закону України «Про електронні комунікації» [168] новою частиною такого змісту:

«6. Мобільні оператори повинні впроваджувати засоби захисту від перехоплення сигналу, несанкціонованого доступу до мережі та атак типу man-in-the-middle.»;

запровадити національну програму з мобільної безпеки. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«Розробити та подати Кабінетові Міністрів України на затвердження національну програму з підвищення мобільної безпеки, яка поміж іншого має включати:

1) проведення освітніх кампаній щодо мобільної безпеки;

2) запровадження стандартів з кібербезпеки для розробників мобільних додатків;

3) надання рекомендацій громадянам щодо захисту мобільних пристроїв;

4) створення систему моніторингу загроз мобільній безпеці, що забезпечить:

виявлення потенційних загроз мобільній безпеці;

сповіщення користувачів про актуальні ризики;

надання рекомендацій користувачам щодо уникнення загроз».

Проблеми з ідентифікацією джерел атак, зокрема:

складність ідентифікації реальних джерел атак, особливо в умовах використання VPN і проксі;

відсутність необхідного технічного обладнання для аналізу інцидентів.

Наприклад, 19 грудня, 2024 р. відбулася наймасштабніша зовнішня кібератака на державні реєстри України. Тимчасово було призупинено роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції [198]. «Точно зрозуміло, що атака здійснювалася росіянами з метою порушити роботу критично важливої інфраструктури держави», – зазначила Віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України – Міністр юстиції Ольга Стефанішина [199]. Голова підкомітету з питань безпеки в кіберпросторі, урядового зв’язку, криптографічного захисту інформації Комітету Верховної Ради України з питань нацбезпеки, оборони та розвідки Олександр Федієнко, повідомив, що атака була добре підготовленою, а вхід стався з акаунту найвищого рівня. Для атаки ворог міг також вдатися до вербування працівника установи. Також міг бути застосований багаторівневий механізм підкладання флешки, щоб вона прийшла в людини внутрішній периметр та була включена. «Тут може бути фішинг комп’ютерів усіх

працівників, які, можливо, працюють із закритим контуром, дистанційно, що в принципі заборонено.» [198].

В Огляді подій в сфері кібербезпеки, представленому Національним координаційним центром кібербезпеки Ради безпеки і оборони України в лютому 2024 р., зазначається, що вразливості у продуктах Ivanti вже другий місяць створюють проблеми користувачам та кібербезпековим органам по всьому світу. Виходять все нові дані про вразливості у продуктах Ivanti, а ENISA (Європейське агентство з мережевої та інформаційної безпеки) та CERT-EU (Урядова команда реагування на комп'ютерні надзвичайні події України) навіть випустили спільні рекомендації для європейських споживачів. Загрози кібербезпеці ОТ (Operational Technology) не лише не зменшуються, але стають все більш системними. Виробники обладнання та ОТ-рішень все частіше знаходять нові вразливості у своїх продуктах – лише у лютому Siemens виявив 275 вразливостей у своїх виробах які активно використовуються у сфері автоматизації виробничих процесів. Звіт відомої компанії Dragos Inc, що займається безпековими рішеннями для промислової інфраструктури, підтверджує, що зловмисники все інтенсивніше входять в цю, відносно нову, сферу – у 2023 році додалось ще три кіберугрупування, які націлені саме на ОТ інфраструктуру (таким чином Dragos наразі відстежує 21 таке угрупування). Проблеми є не лише з виявленням вразливостей, але і зі спробами їх виправити. Дослідження показали, що організації з системами ОТ часто знають про недоліки, які використовуються в їхньому середовищі, але вони не можуть вирішити проблему [200].

Згідно зі звітом Insikt Group (дослідницький підрозділ всесвітньовідомої компанії Recorded Future, який спеціалізується на дослідженні загроз у сфері кібербезпеки), опублікованому 11 січня 2024 р., широке поширення GitHub в IT середовищах дозволяє суб'єктам загрози легко розміщувати та доставляти зловмисне корисне навантаження, а також використовувати його як розв'язувачів, командно контрольних точок і точок викрадення даних. За словами дослідників, використання служб GitHub, як зловмисної інфраструктури, дозволяє зловмисникам змішуватись із законним мережевим трафіком, часто

обходячи традиційні засоби захисту та ускладнюючи відстеження інфраструктури та атрибуцію акторів [201].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

запровадити обов'язкове використання національної системи моніторингу кіберзагроз для всіх об'єктів критичної інфраструктури та забезпечити обмін інформацією про джерела атак між державними структурами та приватними компаніями. З цією метою доповнити статтю 8 Закону України «Про основні засади забезпечення кібербезпеки України» [2] новою частиною такого змісту:

«10. Суб'єкти критичної інфраструктури зобов'язані підключитися до національної системи моніторингу кіберзагроз для автоматичного виявлення джерел атак та аналізу підозрілої активності.

Державні установи та приватні компанії, що працюють із критичною інформаційною інфраструктурою, зобов'язані передавати дані про кіберінциденти та джерела атак до національної системи моніторингу кібербезпеки.»;

запровадити контроль за використанням анонімних мереж (VPN, анонімайзерів та проксі-серверів тощо) для запобігання використанню їх кіберзлочинцями. Для цього статтю 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [5] доповнити новими частинами такого змісту:

«Провайдери інтернет-послуг зобов'язані моніторити використання VPN, анонімних проксі-серверів та виявляти підозрілу активність, що може свідчити про підготовку або здійснення кібератаки.»;

зобов'язати державні установи використовувати програмне забезпечення з функціями автоматичного аналізу джерел атак. Для цього статтю 4 Закону України «Про публічні закупівлі» [151] доповнити новою частиною такого змісту:

«10. Закупівля програмних рішень для державних установ та критичної інфраструктури повинна передбачати наявність у таких рішеннях засобів аналізу джерел атак, виявлення загроз та реагування на інциденти.»;

встановити обов’язковість впровадження технологій штучного інтелекту для аналізу кіберзагроз. Для цього статтю 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [5] доповнити новою частиною такого змісту:

«У системах кібербезпеки державних органів та суб’єктів критичної інфраструктури впроваджуються алгоритми штучного інтелекту для аналізу мережевого трафіку, виявлення аномалій та визначення ймовірних джерел атак.»;

розширити повноваження правоохоронних органів щодо використання кіберрозвідки для виявлення джерел атак. Для цього частину першу статті 8 Закону України «Про оперативно-розшукову діяльність» [202] доповнити новим підпунктом такого змісту:

«22) використовувати спеціалізоване програмне забезпечення для відстеження та аналізу трафіку з метою ідентифікації джерел кібератак.»;

посилити кримінальну відповідальність за використання ботнетів, анонімних мереж та проксі-серверів для здійснення атак. Наприклад, доповнивши частину другу статті 361 Кримінального кодексу України [162] новим абзацом такого змісту:

«Ті самі дії, вчинені через анонімні мережі або VPN, караються позбавленням волі строком від 5 до 10 років із конфіскацією обладнання та забороною займати певні посади строком до 5 років.»;

розробити та впровадити державну платформу з аналізу атак для ідентифікації їх джерел. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«створити державну платформу з аналізу атак для ідентифікації їх джерел, яка забезпечуватиме:

автоматизований аналіз атак у реальному часі;

ідентифікацію IP-адрес, хостів, геолокації атакуючих систем;

обмін інформацією з міжнародними партнерами щодо кіберзагроз».

Відсутність стандартів кібербезпеки для блокчейн-технологій, а саме:

використання блокчейн-технологій у фінансових та інших секторах відбувається без чітких стандартів кіберзахисту;

відсутні державні стандарти безпеки для блокчейн-систем;

не забезпечено регулювання зберігання та використання криптографічних ключів;

не здійснюється ліцензування та аудит блокчейн-платформ;

не запроваджено механізми моніторингу транзакцій для запобігання шахрайству.

Вирішення зазначених питань на сьогодні для України, на нашу думку, є надзвичайно актуальним та дозволить зменшити ризики кібератак, підвищити довіру до технології блокчейн та сприяти розвитку безпечного цифрового ринку в Україні.

Відсутність єдиних стандартів взаємодії блокчейн-мереж і недостатнє регулювання в галузі криптовалют і цифрових активів у багатьох країнах створюють правові та економічні ризики для учасників цієї екосистеми [203].

Г. Терещенко та І. Кириченко в своєму дослідженні показують, що упровадження стандартів і регулювань є критичним для успішної інтеграції та розвитку блокчейнтехнологій [204].

С. О. Бойчук резюмує, що імплементація блокчейн-технології в фінансовій сфері є непростим завданням, яке має ряд викликів. Основні труднощі, що можуть виникнути, включають: культурну трансформацію, недостатньо обґрунтоване зростання ефективності, невисокий рівень реалізації, технічні обмеження, відсутність стандартизації, а також питання безпеки та конфіденційності [205].

Г. М. Мутерко разом з іншими дослідниками стверджують, що основними проблемами впровадження технології блокчейн на фінансовому ринку є недостатня окупність інвестицій у технології, відсутність чіткого нагляду та

стандартизації. Швидкість розвитку технології та їх впровадження в соціально-економічні процеси є настільки великою, що може становити певну загрозу для країни, якщо не буде відповідної реакції через певне регулювання, встановлення стандартів та загальних правил використання [206].

З метою створення умов для вирішення зазначеної проблеми пропонуємо:

встановити обов'язкові вимоги до безпеки блокчейн-платформ, які використовуються для фінансових транзакцій та зберігання даних. Для цього статтю 9 Закону України «Про віртуальні активи» [207] доповнити новою частиною такого змісту:

«8. Блокчейн-платформи, що використовуються для фінансових операцій, повинні відповідати стандартам безпеки, визначеним Національним банком України та Держспецзв'язку, зокрема, забезпечувати криптографічний захист даних, безпечне зберігання приватних ключів та захист від несанкціонованого доступу.»;

встановити обов'язкові вимоги до смарт-контрактів та забезпечення їх безпечного використання. Для цього статтю 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» [174] доповнити новою частиною такого змісту:

«5. Смарт-контракти, що використовуються для фінансових операцій або державних реєстрів, повинні мати сертифіковане аудиторське підтвердження від спеціалізованих кібербезпекових компаній, що підтверджує їх відповідність стандартам безпеки.»;

з метою забезпечення безпеки зберігання приватних ключів та криптографічних алгоритмів у блокчейн-технологіях встановити відповідні обов'язкові вимоги до суб'єктів, які використовують блокчейн для зберігання конфіденційних даних. Для цього статтю 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [5] доповнити новою частиною такого змісту:

«Усі суб'єкти, які використовують блокчейн для зберігання конфіденційних даних, зобов'язані:

1) використовувати сертифіковані апаратні засоби для зберігання приватних ключів;

2) забезпечувати резервне копіювання ключів у зашифрованому вигляді;

3) дотримуватися міжнародних стандартів кібербезпеки при роботі з блокчейн-системами.»;

посилити контроль за транзакціями в блокчейн-системах для запобігання фінансуванню тероризму та відмиванню коштів. Для цього статтю 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [208] доповнити новою частиною такого змісту:

«16. Банки та фінансові установи, які проводять операції з використанням блокчейн-технологій, зобов'язані:

1) використовувати автоматизовані системи аналізу транзакцій для виявлення підозрілих операцій;

2) запровадити механізми ідентифікації учасників транзакцій;

3) здійснювати аудит безпеки своїх блокчейн-платформ не рідше одного разу на рік.»;

зобов'язати державні органи використовувати блокчейн для ведення державних реєстрів із підвищеним рівнем безпеки. Наприклад, доповнивши статтю 6 Закону України «Про захист персональних даних» [166] новою частиною такого змісту:

«14. Усі державні реєстри, які зберігають персональні дані або критичну інформацію, повинні використовувати блокчейн-системи, що відповідають стандартам безпеки ISO 27001 та NIST SP 800-57.»;

створити державний центр, який відповідатиме за розробку та впровадження стандартів безпеки для блокчейн-технологій. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії

кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«Створити Державний блокчейн-центр , який поміж іншого має бути відповідальний за:

1) розробку національних стандартів кібербезпеки для блокчейн-технологій;

2) перевірку та ліцензування платформ, що використовують блокчейн у державних та фінансових системах;

3) моніторинг нових кіберзагроз у сфері блокчейну».

Недостатній рівень міжнародної співпраці, а саме:

обмежена співпраця з міжнародними організаціями у сфері кібербезпеки;

відсутність інтеграції в глобальні платформи обміну інформацією про загрози (наприклад, платформи під егідою НАТО та/або ЄС);

слабка взаємодія з міжнародними організаціями щодо проведення спільних розслідувань кіберзлочинів та обміну інформацією;

відсутність фінансування міжнародних кіберпроєктів;

недостатній рівень інтеграції України в міжнародні системи моніторингу кіберзагроз**.**

М. С. Тєтєвін зазначає, що у сучасному цифровому світі кібербезпека стала однією з найбільш актуальних проблем, оскільки зростання кількості підключених пристроїв призвело до збільшення кіберзагроз, які становлять серйозний ризик для національної та міжнародної безпеки. У цьому контексті співпраця між країнами стає надзвичайно важливою для захисту суверенітету та забезпечення кібербезпеки на глобальному рівні. Ключове значення має також міжнародне співробітництво з організаціями, які визнають безпеку однією з основних цілей, такими як НАТО та Європейський Союз

Міжнародна співпраця в галузі кібербезпеки є надзвичайно важливою, оскільки інтернет не має фізичних кордонів, і кіберзагрози можуть легко перетнути державні межі [209].

М. С. Тєтєвін висловлює думку, з якою ми погоджуємось, що сьогодні, коли в нашій державі Україні 10 років йде війна, і не лише конвенційними засобами та методами, а й у тому числі на інформаційному фронті, участь у міжнародному процесі має вкрай важливе значення [209].

В. В. Зуй робить висновок, що обрання нашою державою стратегічного курсу на набуття повноправного членства України в Європейському Союзі вимагає ефективної реалізації державної політики у сферах європейської інтеграції щодо кібербезпеки (оборони) вочевидь [144].

Т. Г. Мужанова разом з іншими в своїй праці показує, що досвід розробки і впровадження політики кібербезпеки ЄС може бути еталоном кращих практик для інших держав, в тому числі України, стати рушійною силою для впровадження нових ініціатив для вирішення проблем кібербезпеки [210].

К. Корсун констатує, що на сьогоднішній момент рівень співпраці у сфері кібер безпеки між Україною та НАТО не є на належному рівні [211]. На його думку, важливим аспектом є посилення співпраці зі структурами НАТО та окремими країнами щодо обміну інформаціє [211].

Цілком слушно К. Корсун вносить пропозицію, що співробітництво у сфері кібербезпеки може розвиватися одночасно на декількох рівнях:

багатонаціональний рівень у рамках приєднання до центрів передового досвіду;

двосторонньому рівні з такими країнами як передусім Естонія, Румунія, Велика Британія, Чехія, які приділяють особливу увагу кібер захисту;

національному рівню – створення відповідних спроможностей всередині країни за рахунок технічної та експертної підтримки структур НАТО [211].

Кабінет Міністрів України також визнав слабкість державно-приватного партнерства у сфері захисту критичної інфраструктури та недостатній рівень міжнародного співробітництва з цих питань.

За інформацією Національного інституту стратегічних досліджень, як експерти-освітяни, так і професійна ІТ-спільнота констатують наявність системних проблем у сфері кібернетичної безпеки. Однією з яких вважають

відірваність фахівців з інформаційної та кібербезпеки від міжнародної системи стандартизації [213].

З метою створення умов щодо сприяння інтеграції з НАТО та ЄС у сфері кібербезпеки та вирішення зазначеної проблеми пропонуємо:

розробити новий закон (Закон України «Про міжнародну співпрацю у сфері кібербезпеки»), що регламентуватиме взаємодію України з міжнародними партнерами у сфері кібербезпеки. Основні положення цього закону мають унормовувати:

- впровадження єдиної системи обміну інформацією про кіберзагрози з партнерами НАТО та ЄС;
- механізми екстрадиції кіберзлочинців, що здійснюють атаки на українські об'єкти;
- впровадження міжнародних стандартів у розслідування кіберзлочинів.

розширити міжнародну співпрацю шляхом створення спеціалізованих органів координації кібербезпеки. З цією метою Закон України «Про основні засади забезпечення кібербезпеки України» [2] доповнити новою статтею 9^1 такого змісту**:**

«Стаття 9^1. Національний центр міжнародної координації з кібербезпеки

1. Завданнями Національного центру міжнародної координації з кібербезпеки є:

1) обмін інформацією про кіберзагрози та атаки з НАТО, ЄС та іншими міжнародними організаціями;

2) співпраця з Interpol та Europol щодо розслідування міжнародних кіберзлочинів;

3) спільно з міжнародними експертами розробка рекомендацій та стандартів кіберзахисту.

2. Національний центр міжнародної координації з кібербезпеки забезпечує:

1) взаємодію України з міжнародними організаціями, зокрема NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) та European Union Agency for Cybersecurity (ENISA);

2) участь у міжнародних кібернавчаннях та обмін досвідом з провідними країнами у сфері кіберзахисту;

3) підготовку фахівців у галузі кібербезпеки через міжнародні програми навчання.»;

встановити принципи міжнародної кібероборони та участі України в міжнародних кібероперація. З цією метою статтю 31 Закону України «Про національну безпеку України» [3] доповнити новою частиною такого змісту:

«4. Україна бере участь у міжнародних кібероперація, спрямованих на протидію ворожим кіберзагрозам, у співпраці з країнами-партнерами НАТО та ЄС. Для цього створюється Національний центр кібероборони, який здійснює стратегічне планування, аналіз загроз та кібероперації оборонного характеру.»;

у Законі України про Державний бюджет України запровадити окрему статтю видатків для фінансування проєктів міжнародного співробітництва у сфері кібербезпеки, зокрема, участі у програмі NATO Cyber Defence Pledge, розвитку кіберінфраструктури в рамках співпраці з ЄС та залучення експертів з міжнародних організацій;

забезпечити підключення до міжнародних систем кібермоніторингу для виявлення загроз. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«Забезпечити інтеграцію державних органів України в міжнародні системи кібермоніторингу, зокрема:

Forum of Incident Response and Security Teams (FIRST) – для обміну даними про кіберінциденти;

Shadowserver Foundation – для моніторингу кіберзагроз у реальному часі;

MITRE ATT&CK – для аналізу тактик і методів кіберзлочинців»;

запровадити механізм взаємодії з провідними IT-компаніями світу (Google, Microsoft, Cisco) для отримання актуальних оновлень щодо кіберзагроз. З цією метою пропонуємо до плану заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447 [4], на наступний період (План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України було затверджено розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163 [158]) включити таке завдання:

«Мінцифри забезпечити стратегічну співпрацю Уряду України з міжнародними технологічними компаніями, щодо:

отримання інформації про вразливості та загрози в реальному часі;

використання передових рішень штучного інтелекту для захисту державних інформаційних систем;

спільну розробку нових методів захисту кіберпростору.

Висновки до розділу 3

Розглянуто поняття «злочинність у сфері комп'ютерної інформації», посилаючись як на наукові, так і на законодавчі визначення. Зосереджено увагу на відмінності термінів «кіберзлочинність» і «злочинність у сфері комп'ютерної інформації». «Кіберзлочинність» охоплює злочини, пов'язані як з використанням комп'ютерних технологій, так і з глобальними мережами. Тоді, як «злочинність у сфері комп'ютерної інформації» більш конкретно стосується злочинів проти комп'ютерних систем або даних. Загалом можна констатувати, що сьогодні кіберзлочинність включає широкий спектр протиправних дій, від несанкціонованого доступу до державних комп'ютерних мереж і крадіжки особистих даних до фінансового шпигунства та відмивання грошей.

Проведено наукове дослідження сучасного стану кіберзлочинності та її впливу на безпеку держави. Визначено ключові загрози, що виникають у

цифровому просторі, запропоновано адміністративно-правові методи запобігання та протидії цим загрозам у контексті забезпечення безпеки держави.

Визначено, що комп'ютерна злочинність постійно розвивається у зв'язку з удосконаленням і появою нових IT-технологій, збільшенням кількості користувачів Інтернету та мобільних пристроїв, а також переходом на електронний документообіг в організаціях. Комп'ютерні злочини можна розділити на незаконне використання програмного забезпечення, шахрайство та атаки, які використовують вразливі місця системи.

У сфері забезпечення кібербезпеки важливою є державно-приватне партнерство, але держава відіграє провідну роль. Існує три основні рівні кіберзагроз, кожен із яких має свої специфічні типи загроз. Особливу загрозу національній безпеці держав становлять такі дії у кіберпросторі, як інформаційна війна та кібершпигунство.

Вирішальним для забезпечення кібербезпеки пропонується використання технології WorkFlow та розвиток державних систем кібербезпеки. Зокрема, запропоновано модель двофакторної автентифікації державних службовців. Використання стандартизованих мов програмування та форматів, таких як XML, EDIFACT, RDFS, OWL, є важливим для забезпечення сумісності та безпеки даних.

Дослідження питань інформаційного протистояння, у тому числі визначення можливостей планування дій щодо впливу чи протидії інформаційним впливам, потребує детального аналізу основних напрямів кіберзахисту. Крім суто цивільного кіберзахисту, сучасна держава повинна мати можливість активно протидіяти кіберзагрозам, розвиваючи активні протидії. Ці події мають неабияку актуальність і значення для сучасної України. Важливим чинником глобального інформаційного простору стає міжнародний інформаційний тероризм, особливо з огляду на використання високотехнологічних методів. Визначено ключові напрямки, які слід враховувати при розробці стратегій кібербезпеки, серед яких:

стратегія кіберінформаційної протидії системам управління;

електронне протистояння;

психологічне кіберпротистояння;

хакерська війна (використання комп'ютерних технологій для незаконного доступу або порушення роботи ворожих систем);

кібернетичні та мережеві війни;

економічна кіберінформаційна війна.

Зроблено висновок щодо необхідності посилення державної кібербезпеки на всіх рівнях, від окремого користувача до національних державних органів. В дисертаційній роботі запропоновані конкретні рекомендації щодо захисту від кіберзагроз.

Останнім часом спостерігається суттєва зміна комплексу факторів, що визначають комп'ютерну злочинність на державному рівні. Крім традиційних соціальних, економічних, правових, кадрових, організаційних і технічних аспектів все більшого значення набувають політичні фактори. До них належать геополітичні аспекти, зокрема військово-політичні, глобальні економічні та міжнародні політичні елементи, а також політичні та спостережні фактори, пов'язані з недостатнім соціальним і державним контролем над кіберпростором. Інші важливі чинники включають політико-кримінальний (включаючи кібертероризм, кіберекстремізм і хактивізм), політико-інформаційний (кібершпигунство) та політико-інституційний (зловживання ІТ-технологіями). Ключовим моментом еволюції кіберзлочинності, що перетворює її на технотронний злочин, є її самовизначення. Цей процес означає здатність комп'ютерної злочинності до автономного регенерування, тобто до самостійного відтворення злочинів у соціальному середовищі. Ці прояви визначають перспективи подальших досліджень сучасних кіберзагроз та заходів щодо їх запобігання.

Зроблено висновок, що концепція кібербезпеки передбачає збереження конфіденційності інформації та протидію цифровим атакам, а також будь-якому зовнішньому впливу, спрямованому на їх викрадення чи фальсифікацію.

Останнім часом найсерйозніші атаки спрямовані на фінансовий сектор України, зокрема великі банки, які істотно впливають на фінансову систему країни.

Розглянуто вплив кібербезпеки на функціонування фінансових установ. Внесено пропозиції щодо напрямків удосконалення адміністративно-правових засад його забезпечення. Як правило, кібербезпеки можна досягти за допомогою таких засобів:

спеціалізоване програмне забезпечення;

низка технічних апаратних рішень, пов’язаних із цифровою інфраструктурою, підтримкою серверів і центрів обробки даних;

впровадження нормативної бази для обробки персональних даних клієнтів у фінансових установах та політики щодо їх використання.

Очевидно, що на сьогодні залишається важливим та актуальним питання впливу кібербезпеки на стабільність діяльності фінансових установ та вдосконалення її адміністративно-правового забезпечення.

В роботі виконано дослідження, спрямоване на аналіз сучасних тенденцій у кібербезпеці, її впливу на стабільність фінансових установ та вдосконалення відповідного адміністративно-правового забезпечення. Детально проаналізовано питання підтримки життєво важливих функцій кібербезпеки в контексті зростання цифрових загроз. Узагальнено практичний досвід великих фінансових установ у формуванні власної стратегії кібербезпеки та визначено особливості адміністративно-правових засад для підтримки цих інструментів. Визначено сучасні тенденції у цифрових технологічних рішеннях фінансових установ, спрямованих на забезпечення власної безпеки в цифровому просторі та її подальшу підтримку шляхом впровадження ефективних цифрових та інноваційних рішень. Проаналізовано теоретичні, методологічні та практичні підходи до кіберзахисту та цифрових інструментів, які допомагають підтримувати стабільність фінансових установ, та запропоновано шляхи вдосконалення адміністративно-правових засад щодо їх ефективного функціонування.

Зі стрімким цифровим розвитком сучасні методи шифрування даних і криптографії стали найпоширенішими серед фінансових установ. Вони спрямовані на надання якісних послуг і створення безпечного середовища для зберігання та роботи з даними. Криптографія стала найпопулярнішим засобом захисту даних, який вимагає ефективного шифрування.

Крім того, впровадження хмарних технологій є засобом захисту даних від фізичних носіїв. Така децентралізована система найбільш популярна в США, Китаї, Німеччині, Швейцарії та багатьох інших країнах, які вважаються світовими фінансовими центрами.

Розглянуто питання уникнення кібератак і посилення їх засобів для забезпечення найбільш ефективної безпеки для каналів зв'язку клієнтів, таких як веб-сайти, мобільні додатки, онлайн-платформи та термінали. Впровадження цифрових систем розпізнавання обличь, відстеження транзакцій та перевірка їх законності є ефективним методом запобігання негативним наслідкам цифрових загроз.

Війна в Україні призвела до потужної атаки на багато українських банків та інших фінансових установ, що працюють в Україні. Проте, незважаючи на такі дії країни-агресора, фінансові інституції реалізують різні ефективні стратегії, серед яких:

географічна диверсифікація розташування центрів обробки даних;

використання резервних систем;

ефективне власне програмне забезпечення;

інтеграція хмарної системи.

Ці методи можуть допомогти забезпечити кібербезпеку фінансових установ у контексті цифрової війни, що може бути корисним для всього світу.

Показано, що вплив кібербезпеки на стабільність функціонування фінансової установи є суттєвим, практично, вирішальним фактором, що забезпечує планування діяльності фінансової установи, мінімізацію та запобігання ризикам, безперервність функціонування всієї структури і вимагає високоякісних технологічних рішень.

В дисертаційному досліджені детально проаналізовано та узагальнено інформацію стосовно впливу кібербезпеки на стабільність функціонування фінансової установи. Розроблено комплекс заходів щодо запобігання відповідним ризикам та підвищення рівня кібербезпеки фінансових установ.

Сформульовано заходи, які є ключовими у впливі на кібербезпеку банків та спрямовані на диверсифікацію ризиків та їх уникнення, використання хмарних сервісів і технологій автентифікації, а також посилення фінансового моніторингу.

Поведений в дисертаційному дослідженні аналіз наукової літератури, аналітичних публікацій широкого кола експертів і чинної нормативно-правової бази надали можливість сформулювати наступні основні проблеми та актуальні виклики сьогодення в сфері забезпечення кібербезпеки та кіберзахисту, протидії кіберзагрозам, таким як кібератаки та кіберзлочинність, в умовах воєнного стану та повоєнної відбудови України:

недостатній рівень кіберзахисту критичної інфраструктури;

недостатнє фінансування кібербезпеки;

дефіцит кваліфікованих спеціалістів;

високий рівень кіберзагроз;

низький рівень обізнаності громадян;

слабка координація між органами влади;

відсутність кіберстрахування;

низька кіберкультура в бізнесі;

відсутність стандартів кібербезпеки для блокчейн-технологій;

недостатній рівень міжнародної співпраці.

Запропоновано шляхи вирішення зазначених проблем у сфері кібербезпеки України, створення сучасної ефективної системи забезпечення кібербезпеки та кіберзахисту, що на даний час є вкрай актуальним питанням для нашої держави, шляхом вдосконалення нормативно-правового регулювання адміністративно-правових засад забезпечення кібербезпеки. Зокрема, розроблено законопроєкт, яким запропоновано системне та комплексне вдосконалення забезпечення

кібербезпеки України. Законопроєктом пропонується внести зміни до статті 361 Кримінального кодексу України, статей 15 і 17 Закону України «Про захист прав споживачів», статті 8 Закону України «Про оперативно-розшукову діяльність», статті 6 Закону України «Про інформацію», статті 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах», статті 2^1 Закону України «Про державну підтримку сільського господарства України», статей 6, 12, 24 і 28 Закону України «Про захист персональних даних», статей 4 і 18 Закону України «Про державно-приватне партнерство», статті 16 Закону України «Про розвиток та державну підтримку малого і середнього підприємництва в Україні», статті 15 Закону України «Про зайнятість населення», статті 16 Закону України «Про технічні регламенти та оцінку відповідності», статті 14 Закону України «Про електронну комерцію», статті 48 Закону України «Про державну службу», статті 4 Закону України «Про публічні закупівлі», статті 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», статей 6, 8, 9, 11 і 13 Закону України «Про основні засади забезпечення кібербезпеки України», статті 31 Закону України «Про національну безпеку України», статті 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», статей 31 і 104 Закону України «Про електронні комунікації», статей 21 і 22 Закону України «Про критичну інфраструктуру», статті 4 Закону України «Про страхування», статті 9 Закону України «Про віртуальні активи». З метою імплементації зазначених законодавчих змін також розроблено пропозиції до постанов і розпоряджень Кабінету Міністрів України.

ВИСНОВКИ

У проведеному дисертаційному дослідженні здійснено теоретичне узагальнення й запропоновано нове вирішення наукового завдання, яке полягало в комплексному аналізі теоретико-правових підходів і формулюванні адміністративно-правових засад забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України.

В результаті сформульовано такі висновки науково-теоретичного та практичного характеру:

1. Показано, що термін «кібербезпека» набуває все більшого поширення в останні часи, водночас, використання цього терміну та визначення його контексту в різних наукових працях і нормативно-правових документах значно різняться між собою.

Проаналізовано нормативно-правові джерела та наукову літературу, узагальнено науковий матеріал щодо визначень терміну «кібербезпека». Встановлено такі його ключові аспекти:

використання комп’ютерних систем і телекомунікаційних мереж;

нейтралізація негативних інформаційних впливів на технологічному рівні;

захист основоположних прав і життєво важливих інтересів людини і громадянина, суспільства і держави в кібернетичному середовищі, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем;

нейтралізація загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах;

спрямованість на досягнення і утримання потенційними протиборчими сторонами переваги в протидії новим загрозам безпеці для власних об’єктів критично важливої інформаційної і кіберінфраструктури.

2. Досліджено організаційно-адміністративні засади системи забезпечення кібербезпеки та кіберзахисту.

Показано, що кібербезпека являє собою правовий інститут, тобто цілу систему юридичних норм, у вигляді правового об'єкта якого розглядають регулювання безпечного стану обробки інформації у кіберпросторі. Тоді, як під кіберзахистом слід розуміти систему (механізм) засобів різного характеру (правового, організаційного, ресурсно-фінансового, програмно-технічного та іншого характеру), за допомогою яких здійснюється діяльність у кіберпросторі з охорони певних його об'єктів від протиправних посягань (наприклад, кіберзлочинів) і створення перешкод у реалізації загроз кримінального характеру.

Виходячи із зазначеного визначено основні суб'єкти та об'єкти кібербезпеки та кіберзахисту.

3. Встановлено, що подальшого вдосконалення потребують визначення термінів «кібербезпека», «кіберзлочинність», «приватність у віртуальному просторі» та правового регулювання віртуального світу.

Показано, що нові технологічні реалії, міжнародні відносини та геополітична ситуація стали серйозними викликами для системи правових відносин у сучасному світі. Міжнародні правові норми та національне законодавство відіграють наздоганяючу роль у системах кібербезпеки та конфіденційності віртуального простору. Це ще більше посилює загрозу кіберзлочинності. Нормативно-правова база віртуальної сфери, як в Україні, так і в усьому світі, має встигати за розвитком технологій.

Проте самого правового регулювання недостатньо для вирішення цих проблем. Іншими важливими факторами забезпечення кібербезпеки та конфіденційності у віртуальному світі є кібергігієна, медіаграмотність і кібердетоксикація.

4. Проведено комплексне наукове дослідження визначення правового статусу кібератак та кібервійськових операцій, який до сих пір досліджено лише фрагментарно.

Трансформація конфліктної активності в кіберпростір провокує швидку глобалізацію конфронтації з можливістю залучення міжнародних учасників, які мають вплив на міжнародні процеси. Враховуючи особливості кіберпростору, кібератаки як форма політичного кіберконфлікту можуть призводити до міжнародних конфліктів, що охоплюють територіально визначені зони.

Визначено, що оскільки в інформаційному суспільстві формується уявлення про кіберконфлікт, негативні наслідки його ескалації, то інформаційне протиборство здійснюється для впливу на масову свідомість, за допомогою спотворення реальності щодо наслідків конфронтації сторін. Результати кіберконфліктів мають вагомий вплив на процес прийняття найважливіших у світі політичних рішень.

5. Показано, що трансформація у військових атак у кібервійськові є проявом осучаснення ведення військових дій та реалізації глобалізаційних змін. Доведено, що кібервійськові атаки стають невід'ємною формою існування демократичного устрою. Визначено, що виникає потреба у формуванні системи реагування органами управління, на небезпеку, яку вони можуть нести суспільству, в тому числі, необхідність у цифровій трансформації, як діяльності направленій на пошук ефективних механізмів захисту інформаційного середовища.

На прикладі НАТО, Сполучених Штатів Америки та Китайської Народної Республіки досліджено сучасний міжнародний досвід щодо реакції на кібератаки, або окремі форми прояву кіберборотьби, який, на сьогодні, зводиться до практики глобальних учасників на внутрішньому та зовнішньому рівні щодо реалізації кібервпливу на політичні процеси.

Показано, що сучасна російсько-українська війна демонструє використання спецслужбами інформації, яку громадяни публікують публічно в соціальних мережах. Держава-агресор активно використовує кіберпростір. Основною формою цього є створення арсеналу наступальної кіберзброї, застосування якої є незворотнім і може мати незворотні деструктивні наслідки. Водночас інформаційно-комунікаційні системи державних органів України та

об'єкти критичної інформаційної інфраструктури зазнають впливу, спрямованого на виведення їх з ладу (кібердиверсії), отримання негласного доступу та управління, ведення розвідувально-підривної діяльності.

6. Показано, що на даний час значною є проблема фішингових атак в технологічному секторі, яка потребує негайного вирішення, оскільки кіберзлочини, такі як шахрайство, крадіжка особистих даних, шпигунство та атаки на критичну інфраструктуру, можуть мати значні наслідки як для окремих осіб, так і для цілих організацій та держав.

Проведено дослідження проблеми кіберзлочинності та кібербезпеки, за результатами якого запропоновано напрямки удосконалення адміністративно-правових засад забезпечення кібербезпеки в Україні щодо боротьби з комп'ютерними злочинами й кібератаками.

Зазначено, що кіберзлочини часто складні для розслідування через брак кваліфікованих кадрів, необхідних інструментів та міжнародної співпраці.

7. З урахуванням загроз сьогодення запропоновано комплексний підхід до кіберзахисту, який поєднує різні методи та інструменти. Серед актуальних проблем кібербезпеки виділено такі:

кіберзлочинці постійно вдосконалюють свої методи, що робить кібератаки все більш складними для виявлення та нейтралізації;

існує гостра нестача фахівців з кібербезпеки, що ускладнює захист організацій від кібератак;

різні організації та країни мають різні підходи до кібербезпеки, що ускладнює міжнародну співпрацю;

зростання залежності від Інтернету робить суспільство більш вразливим до кібератак;

кіберзлочинність постійно еволюціонує, з'являються нові типи кіберзлочинів, що потребує постійного вдосконалення методів боротьби з ними.

Показано, що ефективна боротьба з кіберзлочинністю потребує співпраці між державами, приватним сектором та громадянами. Необхідно постійно вдосконалювати методи кібербезпеки, використовуючи нові технології та

підвищуючи обізнаність. Важливо розробити міжнародні стандарти та законодавство для боротьби з транснаціональною кіберзлочинністю. Майбутнє кібербезпеки залежить від здатності різних зацікавлених сторін працювати разом для захисту інформаційних систем та даних.

8. Запропоновано авторську методику впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України. Зазначений матеріал є актуальним сьогодні на глобальному рівні. В нашій державі викладена авторська пропозиція потребує окремої уваги. Зазначається, що авторська методика впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України потребує подальшого вивчення та аналізу.

Вважаємо, що в період воєнного часу авторська методика впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України є важливою та має бути впроваджена у вигляді відповідної програми з удосконалення обізнаності населення щодо існуючих механізмів захисту об'єктів кіберзахисту. Вона допоможе суспільству та поліпшить обізнаність щодо захисту своїх прав на конфіденційність інформації та об'єкти інтелектуальної власності тощо. Зростання ж обізнаності про кібербезпеку допоможе людям краще захищати себе від кіберзлочинності. Зазначена розробка є важливою та актуальною і надає гарантію захисту людських прав, під час воєнного вторгнення росії на територію України та на стадії відновлення.

Внесено пропозицію щодо поліпшення обізнаності населення шляхом реалізації відповідної інформаційної політики Кабінетом Міністрів України як органу, який відповідно до частини третьої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю, через профільні центральні органи виконавчої влади: Міністерство цифрової трансформації України, Міністерство культури та

стратегічних комунікацій України, Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України тощо.

9. Розглянуто поняття «злочинність у сфері комп'ютерної інформації», шляхом аналізу наукових та законодавчих визначень. Продемонстровано відмінності термінів «кіберзлочинність» і «злочинність у сфері комп'ютерної інформації». «Кіберзлочинність» охоплює злочини, пов'язані як з використанням комп'ютерних технологій, так і з глобальними мережами. Тоді, як «злочинність у сфері комп'ютерної інформації» більш конкретно стосується злочинів проти комп'ютерних систем або даних. Загалом можна констатувати, що сьогодні кіберзлочинність включає широкий спектр протиправних дій, від несанкціонованого доступу до державних комп'ютерних мереж і крадіжки особистих даних до фінансового шпигунства та відмивання грошей.

Проведено наукове дослідження сучасного стану кіберзлочинності та її впливу на безпеку держави. Визначено ключові загрози, що виникають у цифровому просторі, запропоновано адміністративно-правові методи запобігання та протидії цим загрозам у контексті забезпечення безпеки держави.

Визначено, що комп'ютерна злочинність постійно розвивається у зв'язку з удосконаленням і появою нових IT-технологій, збільшенням кількості користувачів Інтернету та мобільних пристроїв, а також переходом на електронний документообіг в організаціях. Комп'ютерні злочини можна розділити на незаконне використання програмного забезпечення, шахрайство та атаки, які використовують вразливі місця системи.

10. Показано, що вирішальним для забезпечення кібербезпеки є розвиток державних систем кібербезпеки. Зокрема, запропоновано модель двофакторної автентифікації державних службовців.

Визначено ключові напрямки, які слід враховувати при розробці стратегій кібербезпеки, серед яких:

стратегія кіберінформаційної протидії системам управління;

електронне протистояння;

психологічне кіберпротистояння;

хакерська війна (використання комп’ютерних технологій для незаконного доступу або порушення роботи ворожих систем);

кібернетичні та мережеві війни;

економічна кіберінформаційна війна.

Зроблено висновок щодо необхідності посилення державної кібербезпеки на всіх рівнях, від окремого користувача до національних державних органів. Розроблено рекомендації щодо захисту від кіберзагроз.

Показано, що останнім часом спостерігається суттєва зміна комплексу факторів, що визначають комп’ютерну злочинність на державному рівні. Крім традиційних соціальних, економічних, правових, кадрових, організаційних і технічних аспектів все більшого значення набувають політичні фактори. До них належать геополітичні аспекти, зокрема військово-політичні, глобальні економічні та міжнародні політичні елементи, а також політичні та спостережні фактори, пов’язані з недостатнім соціальним і державним контролем над кіберпростором. Інші важливі чинники включають політико-кримінальний (включаючи кібертероризм, кіберекстремізм і хактивізм), політико-інформаційний (кібершпигунство) та політико-інституційний (зловживання ІТ-технологіями). Ключовим моментом еволюції кіберзлочинності, що перетворює її на технотронний злочин, є її самовизначення. Цей процес означає здатність комп’ютерної злочинності до автономного регенерування, тобто до самостійного відтворення злочинів у соціальному середовищі. Ці прояви визначають перспективи подальших досліджень сучасних кіберзагроз та заходів щодо їх запобігання.

11. Розглянуто вплив кібербезпеки на функціонування фінансових установ. Внесено пропозиції щодо напрямків удосконалення адміністративно-правових засад його забезпечення. Зокрема, за допомогою таких засобів:

спеціалізоване програмне забезпечення;

низка технічних апаратних рішень, пов’язаних із цифровою інфраструктурою, підтримкою серверів і центрів обробки даних;

впровадження нормативної бази для обробки персональних даних клієнтів у фінансових установах та політики щодо їх використання.

Досліджено вплив сучасних тенденцій у кібербезпеці на стабільність фінансових установ. Розглянуто питання підтримки життєво важливих функцій кібербезпеки в контексті зростання цифрових загроз. Узагальнено практичний досвід великих фінансових установ у формуванні власної стратегії кібербезпеки та визначено особливості адміністративно-правових засад для підтримки цих інструментів.

Проаналізовано теоретичні, методологічні та практичні підходи до кіберзахисту та цифрових інструментів, які допомагають підтримувати стабільність фінансових установ, та запропоновано шляхи вдосконалення адміністративно-правових засад щодо їх ефективного функціонування.

Показано, що вплив кібербезпеки на стабільність функціонування фінансової установи є суттєвим, практично, вирішальним фактором, що забезпечує планування діяльності фінансової установи, мінімізацію та запобігання ризикам, безперервність функціонування всієї структури і вимагає високоякісних технологічних рішень. Узагальнено інформацію стосовно впливу кібербезпеки на стабільність функціонування фінансової установи. Розроблено комплекс заходів щодо запобігання відповідним ризикам та підвищення рівня кібербезпеки фінансових установ. Сформульовано заходи, які є ключовими у впливі на кібербезпеку банків та спрямовані на диверсифікацію ризиків та їх уникнення, використання хмарних сервісів і технологій автентифікації, а також посилення фінансового моніторингу.

12. Поведено аналіз наукової літератури, аналітичних публікацій широкого кола експертів і чинної нормативно-правової бази, на підставі якого сформульовано наступні основні проблеми та актуальні виклики сьогодення в сфері забезпечення кібербезпеки та кіберзахисту, протидії кіберзагрозам, таким як кібератаки та кіберзлочинність, в умовах воєнного стану та повоєнної відбудови України:

недостатній рівень кіберзахисту критичної інфраструктури;

недостатнє фінансування кібербезпеки;

дефіцит кваліфікованих спеціалістів;

високий рівень кіберзагроз;

низький рівень обізнаності громадян;

слабка координація між органами влади;

відсутність кіберстрахування;

низька кіберкультура в бізнесі;

відсутність стандартів кібербезпеки для блокчейн-технологій;

недостатній рівень міжнародної співпраці.

Запропоновано шляхи вирішення зазначених проблем у сфері кібербезпеки України, створення сучасної ефективної системи забезпечення кібербезпеки та кіберзахисту, що на даний час є вкрай актуальним питанням для нашої держави, шляхом вдосконалення нормативно-правового регулювання адміністративно-правових засад забезпечення кібербезпеки. Зокрема, розроблено законопроєкт, яким запропоновано системне та комплексне вдосконалення забезпечення кібербезпеки України. Законопроєктом пропонується внести зміни до статті 361 Кримінального кодексу України, статей 15 і 17 Закону України «Про захист прав споживачів», статті 8 Закону України «Про оперативно-розшукову діяльність», статті 6 Закону України «Про інформацію», статті 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах», статті 2^1 Закону України «Про державну підтримку сільського господарства України», статей 6, 12, 24 і 28 Закону України «Про захист персональних даних», статей 4 і 18 Закону України «Про державно-приватне партнерство», статті 16 Закону України «Про розвиток та державну підтримку малого і середнього підприємництва в Україні», статті 15 Закону України «Про зайнятість населення», статті 16 Закону України «Про технічні регламенти та оцінку відповідності», статті 14 Закону України «Про електронну комерцію», статті 48 Закону України «Про державну службу», статті 4 Закону України «Про публічні закупівлі», статті 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», статей 6, 8, 9, 11 і 13 Закону України «Про основні засади забезпечення кібербезпеки України»,

статті 31 Закону України «Про національну безпеку України», статті 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», статей 31 і 104 Закону України «Про електронні комунікації», статей 21 і 22 Закону України «Про критичну інфраструктуру», статті 4 Закону України «Про страхування», статті 9 Закону України «Про віртуальні активи». З метою імплементації зазначених законодавчих змін також розроблено пропозиції до постанов і розпоряджень Кабінету Міністрів України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

4. Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

5. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

6. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Центр досліджень соціальних комунікацій НБУВ. [Електронний ресурс]. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2759:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnimzagrozam&catid=8&Itemid=350.

7. Статистика кібератак на українську критичну інформаційну інфраструктуру: 15 – 22 березня. Офіційний веб-портал Державної служби спеціального зв'язку та захисту інформації України. 2022. [Електронний ресурс].

URL: https://www.cip.gov.ua/ua/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya.

8. Завгородня Ю.В. Кіберконфлікти як сучасна загроза цифровізації суспільства: політичний аспект. Актуальні проблеми філософії та соціології. 2022. № 35. С. 90.

9. Ржевська Н.Ф. Геоінформаційний чинник, як механізм трансформації міжнародних конфліктів. Вісник Донецького національного університету. Політичні науки. 2016. С. 45–46.

10. Ожеван М. Фронти й тили великих інформаційних війн: загальні інформаційні потреби та інтереси. Підприємництво в Україні. 2001. № 4(5). С. 20.

11. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навч. посіб. / за заг. ред. В.О. Жадька ; ред.-упор. О.І. Харитоненко, Ю.С. Полтавець. Київ: Видавництво НПУ імені М. П. Драгоманова, 2018. 356 с.

12. The National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security (February 2003). [Електронний ресурс]. URL: https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf.

13. Виноградський О. Нова кіберстратегія США: плани і цілі. 30.03.2017. Defense Express. [Електронний ресурс]. URL: https://old.defence-ua.com/index.php/statti/2642-nova-kiberstratehiya-ssha-plany-i-tsili.

14. D. Volz. Trump signs order aimed at upgrading government cyber defences. 12.05.2017. Reuters. [Електронний ресурс]. URL: https://www.reuters.com/article/us-usa-trump-cyber-idUSKBN1872L9/?il=0.

15. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11, 2017. Офіційний веб-портал. [Електронний ресурс]. URL: https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

16. Zavhorodnia Yu. Features of protection of China’s national interests within cybernetic space. European Political and Law Discourse. 2021. Vol. 8. Issue 6. P. 38.

17. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 190 с.

18. Костюкова Ю. Польща та Україна підписали меморандум про співпрацю у сфері кіберзахисту. Вебсайт mind.ua. 22.08.2022. [Електронний ресурс]. URL: https://mind.ua/news/20245980-polshcha-ta-ukrayina-pidpisali-memorandum-pro-spivpracyu-u-sferi-kiberzahistu.

19. Лідери країн НАТО схвалили комплексну політику кіберзахисту альянсу. Вебсайт Інтерфакс-Україна. 14.06.2021. [Електронний ресурс]. URL: https://ua.interfax.com.ua/news/general/750063.html.

20. Гвоздь В. Кіберконфлікт і геополітика – новий фронт «холодної війни». Європа загальних цінностей або Європа спільних інтересів?: матеріали 28-ого економічного форуму, м. Криниця-Здруй, Польща, 4-6 вересня 2018 р. Криниця-Здруй, Польща, 2018. [Електронний ресурс]. URL: https://bintel.org.ua/nash_archiv/arxiv-voyenni-pitannya/arxiv-gibridnia-vijna/09_05_krynica/.

21. Завгородня Ю.В. Роль НАТО у боротьбі з кіберконфліктами. Регіональні студії. 2022. № 30. С. 67.

22. Zavhorodnia Yu.V. Political conflicts as a prerequisite for the Russian-Ukrainian war: manipulative features. The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects: Scientific monograph. Riga, Latvia : «Baltija Publishing», 2022. С. 911. 1436 p).

23. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. Юридичний науковий електронний журнал. 2022. № 12. С. 409–414. [Електронний ресурс]. DOI: https://doi.org/10.32782/2524-0374/2022-12/96.

24. Geers K. Strategic cyber security. Tallinn. NATO Cooperative Cyber Defence Centre of Excellence, 2011. 169 p. [Електронний ресурс]. URL: https://ccdcoe.org/library/publications/strategic-cyber-security/.

25. Музика В. В. Атрибуція кібератак проти об’єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення: дис. д-ра філософії: 081 / Нац. ун-т. «Одеська юридична академія». Одеса, 2021. 219 с.

26. Фещуков Г. В. Застосування МГП по відношенню до кібероперацій, що проводяться під час збройних конфліктів. Юридичний науковий електронний журнал. 2023. № 9. С. 437–439. [Електронний ресурс]. DOI: https://doi.org/10.32782/2524-0374/2023-9/106.

27. L. Freeman, A. Ghahremani, S. Lombardo. The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris. Веб-сайт. [Електронний ресурс]. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russiascyberwar-against-ukraine/.

28. K. Chan Yoon Onn. The Prosecutor’s New Policy on ‘Cyber Operations’ before the International Criminal Court (and its Implications for Ukraine): Some Preliminary Reflections. Blog of the European Journal of International Law. [Електронний ресурс]. Веб-сайт. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-the-international-criminal-court-and-its-implications-for-ukraine-some-preliminary-reflections/.

29. Information for victims. Офіційний веб-сайт Міжнародного кримінального суду. [Електронний ресурс]. URL: https://www.icc-cpi.int/victims/ukraine.

30. Римський статут Міжнародного кримінального суду. Офіційний веб-сайт Міністерства юстиції України. [Електронний ресурс]. URL: https://minjust.gov.ua/m/mijnarodniy-kriminalniy-sud.

31. Michael N. Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. 2013. [Електронний ресурс]. DOI: https://doi.org/10.1017/CBO9781139169288.

32. Eichensehr, K. Ukraine, cyberattacks, and the lessons for international law. AJIL Unbound, 2022. v. 116. С. 145 – 149. [Електронний ресурс]. DOI: https://doi.org/10.1017/aju.2022.20.

33. Di Nicola, A. Towards digital organized crime and digital sociology of organized crime. Trends Organized Crime. 2022. [Електронний ресурс]. DOI: https://doi.org/10.1007/s12117-022-09457-y.

34. Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., Orlovskyi, R. Cybersecurity as a component of the national security of the state. Journal of Security and Sustainability. 2020. v. 9. Issues 3. C. 775 - 784. [Електронний ресурс]. DOI: https://doi.org/10.9770/jssi.2020.9.3(4).

35. Wang, P., Su, M. and Wang, J. 2021. Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer-to-peer lending market in China. The British Journal of Criminology, 2021. v. 61. Issues 2. C. 303 – 324. [Електронний ресурс]. DOI: https://doi.org/10.1093/bjc/azaa064.

36. Shablystyi, V., Prymachenko, V., Filipp, A., Doroshenko, L., Burbyka, V. Legal principles of cyber protection of critical infrastructure facilities. 2019. Journal of Legal, Ethical and Regulatory. v. 22. Issues 6. C. 1-6. [Електронний ресурс]. URL: https://www.abacademies.org/articles/Legal-principles-of-cyber-protection-of-critical-infrastructure-facilities-1544-0044-22-6-430.pdf.

37. Collier, B., Clayton, R., Hutchings, A. and Thomas, D. Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. The British Journal of Criminology. 2021. v. 61. Issues 5. C. 1407 – 1423. [Електронний ресурс]. DOI: https://doi.org/10.1093/bjc/azab026.

38. Jordan, K., Weller, M. Academics and social networking sites: benefits, problems and tensions in professional engagement with online networking. Journal of Interactive Media in Education. 2018. Issues 1. pp. 1 - 9. [Електронний ресурс]. DOI: https://doi.org/10.5334/jime.448.

39. Avanesova, N., Tahajuddin, S., Hetman, O., Serhiienko, Y., Makedon, V. Strategic management in the system model of the corporate enterprise organizational development. Economics and Finance, 2021. v. 1. Issues 9. C. 18 – 30. [Електронний ресурс]. DOI: https://doi.org/10.51586/2311-3413.2021.9.1.18.30.

40. Holt, T.J., Chermak, S.M., Freilich, J.D., Turner, N., Greene- Colozzi, E. Introducing and Exploring the Extremist Cybercrime Database (ECCD). Crime &

Delinquency, 2022. Volume 69, Issue 12. С. 2411 – 2436. [Електронний ресурс]. DOI: https://doi.org/10.1177/00111287221083899.

41. Akoto, W. Accountability and cyber conflict: examining institutional constraints on the use of cyber proxies. Conflict Management and Peace Science, 2022. v. 39. Issues 3. с. 311 – 332. [Електронний ресурс]. DOI: https://doi.org/10.1177/07388942211051264.

42. Dupont, B., Whelan, C. Enhancing relationships between criminology and cybersecurity. Journal of Criminal Law and Criminology, 2021. v. 54. Issues 1. С. 76 – 92. [Електронний ресурс]. DOI: https://doi.org/10.1177/00048658211003925.

43. Chowdhury, N., Nystad, E., Reegård, K., Gkioulos, V. Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 2022. V. 12. Issues 3. С. 299 - 310. [Електронний ресурс]. DOI: https://doi.org/10.18280/ijsse.120304.

44. Leukfeldt, E. R., Lavorgna, A., Kleemans, E. R. Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. The European Journal on Criminal Policy and Research, 2017. V. 23. Issues 3. С. 287 – 300. [Електронний ресурс]. DOI: https://doi.org/10.1007/s10610-016-9332-z.

45. Tropina, T. Cybercrime: Setting international standards. Routledge handbook of international cybersecurity. Routledge, London, 2020. Chapter 11, pp. 148 – 160. [Електронний ресурс]. DOI: https://doi.org/10.4324/9781351038904.

46. Lavorgna, A. Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology. Trends in Organized Crime. 2023. [Електронний ресурс]. DOI: https://doi.org/10.1007/s12117-023-09486-1.

47. V. Ievdokymov, A. Frikel, V. Polishchuk, S. Savchuk, I. Klimova. Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention. Economic Affairs. 2024. Vol. 69, Issue 1 Special. pp. 61 – 69. [Електронний ресурс]. DOI: https://doi.org/10.46852/0424-2513.1.2024.8.

48. Cybersecurity in the United Nations system organizations. 2021. Офіційний веб-портал. [Електронний ресурс]. URL: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf.

49. Makedon, V., Zaikina, H., Slusareva, L., Shumkova, O., Zhmaylova, O. Rebranding in the Enterprise Market Policy. Proceedings of the 34rd International Business Information Management Association Conference, IBIMA Conference: 13 - 14 November 2019, Madrid, Spain. pp. 9472-9476. [Електронний ресурс]. URL: https://ibima.org/accepted-paper/rebranding-in-the-enterprise-market-policy/.

50. B. Lenaerts-Bergmans. 10 Types of Social Engineering Attacks and how to prevent them. November 08, 2023. Сайт Crowdstrike. [Електронний ресурс]. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/.

51. Dumchykov, M., Utkina, M., Bondarenko, O. Cybercrime as a Threat to the National Security of the Baltic States and Ukraine: The Comparative Analysis. International Journal of Safety and Security Engineering. 2022. Vol. 12, Issue 4. pp.481-490. [Електронний ресурс]. DOI: https://doi.org/10.18280/ijsse.120409.

52. Chief Economists Outlook, May 2023. [Електронний ресурс]. URL: https://www3.weforum.org/docs/WEF_Chief_Economists_Outlook_May2023.pdf.

53. L. Kormych, Y. Zavhorodnia. The concept of modern political confrontation in cyber space. Journal of Cybersecurity, 2023. Vol. 9. Issues 1. pp. 1 – 7. [Електронний ресурс]. DOI: https://doi.org/10.1093/cybsec/tyad017.

54. Drafting Data Protection Legislation: A Study of Regional Frameworks. 2023. Офіційний веб-сайт ПРООН. [Електронний ресурс]. URL: https://www.undp.org/publications/drafting-data-protection-legislation-study-regional-frameworks.

55. Heidi, A. Digital transformation, development and productivity in developing countries: is artificial intelligence a curse or a blessing? Review of Economics and Political Science, 2022. vol. 7. Issues 4. C. 238 – 256. [Електронний ресурс]. DOI: https://doi.org/10.1108/REPS-11-2019-0145.

56. McAfee, A., Brynjolfsson, E. Machine, Platform, Crowd: Harnessing Our Digital Future. New York: W.W. Norton & Company. 2017. 416 с. Електронний ресурс]. URL: https://wwnorton.com/books/Machine-Platform-Crowd/.

57. J. Pearson, C. Bing. The cyber war between Ukraine and Russia: An overview. Reuters, 10.05.2022. [Електронний ресурс]. URL: https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/.

58. Johansson, E., Johansson, K.M. Along the government–media frontier: Press secretaries offline/online. Journal of Public Affairs, 2022. Vol. 22. Issues S1. [Електронний ресурс]. DOI: https://doi.org/10.1002/pa.2759.

59. Taherdoost, H. Cybersecurity vs. Information Security. Procedia Computer Science, 2022. Vol. 215. pp. 483-487. [Електронний ресурс]. DOI: https://doi.org/10.1016/j.procs.2022.12.050.

60. Ross, P., Maynard, K. Towards a 4th industrial revolution. Intelligent Buildings International, 2021. Vol. 13. Issues 3. pp. 159 - 161. [Електронний ресурс]. DOI: https://doi.org/10.1080/17508975.2021.1873625.

61. Makedon, V., Krasnikova, N., Krupskyi, O., Stasiuk, Y. Arrangement of Digital Leadership Strategy by Corporate Structures: A Review. Economic Studies Journal, 2022. Vol. 31. Issues 8. pp. 19-40.

62. A. Hakeem, S. A., Hussein, H. H., Kim, H. Security requirements and challenges of 6G technologies andapplications. Sensors. 2022. Vol. 22. Issues 5. Number 1969. pp. 1 - 43. [Електронний ресурс]. DOI: https://doi.org/10.3390/s22051969.

63. Hodula, M. Does Fintech credit substitute for traditional credit? Evidence from 78 countries. Finance Research Letters, 2022. Vol. 46. Part B. [Електронний ресурс]. DOI: https://doi.org/10.1016/j.frl.2021.102469.

64. Levytska, S., Pershko, L., Akimova, L., Akimov, O., Havrilenko, K., & Kucherovskii, O. A risk-oriented approach in the system of internal auditing of the subjects of financial monitoring. International Journal of Applied Economics, Finance

and Accounting, 2022. Vol. 14. Issues 2. pp. 194-206. [Електронний ресурс]. DOI: https://doi.org/10.33094/ijaefa.v14i2.715.

65. Anand, K., Duley, C., Gai, P. Cybersecurity and Financial Stability. Deutsche Bundesbank Discussion Paper. 2022. No. 08. 53 c. [Електронний ресурс]. DOI: http://doi.org/10.2139/ssrn.4073158.

66. Buchak, G., Matvos, G., Piskorski, T., Seru, A. Fintech, regulatory arbitrage, and the rise of shadow banks. Journal of Financial Economics, 2018. Vol. 130. Issues 3. pp. 453–483. [Електронний ресурс]. DOI: https://doi.org/10.1016/j.jfineco.2018.03.011.

67. Nikonenko, U., Shtets, T., Kalinin, A., Dorosh, I., Sokolik, L. Assessing the policy of attracting investments in the main sectors of the economy in the context of introducing aspects of Industry 4.0. International Journal of Sustainable Development and Planning, 2022. Vol. 17. Issues 2. pp. 497-505. [Електронний ресурс]. DOI: https://doi.org/10.18280/ijsdp.170214.

68. Melnyk, D. S., Parfylo, O. A., Butenko, O. V., Tykhonova, O. V., Zarosylo, V. O. Practice of the member states of the European Union in the field of anti-corruption regulation. Journal of Financial Crime, 2022. Vol. 29. Issues 3. pp. 853-863. [Електронний ресурс]. DOI: https://doi.org/10.1108/JFC-03-2021-0050.

69. Kotidis, A., Schreft, S. Cyberattacks and Financial Stability: Evidence from a Natural Experiment. Finance and Economics Discussion Series 2022-025. Washington: Board of Governors of the Federal Reserve System. May 2022. 55 c. Офіційний веб-сайт Федеральної Резервної Системи США. [Електронний ресурс]. DOI: https://doi.org/10.17016/FEDS.2022.025.

70. Cerasi, V., Deininger, S., Gambacorta, L., Oliviero, T. How post-crisis regulation has affected bank CEO compensation. Journal of International Money and Finance, Forthcoming. 2020. Vol. 104. [Електронний ресурс]. DOI: https://doi.org/10.1016/j.jimonfin.2020.102153.

71. Sumets, A., Kniaz, S., Heorhiadi, N., Skrynkovskyy, R., Matsuk, V. Methodological toolkit for assessing the level of stability of agricultural enterprises.

Agricultural and Resource Economics, 2022. Vol. 8. Issues 1. pp. 235-255. [Електронний ресурс]. DOI: https://doi.org/10.51599/are.2022.08.01.12.

72. Novak, A., Pravdyvets, O., Chornyi, O., Sumbaieva, L., Akimova, L., Akimov, O. Financial and economic security in the field of financial markets at the stage of european integration. International Journal of Professional Business Review, 2022. Vol. 7. Issues 5. pp. 01 – 20. [Електронний ресурс]. DOI: https://doi.org/10.26668/businessreview/2022.v7i5.e835.

73. Atstaja, D., Koval, V., Grasis, J., Kalina, I., Kryshtal, H., Mikhno, I. Sharing model in circular economy towards rational use in sustainable production. Energies, 2022. Vol. 15. Issues 3. No. 939. [Електронний ресурс]. DOI: https://doi.org/10.3390/en15030939.

74. Ceylan, I. E. The impact of firm-specific and macroeconomic factors on financial distress risk: A case study from Turkey. Universal Journal of Accounting and Finance, 2021. Vol. 9. Issues 3. pp. 506–517. [Електронний ресурс]. DOI: https://doi.org/10.13189/ujaf.2021.090325.

75. Böhme, R., Laube, S., Riek, M. A Fundamental Approach to Cyber Risk Analysis. Variance Journal. 2017. vol. 12. Issues 2. pp. 161 – 185. [Електронний ресурс]. URL: https://www.casact.org/sites/default/files/2021-07/Approach-Cyber-Risk-Bohme-Laube-Riek.pdf.

76. Kou, G., Olgu Akdeniz, Ö., Dinçer, H., S. Yüksel. Fintech investments in European banks: a hybrid IT2 fuzzy multidimensional decision-making approach. Financial Innovation, 2021. Vol. 7. No. 39. [Електронний ресурс]. DOI: https://doi.org/10.1186/s40854-021-00256-y.

77. Hu, D., Zhao, S., Yang, F. Will fintech development increase commercial banks' risk-taking? Evidence from China. Electronic Commerce Research. 2022. Vol. 24. pp. 37 – 67. [Електронний ресурс]. DOI: https://doi.org/10.1007/s10660-022-09538-8.

78. Hooks, D., Davis, Z., Agrawal, V., Li, Z. Exploring factors influencing technology adoption rate at the macro level: A predictive model. Technol. Soc., 2022. Vol. 68. [Електронний ресурс]. DOI: https://doi.org/10.1016/j.techsoc.2021.101826.

79. Borodina, O., Kryshtal, H., Hakova, M., Neboha, T., Olczak, P., Koval, V. A. conceptual analytical model for the decentralized energy-efficiency management of the national economy. Polityka Energetyczna, 2022. Vol. 25. Issues 1. pp. 5 - 22. [Електронний ресурс]. DOI: https://doi.org/10.33223/epj/147017.

80. Schmidt, E., Cohen, D. The New Digital Age: Reshaping the Future of People, Nations and Business. 1st ed. New York: Knopf, 2013, 315 p.

81. Zayed, N. M., Edeh, F. O., Darwish, S., Islam, K. M. A., Kryshtal, H., Nitsenko, V., Stanislavyk, O. Human resource skill adjustment in service sector: Predicting dynamic capability in post-COVID-19 work environment. Journal of Risk and Financial Management, 2022. Vol. 15. Issues 9, pp. 3-12. [Електронний ресурс]. DOI: https://doi.org/10.3390/jrfm1509040.

82. Kovalko, O., Eutukhova, T., Novoseltsev, O. Energy-Related Services as a Business: Eco-Transformation Logic to Support the Low-Carbon Transition. Energy Engineering, 2022. Vol. 119. Issues 1, pp. 103–121. [Електронний ресурс]. DOI: https://doi.org/10.32604/EE.2022.017709.

83. Lelyk, L., Olikhovskyi, V., Mahas, N., Olikhovska, M. An integrated analysis of enterprise economy security. Decision Science Letters, 2022. Vol. 11. Issues 3, pp. 299-310. [Електронний ресурс]. DOI: https://doi.org/10.5267/j.dsl.2022.2.003.

84. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань. Київ, 2019. №9 (вересень). 80 с. [Електронний ресурс]. URL: https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi.

85. І. Довгаль, О. Войтович, Д. Майорников. Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак. Освітній серіал. 2018. [Електронний ресурс]. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

86. Borodina, O., Kryshtal, H., Hakova, M., Neboha, T., Olczak, P., Koval, V. A conceptual analytical model for the decentralized energyefficiency management of the national economy. Polityka Energetyczna – Energy Policy Journal, 2022. Vol. 25. Issues 1, pp. 5-22. [Електронний ресурс]. DOI: https://doi.org/10.33223/epj/147017.

87. І. З. Брацук. Теоретико-правові засади імплементації права Європейського Союзу в національне право держав-членів: монографія Львів: ЛНУ імені Івана Франка, 2016. 230 с.

88. Шемчук В. В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз: монографія. Київ: Видавництво Ліра-К, 2020. 352 с.

89. Kovacs, L. Cyber Security Policy and Strategy in the European Union and NATO. Land Forces Academy Review, 2018. Vol. 23. Issues 1, pp. 16 – 24. [Електронний ресурс]. DOI: https://doi.org/10.2478/raft-2018-0002.

90. Клименко Н. Г. Еволюція змісту концепту «безпека» за різних історичних епох та політичних систем. Державне управління: удосконалення та розвиток. 2019. № 8. [Електронний ресурс]. DOI: https://doi.org/10.32702/2307-2156-2019.8.20.

91. Пазюк А. В. Міжнародне інформаційне право: теорія і практика. Монографія. Дніпропетровськ: «Середняк Т. К.», 2015. 447 с. [Електронний ресурс]. URL: https://www.iir.edu.ua/sites/default/files/2023-03/%D0%9F%D0%B0%D0%B7%D1%8E%D0%BA_%D0%90_%D0%92_%20%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B5%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5%20%D0%BF%D1%80%D0%B0%D0%B2%D0%BE_%D1%82%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D1%96%20%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B0.pdf.

92. Voytsikhovkyy, A. Cyber security as an important component of the national security protection system of European countries. Journal of East European Law, 2018. Vol. 53, pp. 26-37. [Електронний ресурс]. URL: http://easternlaw.com.ua/wpcontent/uploads/2018/07/voytsikhovskyy_53.pdf.

93. А. Пазюк. Приватність та Інтернет. Офіційний інформаційний портал Харківської правозахисної групи «Права людини в Україні». 04.09.2000. [Електронний ресурс]. URL: https://khpg.org/968016432.

94. Bulavina, S., Davydova, T. Consequences of non-compliance with the right to privacy on the Internet: an international aspect. Historical and Legal Journal, 2020. Issues 1(15), pp. 8 - 13. [Електронний ресурс]. URL: http://chasopys.hl.vnu.volyn.ua/index.php/chasopys/issue/view/15.

95. Бакалінська О. О. Правове забезпечення кіберзахисту в Україні. Координата. Платформа стратегічної та законотворчої аналітики. 24.02.2020. [Електронний ресурс]. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini.

96. О. Бакалінська. Сучасні тенденції правового регулювання кібербезпеки та інтелектуальної власності. Теорія і практика інтелектуальної власності, 2022. № 5, с. 82 - 92. [Електронний ресурс]. DOI: https://doi.org/10.33731/52022.270899.

97. Lytvyn, N., Andrushchenko H., Zozulya Y., Nikanorova O., Rusal L. Enforcement of court decisions as a social guarantee of protection of citizens' rights and freedoms. Prawo i Wiez, 2022. Vol. 39, pp. 80-102. [Електронний ресурс]. DOI: https://doi.org/10.36128/priw.vi39.351.

98. Mia, M. M., Rizwan, S., Zayed, N. M., Nitsenko, V., Miroshnyk, O., Kryshtal, H., Ostapenko, R. The Impact of Green Entrepreneurship on Social Change and Factors Influencing AMO Theory. Systems, 2022. Vol. 10. Issues 5, pp. 1 - 19. [Електронний ресурс]. DOI: https://doi.org/10.3390/systems10050132.

99. О. Звездова, О. Вакалюк. Стратегія забезпечення кібербезпеки в гібридній війні. Acta de Historia & Politica: Saeculum, 2021-2022. Vol. 3, с. 82 - 90, [Електронний ресурс]. DOI: https://doi.org/10.26693/ahpsxxi2021-2022.03.082.

100. Бірюков Д. С., Кондратов С. І. Стратегія захисту критичної інфраструктури в системі національної безпеки держами. Стратегічні пріоритети, 2012, № 3 (24). С. 107 – 113.

101. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь / Д. С. Бірюков, С. І. Кондратов. Київ: Національний інститут стратегічних досліджень, 2012. 96 с. Офіційний веб-сайт Національного інституту стратегічних досліджень. [Електронний ресурс]. URL: https://niss.gov.ua/sites/default/files/2013-02/Sots_zahust-86178.pdf.

102. Declaration by the Committee of Ministers on Internet governance principles, Adopted by the Committee of Ministers on 21 September 2011, at the 1121st meeting of the Ministers' Deputies, Council of Europe. Committee of Ministers, 2011. Офіційний веб-сайт Council of Europe Portal. [Електронний ресурс]. URL: https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016805cc2f6%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}.

103. The Internet Governance Strategy for 2016-2019, Adopted by the Committee of Ministers on 30 March 2016, at the 1252th meeting of the Ministers' Deputies, Council of Europe. Committee of Ministers, 2016. Офіційний веб-сайт Council of Europe Portal. [Електронний ресурс]. URL: https://rm.coe.int/internet-governance-strategy-2016-2019-updated-version-06-mar-2018/1680790ebe.

104. Резолюція Генеральної Асамблеї ООН A/RES/75/176 «Право на приватність у цифрову епоху» від 16 грудня 2020 року. Офіційний веб-сайт Організації Об'єднаних Націй. [Електронний ресурс]. URL: https://digitallibrary.un.org/record/3896430?v=pdf#files.

105. Ю. Даниленко. Від Ш до І: що таке штучний інтелект та як він трансформує світ. Speka. 01.02.2022. [Електронний ресурс]. URL: https://speka.media/ai/vid-s-do-i-shhotake-stucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039.

106. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS COM(2021) 118 final «2030 Digital Compass: the European way for the Digital Decade» on 09.03.2021. Офіційний веб-сайт Європейської Комісії. [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118.

107. Конвенція про кіберзлочинність від 23 листопада 2001 року. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

108. Конституція України від 26 червня 1996 року. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

109. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

110. The end of privacy. The Economist. 29.04.1999. [Електронний ресурс]. URL: https://www.economist.com/leaders/1999/04/29/the-end-of-privacy.

111. Діордіца І. В. Поняття та зміст національної системи кібербезпеки. 2016. Офіційний веб-сайт Глобальної організації союзницького лідерства. [Електронний ресурс]. URL: https://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/.

112. Franscella, J. Cybersecurity vs. cyber security: When, why and how to use the term. SecurityWeek. 17.07.2013. [Електронний ресурс]. URL: http://www.infosecisland.com/blogview/23287-Cybersecurity-vsCyber-Security-When-Why-and-How-to-Use-the-Term.html.

113. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України. Дис. канд. юрид. наук: 12.00.07. Суми, 2018. 221 с. [Електронний ресурс]. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/70638/1/diss_Bukhariev.pdf.

114. Коваленко Н. В. Про правовий режим кібербезпеки в Україні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 96 - 100. [Електронний ресурс]. URL: http://nbuv.gov.ua/UJRN/apvu_2016_3_24.

115. Stubley, D. What is cyber security? 7elements. 07.07.2013. [Електронний ресурс]. URL: https://www.7elements.co.uk/resources/blog%20/what-is-cyber-security/.

116. Information systems defence and security: France’s strategy. – French Network and Information Security Agency. 2011. 24 с. [Електронний ресурс]. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/France_2011_2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

117. Cyber Security Strategy for Germany. Офіційний веб-портал Федерального Міністерства внутрішніх справ, будівництва і громад ФРН.

[Електронний ресурс]. URL: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=5.

118. Nationai Cyber Security Strategy. Офіційний веб-портал Міністерства громадської безпеки Канади. [Електронний ресурс]. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

119. Government of Canada's Enterprise Cyber Security Strategy. Офіційний веб-портал Уряду Канади. [Електронний ресурс]. URL: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html.

120. National Cyber Security Strategy and Action Plan (2020-2023). 29.12.2020. Офіційний веб-портал Офісу цифрової трансформації при Президентові Турецької Республіки. [Електронний ресурс]. URL: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf.

121. The Netherlands Cybersecurity Strategy 2022-2028. 06.12.2022. National Coordinator for Counterterrorism and Security Ministry of Justice and Security. Офіційний веб-портал. [Електронний ресурс]. URL: https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028.

122. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. НАПрН України, Науково-дослідний інститут інформатики і права. Київ: Видавничий дім «АртЕк». 2017. 107с.

123. 2023-2030 Australian Cyber Security Strategy. 22.11.2023. Офіційний веб-портал Департаменту внутрішніх справ Уряду Австралії. [Електронний ресурс]. URL: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf.

124. Рекомендації Міжнародного телекомунікаційного союзу X.1205 від 18 квітня 2008 року «Мережі передачі даних, відкриті системи комунікацій та безпека». Офіційний веб-портал Міжнародного телекомунікаційного союзу. [Електронний ресурс]. URL: https://www.itu.int/rec/t-rec-x.1205-200804-i.

125. Schatz D., Bashroush R., Wall J. Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security. Journal of Digital Forensics, Security and Law. 2017. № 2. С. 54-74. [Електронний ресурс]. DOI: https://doi.org/10.15394/jdfsl.2017.1476.

126. Alan Calder. Cyber Security: Essential principles to secure your organisation – a pocket guide. ITGP, 2020. 80 с. [Електронний ресурс]. URL: https://www.itgovernance.co.uk/shop/product/cyber-security-essential-principles-to-secure-your-organisation-a-pocket-guide.

127. І. М. Сопілко. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. Юридичний вісник. 2021. Випуск 2 (59). с. 110 – 115. [Електронний ресурс]. DOI: https://doi.org/10.18372/2307-9061.59.15603.

128. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. Випуск № 2 (42). с. 54 – 62. [Електронний ресурс]. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf.

129. Мельник С. В., Тихомиров О. О., Лєнков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. Збірник наукових праць Військового інституту Київськог національного університету імені Тарас Шевченка. 2011. Вип. № 30. С. 165-171. [Електронний ресурс]. URL: http://www.library.univ.kiev.ua/ukr/host/viking/db/ftp/univ/znp_vi_knu/znp_vi_knu_2011_30.pdf.

130. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. Вип. № 2 (5). С. 162-169. [Електронний ресурс]. DOI: https://doi.org/10.37750/2616-6798.2012.2(5).271955.

131. Регламент Європейського парламенту і Ради (ЄС) від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної

безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку). Урядовий портал. [Електронний ресурс]. URL: https://www.kmu.gov.ua/storage/app/sites/1/55-GOEEI/es-2019881.pdf.

132. Бурячок В. Л., Корченко О. Г., Хорошко В. О., Кудінов В. А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. Захист інформації. 2013. Том 15, № 1. С. 5–12.

133. Корченко О. Г., Бурячок В. Л., Гнатюк С. О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. Ukrainian Scientific Journal of Information Security. 2013. Vol. 19. Issue 1. С. 40–44. [Електронний ресурс]. DOI: https://doi.org/10.18372/2225-5036.19.4697.

134. Великий тлумачний словник сучасної української мови / [укл. О. Єрошенко]. — Донецьк : ТОВ «Глорія Трейд», 2012. — 864 с.

135. Запорожець О. Ю. Політика європейського союзу в сфері інформаційної безпеки. Актуальні проблеми міжнародних відносин : зб. наук. пр. Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. Київ. 2009. Вип.87, ч.2. С.36-45.

136. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ: Міжвідом. наук.-дослід. центр з проблеми боротьби з організ. злочинністю, 2012. № 2 (28). С.299-309.

137. Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

138. Рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», введене в дію Указом Президента України від 15 березня 2016 року № 96. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16#n10.

139. Білодід І. К. Словник української мови: в 11 т. Київ: Наукова думка. 1970–1980. Т. 3. 580 с.

140. Грінченко Б. Словник української мови. Київ: Видавництво Академії Наук Української РСР, 1958. Том 2. 766 с.

141. Глушков В. М. Енциклопедія кібернетики у т. 1. Київ, 1974. 596 с.

142. Коломієць О. В. Проблеми національного законодавства в сфері боротьби з кіберзлочинністю та шляхи їх вирішення. Гілея. 2012. Вип. 57 (№ 2). С. 546–551.

143. Шеломенцев В. П. Кримінологічна безпека у кіберпросторі: система понять. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2010. Вип. № 23. С. 342–348.

144. Зуй В. В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. Правове забезпечення адміністративної реформи. 2022. Вип. 4. Ч. 1. С. 231 – 235. [Електронний ресурс]. DOI: https://doi.org/10.32850/sulj.2022.4.1.35.

145. Мануілов Я. С. Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни. Інформація і право. 2023. № 1(44). С. 154 – 167. [Електронний ресурс]. URL: https://ippi.org.ua/sites/default/files/15_25.pdf.

146. М. Делембовський, В. Ткаченко, Д. Мельник. Захист критичної інфраструктури України від кібератак. *Grail of Science*. № 41, pp. 277 – 281. [Електронний ресурс]. DOI: https://doi.org/10.36074/grail-of-science.05.07.2024.043.

147. О. Янковський. Україні потрібна нова кіберстратегія. Українська правда. 14.09.2019. [Електронний ресурс]. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/.

148. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об’єктів критичної інфраструктури». [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

149. Розпорядженням Кабінету Міністрів України від 19 вересня 2023 р. № 25 «Про затвердження Національного плану захисту та забезпечення безпеки

та стійкості критичної інфраструктури». [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text.

150. *Б. Садомська.* Український кіберпростір: безпекові загрози, виклики та перспективи розвитку. 15.12.202. Офіційний веб-сайт Аналітичного центру ADASTRA. [Електронний ресурс]. URL: https://adastra.org.ua/blog/ukrayinskij-kiberprostir-bezpekovi-zagrozi-vikliki-ta-perspektivi-rozvitku?utm_source=chatgpt.com.

151. Закон України «Про публічні закупівлі» від 25 грудня 2015 року № 922-VIII. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/922-19#Text.

152. Закон України «Про державно-приватне партнерство» від 1 липня 2010 року № 2404-VI. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2404-17.

153. В Україні бракує спеціалістів: які сфери зазнали дефіциту. PROZORO. 18.11.2024. [Електронний ресурс]. URL: https://prozoro.net.ua/ua/2024/11/18/v-ukrayini-brakuye-speczialistiv-yaki-sfery-zaznaly-deficzytu/.

154. Кіберзагрози зростають, а спеціалістів стає дедалі менше. 10Guards. 18.10.2024. [Електронний ресурс]. URL: https://10guards.com/ua/blog/2024/10/18/cybersecurity-workforce-growth-stalls-and-skills-gaps-widen/.

155. М. Деркач. Чи готова Україна протистояти кіберзагрозам: стан галузі та перспективи. PaySpace Magazine. 30.01.2024. [Електронний ресурс]. URL: https://psm7.com/uk/world/gotova-li-ukraina-protivostoyat-kiberugrozam-sostoyanie-otrasli-i-perspektivy.html.

156. А. Михайлов. Дефіцит кіберспеціалістів. Чому українські фахівці на вагу золота. SPEKA. 008.06/2023. [Електронний ресурс]. URL: https://speka.media/deficit-kiberspecialistiv-comu-ukrayinski-faxivci-cinuyutsya-na-vagu-zolota-vzjr69?utm_source=chatgpt.com.

157. Закон України «Про зайнятість населення» від 5 липня 2012 року № 5067-VI. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/5067-17#Text.

158. Розпорядження Кабінету Міністрів України від 19 грудня 2023 р. № 1163 «Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України». [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text.

159. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року. Офіційний веб-портал Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. 16.02.2023. [Електронний ресурс]: URL: https://scpc.gov.ua/uk/articles/233?utm=.

160. CERT-UA минулого року опрацювала 4315 кіберінцидентів. Офіційний веб-портал Державної служби спеціального зв'язку та захисту інформації України. 08.01.2025. [Електронний ресурс]: URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

161. Звіті PE 733.549 «Війна Росії проти України: хронологія кібератак». Офіційний веб-портал Європейського парламенту. Жовень 2022 р. [Електронний ресурс]: URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf.

162. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

163. Молодь найкраще обізнана в кібербезпеці, але ризики недооцінюють усі: результати дослідження. Веб-сайт Info Sapiens. 14.06.2023. [Електронний ресурс]: URL: https://www.sapiens.com.ua/en/socpol-research-single-page?id=321.

164. Звіт про проміжне дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки, проведеного за підтримки Офісу Координатора допомоги США Європі та Євразії Державного департаменту Сполучених Штатів Америки. Травень 2023. [Електронний ресурс]: URL:

https://www.sapiens.com.ua/publications/socpol-research/321/promizhne-doslidzhennya-shhodo-informovanosti-pro-osnovni-aspekty-kiberbezpeky-1.pdf.

165. В Україні стартує інформаційно-освітня кампанія з підвищення рівня кібергігієни громадян. Офіційний веб-портал Ради національної безпеки і оборони України. 17.04.2024. [Електронний ресурс]: URL: https://www.rnbo.gov.ua/ua/Diialnist/6853.html.

166. Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

167. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/2657-12.

168. Закон України «Про електронні комунікації» від 16 грудня 2020 року № 1089-IX. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

169. Сучасні тренди кібербезпекової політики: висновки для України: Аналітична записка. Національний інститут стратегічних досліджень. 17.10.2010. [Електронний ресурс]: URL: https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini.

170. Розвиток кіберзахисту – невід'ємна складова цифровізації України. Офіційний веб-портал Міністерства цифрової трансформації України. 30.04.2021. [Електронний ресурс]: URL: https://thedigital.gov.ua/news/rozvitok-kiberzakhistu-nevidemna-skladova-tsifrovizatsii-ukraini.

171. М. Єрема, А. Борисеко. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. Веб-портал Liga:Zakon. 13.04.2022. [Електронний ресурс]: URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.

172. Кібербезпека бізнесу під час війни. Веб-сайт Мінфін. [Електронний ресурс]: URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny.

173. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. Вісник Національного університету «Львівська політехніка». Серія: "Юридичні науки". 2024. Том 11, № 1(41), С. 314-320. [Електронний ресурс]: DOI: https://doi.org/10.23939/law2024.41.314.

174. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

175. Указ Президента України «Про Національний координаційний центр кібербезпеки» від 7 червня 2016 року № 242. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text.

176. Попович Д. В., Бундз Н. Б., Іванків В. О. Проблеми та перспективи розвитку страхування кіберризиків на національному ринку. Молодий вчений. 2023. № 4 (116) с. 168 – 172. [Електронний ресурс]: DOI: https://doi.org/10.32839/2304-5809/2023-4-116-33.

177. Приказюк Н. В., Гуменюк Л. С. Дорожня карта впровадження кібер-страхування в Україні. INNOVATION AND SUSTAINABILITY. 2021. Том 1, № 1. С. 64-72. [Електронний ресурс]: DOI: https://doi.org/10.31649/ins.2021.1.64.72.

178. Закон України «Про страхування» від 18 листопада 2021 року № 1909-IX. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/1909-20#Text.

179. Закон України «Про електронну комерцію» від 3 вересня 2015 року № 675-VIII. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/675-19#Text.

180. Закон України «Про захист прав споживачів» від 12 травня 1991 року № 1023-XII. Відомості Верховної Ради України. 1991. № 30. Ст. 379. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/1023-12#Text.

181. С. Бабік. Якою насправді є кібербезпека в Україні. А чи є взагалі? Думка експерта. Веб-сайт ICTV. 18.01.2021. [Електронний ресурс]: URL:

https://ranok.ictv.ua/ua/2021/01/18/yakoyu-naspravdi-ye-kiberbezpeka-v-ukrayini-a-chi-ye-vzagali-dumka-eksperta/.

182. Роль кібербезпеки в бізнесі та перші кроки для захисту будь-якої компанії. Веб-сайт Антикризовий медіа-центр. 09.02.2024. [Електронний ресурс]: URL: https://acmc.ua/rol-kiberbezpeky-v-biznesi-ta-pershi-kroky-dlya-zahystu-bud-yakoyi-kompaniyi/.

183. 10 принципів кібербезпеки бізнесу. Веб-сайт delo.ua. 31.10.2023. [Електронний ресурс]: URL: https://delo.ua/telecom/10-principiv-kiberbezpeki-dlya-biznesiv-425633/.

184. Проблеми та перспективи захисту персональних даних в Україні. Веб-сайт BSO Privacy Group. 05.02.2021. [Електронний ресурс]: URL: https://bsoprivacygroup.com/data-ptotection-in-ukraine/.

185. В. Фісун. Проблеми захисту персональних даних: досвід України та інших країн. Юридична Газета online. 2020. № 10 (716). [Електронний ресурс]: URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html.

186. Постанова Верховного Суду в від 19 вересня 2018 року в справі № 806/3265/17 (Пз/9901/2/18). [Електронний ресурс]: URL: https://reyestr.court.gov.ua/Review/76822787.

187. Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Електронний ресурс]: URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

188. Закон України «Про розвиток та державну підтримку малого і середнього підприємництва в Україні» від 22 березня 2012 року № 4618-VI. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/4618-17#Text.

189. Закон України «Про державну підтримку сільського господарства України» від 24 червня 2004 року № 1877-IV. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/1877-15#Text.

190. А. Нікітенко. Кібергігієна: сучасний тренд чи комплексний підхід до розбудови системи національної кібербезпеки? Веб-портал Національний кластер кібербезпеки. 09.06.2023. [Електронний ресурс] URL: https://cybersecuritycluster.org.ua/blog/kibergigiyena-suchasnyj-trend-chy-kompleksnyj-pidhid-do-rozbudovy-systemy-naczionalnoyi-kiberbezpeky/.

191. Місяць кібербезпеки: поради від експерта про безпечну поведінку в мережі та новий навчальний курс від Google. Офіційний веб-портал Міністерства цифрової трансформації України. 05.10.2023. [Електронний ресурс]: URL: https://thedigital.gov.ua/news/misyats-kiberbezpeki-poradi-vid-eksperta-pro-bezpechnu-povedinku-v-merezhi-ta-noviy-navchalniy-kurs-vid-google.

192. Інтернет-безпека телефона: як запобігти інфікуванню пристроїв. Офіційний веб-портал ESET. 08.10.2019. [Електронний ресурс]: URL: https://www.eset.com/ua/about/newsroom/blog/smartphone-security/internet-bezopasnost-telefona-kolichestvo-vredonosnykh-programm-dlya-mobilnykh-devaysov-vozroslo/.

193. КІБЕРБЕЗПЕКА. АСПЕКТ 2: МОБІЛЬНІ ТЕЛЕФОНИ. Офіційний веб-портал Міністерства оборони України. [Електронний ресурс]: URL: https://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-2-mobilni-telefoni.html.

194. Закон України «Про державну службу» від 10 грудня 2015 року № 889-VIII. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/889-19#Text.

195. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

196. Постанова Кабінету Міністрів України від 29 грудня 2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту». [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#n9.

197. Закон України «Про технічні регламенти та оцінку відповідності» від 15 січня 2015 року № 124-VIII. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/124-19#Text.

198. Ю. Далецька. Причиною кібератаки на держреєстри міг бути фішинг або підкуп працівників. Бізнес Цензор. 23.12.2024. [Електронний ресурс]: URL: https://biz.censor.net/n3526565.

199. Ю. Далецька. Державні реєстри Мін'юсту не працюють через кібератаку. Бізнес Цензор. 20.12.2024. [Електронний ресурс]: URL: https://biz.censor.net/n3526099.

200. Огляді подій в сфері кібербезпеки, лютий 2024. CYBER DIGEST. Офіційний веб-сайт Ради безпеки і оборони України. [Електронний ресурс]: URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest%202_2024/Cyber%20digest_Fab_2024_UA.pdf.

201. Огляді подій в сфері кібербезпеки, січень 2024. CYBER DIGEST. Офіційний веб-сайт Ради безпеки і оборони України. [Електронний ресурс]: URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf.

202. Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 року № 2135-XII. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

203. Gu X. et al. Review of Privacy Enhancement Methods for Federated Learning in Healthcare Systems, International Journal of Environmental Research and Public Health. 2023. Vol. 20. No. 15. Art. 6539 p. [Електронний ресурс]: DOI: https://doi.org/10.3390/ijerph20156539.

204. Г. Терещенко, І. Кириченко. Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. Innovative technologies and scientific solutions for industries. 2024. No. 1 (27). pp. 164 – 178. [Електронний ресурс]: DOI: https://doi.org/10.30837/ITSSI.2024.27.164.

205. С. О. Бойчук. Роль блокчейн в системі фінансових інновацій. Ефективна економіка. 2023. № 12. [Електронний ресурс]: DOI: http://doi.org/10.32702/2307-2105.2023.12.70.

206. Мутерко Г. М., Кучерівська С. С., Яцко М. В., Малець В. В. Впровадження блокчейн-технологій в економіці України: переваги та виклики. Академічні візії. Випуск 26/2023. с. 1 – 13. [Електронний ресурс]: DOI: http://dx.doi.org/10.5281/zenodo.10389773.

207. Закон України «Про віртуальні активи» від 17 лютого 2022 року № 2074-IX. [Електронний ресурс]: URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.

208. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 6 грудня 2019 року № 361-IX. Офіційний веб-портал Верховної Ради України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text.

209. Тєтєвін М.С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. Науковий вісник Ужгородського Національного Університету. 2024. Серія ПРАВО. Випуск 82: частина 3. с. 263 – 266. [Електронний ресурс]. DOI: https://doi.org/10.24144/2307-3322.2024.82.3.41.

210. Мужанова Т. М., Легомінова С. В., Щавінський Ю. В., Якименко Ю. М., Нестеренко Г. П. Основні підходи й напрями розвитку політики кібербезпеки Європейського Союзу. Кібербезпека: освіта, наука, техніка. 2024. № 4 (24). с. 133 – 149. [Електронний ресурс]. DOI: https://doi.org/10.28925/2663-4023.2024.24.133149.

211. К. Корсун. Щодо можливостей співпраці з НАТО у сфері кібер-безпеки та захисту критичної інфраструктури у кібер сфері. Українська призма. 15.12.2021. [Електронний ресурс]. URL: https://prismua.org/nato5/.

212. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text.

213. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України. Аналітична доповідь. Націо нальний інститут стратегічних досліджень. Київ. 2018. 84 с. [Електронний ресурс]. URL: https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf.

214. Ю. Шипілова. Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем в Україні, 2019. 40 с. [Електронний ресурс]. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf.

215. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. Інформація і право. № 1 (20). 2017. с. 104 – 111. [Електронний ресурс]. URL: https://ippi.org.ua/sites/default/files/13_3.pdf.

216. Резолюція A/RES/57/239 Генеральної Асамблеї Організації Об’єднаних Націй «Створення глобальної культури кібербезпеки» від 20 грудня 2002 року. [Електронний ресурс]. URL: https://docs.un.org/en/A/RES/57/239.

217. An overview of Russia’s cyberattack activity in Ukraine. Special Report: Ukraine. Digital Security Unit. Microsoft Corporation. April 27, 2022. 20 с. [Електронний ресурс]. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

218. A. Greenberg. The Case for War Crimes Charges Against Russia’s Sandworm Hackers. Веб-портал WIRED. May 12, 2022. [Електронний ресурс]. URL: https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/ю

219. *L. Freeman, A. Ghahremani, S. Lombardo.* The Gravity of Russia's Cyberwar against Ukraine. Веб-портал OpinioJuris. 19.04.2023. [Електронний ресурс]. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russias-cyberwar-against-ukraine/.

220. Elements of Crimes. Офіційний веб-портал Міжнародного кримінального суду. [Електронний ресурс]. URL: https://www.icc-cpi.int/sites/default/files/Publications/Elements-of-Crimes.pdf.

221. Політика відбору та пріоритетності справ Офісу прокурора Міжнародного кримінального суду від 15 вересня 2016 року. Офіційний веб-портал Міжнародного кримінального суду. [Електронний ресурс]. URL: https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf.

222. S. Caltagirone. Industrial cyber attacks: a humanitarian crisis in the making. Humanitarian Law & Policy. December 3, 2019. [Електронний ресурс]. URL: https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/.

223. N. Brubaker, K. Lunden, K. Proska, M. Umair, D. Kapellmann Zafra, C. Hildebrandt, R. Caldwell. INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. April 13, 2022. [Електронний ресурс]. URL: https://cloud.google.com/blog/topics/threat-intelligence/incontroller-state-sponsored-ics-tool/.

224. L. Gisel, L. Olejnik. The potential human cost of cyber operations. Report. ICRC Expert Meeting. 14-16 November 2018. Geneva. [Електронний ресурс]. URL: https://shop.icrc.org/the-potential-human-cost-of-cyber-operations-pdf-en.html.

225. Обвинувальний висновок від 15 жовтня 2020 року в кримінальній справі № 20-316. Офіційний веб-сайт Міністерства юстиції Сполучених Штатів Америки. [Електронний ресурс]. URL: https://www.justice.gov/archives/opa/press-release/file/1328521/dl?inline=.

226. Karim A. A. Khan. Technology Will Not Exceed Our Humanity. Digital Front Lines. [Електронний ресурс]. URL: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/.

227. Schmitt M. N. Conduct of hostilities. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. 2017. с. 401-511. [Електронний ресурс]. URL: https://www.cambridge.org/core/books/abs/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/conduct-of-hostilities/61BE8A4936F4C8C0EA53F7CB999F58B4.

228. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8 - 9 July 2016. Офіційний веб-сайт НАТО. [Електронний ресурс]. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

229. Shannon van Sant. Kyiv argues Russian cyberattacks could be war crimes. Вебпортал Politico. 09.01.2023. [Електронний ресурс]. URL: https://www.politico.eu/article/victor-zhora-ukraine-russia-cyberattack-infrastructure-war-crime/.

230. International Humanitarian Law and Cyber Operations during Armed Conflicts. ICRC position paper. November 2019. Офіційний веб-сайт Міжнародного Товариства Червоного Хреста. [Електронний ресурс]. URL: https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.

231. The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare. August 2021. [Електронний ресурс]. URL: https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf.

232. Standard by International Organization for Standardization/International Electrotechnical Commission ISO/IEC 27032:2023 Cybersecurity - Guidelines for Internet security. 06.01.2023. [Електронний ресурс]. URL: https://store.accuristech.com/standards/iso-iec-27032-2023?product_id=2568394&utm_source=google&utm_medium=cpc&utm_campaign=Omni%20|%20Google%20Ads%20|%20ACC-

E%20|%20Top%20|%20Top%20|%20Non-Brand%20(Various%20Standards)%20|%20global%20-%20Dynamic&utm_content=Dynamic%20IEC%20Products&utm_ad=725894111403&utm_term=&matchtype=&device=c&GeoLoc=21580&placement=&network=g&campaign_id=22035107454&adset_id=172916797192&ad_id=725894111403&utm_term=&utm_campaign=Omni+%7C+Google+Ads+%7C+ACC-E+%7C+Non-Brand+(Various+Standards)+%7C+US+-+Dynamic+Ads&utm_source=adwords&utm_medium=ppc&hsa_acc=4039732030&hsa_cam=22035107454&hsa_grp=172916797192&hsa_ad=725894111403&hsa_src=g&hsa_tgt=dsa-2387125952638&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKCAiAwaG9BhAREiwAdhv6Y-iTh02OL1Xy_bKiDs29KC9294Ae2t0NIU_-jtMgSXnoH8fd27foHhoCb-wQAvD_BwE.

233. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

А. Статті в наукових виданнях України, включених до переліку наукових фахових видань України

1. В. Поліщук. Кіберзлочини та кібербезпека: боротьба з комп'ютерними злочинами і кібератаками. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2023. № 3(66). С. 44 – 47. DOI: https://doi.org/10.32689/2522-4603.2023.3.7.

2. **Поліщук В. П.**, Панасевич Л. А. Міжнародне право і кібербезпека: визначення правового статусу кібератак та кібервійськових операцій. *Юридичний науковий електронний журнал*. 2024. № 2. С. 503 – 506. DOI: https://doi.org/10.32782/2524-0374/2024-2/124.

Б. Статті в періодичних наукових виданнях, проіндексованих у наукометричній базі даних Scopus

3. **V. Polishchuk**, V. Yurakh, O. Kravchenko, W. Warawa, I. Kulchii. Legal Regulation of Cybersecurity and Privacy on the Internet as SDG's. *Journal of Lifestyle and SDGs Review*. 2024. v. 4, n. 1. C. 01 – 22. DOI: https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01666.

4. V. Ievdokymov, A. Frikel, **V. Polishchuk**, S. Savchuk, I. Klimova. Cybercrime and Information Protection in the Field of State Security: Current Threats

and Measures for their Prevention. *Economic Affairs*. 2024. Vol. 69, Issue 1 Special. pp. 61 – 69. DOI: https://doi.org/10.46852/0424-2513.1.2024.8.

5. **V. Polishchuk**, N. Fedirko, D. Grytsyshen, K. Ohdanskyi, V. Kotkovskyy. Stability of financial institutions under the influence of cyber threats. *Edelweiss Applied Science and Technology*. 2024. v. 8, n. 6. C. 2501 – 2509. DOI: https://doi.org/10.55214/25768484.v8i6.2498.

Праці, які додатково відображають наукові результати дисертації (Матеріали наукових конференцій)

6. В. П. Поліщук. Визначення правового статусу кібератак та кібервійськових операцій. *Проблеми модернізації України. Випуск 17. Матеріали IX Міжнародної науково-практичної конференції «Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності».* (м. Київ, 23-24 травня 2024 р.). Київ, 2024. С. 373 – 375. URL: https://research.maup.com.ua/assets/files/conferency/17-problemi-modernizacii.pdf.

7. Поліщук В. Права людини в умовах кіберпростору: баланси між безпекою та приватністю. *Міжнародна науково-практична конференція «Інновації та їхній вплив на економіку та суспільство».* (м. Суми, 25 жовтня 2024 р.). Суми, 2024. С. 136 – 138. URL: https://researcheurope.org/wp-content/uploads/2024/11/re-25.10.24.pdf.

Додаток Б

057889
Приватне акціонерне товариство
«Вищий навчальний заклад
«МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ
ПЕРСОНАЛОМ»

Україна, 03039, Київ-39, вул. Фрометівська, 2,
Тел. +38 (044) 490-95-00, maup.com.ua
e-mail: iapm@iapm.edu.ua

МАУП

The Private Joint-Stock Company
«Higher Education Institution
«Interregional
Academy
of Personnel Management»

2, Frometivs`ka Str., 03039 Kyiv, Ukraine,
Tel. +38 (044) 490-95-00, maup.com.ua
e-mail: iapm@iapm.edu.ua

«31» жовтня 2024 № 4528/1

Довідка
про впровадження результатів дисертаційного дослідження
здобувача ступеня доктора філософії
за спеціальністю 081 – Право
Поліщука Володимира Павловича
на тему «Адміністративно-правові засади забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови Україні»

Дослідження Поліщука Володимира Павловича на тему «Адміністративно-правові засади забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови Україні» виконане в рамках наукової теми НДР Міжрегіональної Академії управління персоналом «Дослідження теоретико-методологічних основ розвитку української державності в контексті світових модернізаційних процесів формування національних громадянських суспільств: політичний, юридичний, економічний, соціальний, психологічний та управлінський аспекти» (номер державної реєстрації – 0119U100492). Дисертація відповідає основним науковим напрямкам діяльності Міжрегіональної Академії управління персоналом з тем «Актуальні питання державотворення та захисту прав людини в Україні» (номер державної реєстрації – 0123U104042) та «Актуальні питання юридичної науки та практики» (номер державної реєстрації – 0123U104485).

Дисертація Поліщука В. П. є одним з перших в Україні комплексним дослідженням, спрямованим на аналіз адміністративно-правового забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України. В результаті дослідження сформульовано нові науково-обґрунтовані теоретичні положення та пропозиції щодо вдосконалення національного законодавства, яке здійснює адміністративно-правове регулювання кібербезпеки.

Тези, положення та висновки, наведені у дисертаційному дослідженні «Адміністративно-правові засади забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови Україні» Поліщука В. П. можуть

використовуватись у навчальному процесі закладів вищої освіти при викладанні, підготовці до лекційних та практичних занять, розробці спеціалізованих навчальних курсів, написанні навчальних посібників та науково-дослідницькій роботі студентів спеціальностей «Право», «Кібербезпека та захист інформації», «Фінанси, банківська справа, страхування та фондовий ринок» і «Публічне управління та адміністрування».

Ректор,
доктор юридичних наук,
професор **К. В. Муравйов**

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

УПРАВЛІННЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ У ЛЬВІВСЬКІЙ ОБЛАСТІ
(Управління Держспецзв'язку у Львівській області)

вул. Вітовського, 55, м. Львів, Україна, 79011, тел./факс: (032) 298-63-18,
e-mail: lviv@cip.gov.ua, код згідно з ЄДРПОУ 34814089

31.12.2024 № 37/04-1612 **На №** _____ **від** _____

ДОВІДКА
про результати дисертаційної роботи Поліщука Володимира Павловича на тему «Адміністративно-правові засади забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України»

Дисертаційна робота Поліщука В.П. забезпечує комплексне дослідження адміністративно-правового забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України, організаційно-адміністративних засад системи забезпечення кібербезпеки та кіберзахисту з урахуванням сучасної нормативної бази в цій сфері.

Запропонована авторська методика впровадження механізмів захисту об'єктів кіберзахисту в період воєнного стану та повоєнного відновлення України є актуальною та може бути використана у вигляді відповідної програми з удосконалення існуючих механізмів захисту об'єктів кіберзахисту.

Результати дисертаційної роботи можуть сприяти вдосконаленню застосування положень законодавства України з питань адміністративно-правового забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України, а також використовуватись для внесення змін до нормативно-правових актів, щодо забезпечення кібербезпеки в Україні.

Начальник Управління Сергій ЖУК

ПУМБ

ДОВІДКА
про впровадження результатів
дисертаційного дослідження Поліщука Володимира Павловича
на тему «Адміністративно-правові засади забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України»

Наукове дослідження, проведене Поліщуком Володимиром Павловичем, є одним з перших в державі комплексним вивченням адміністративно- правових засад забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України.

Дисертантом проведено вивчення та глибокий науковий аналіз на згадану вище тему, вивчено позитивні та негативні аспекти сучасного стану адміністративно-правового забезпечення кібербезпеки, розглянуто концептуальні основи її формування та розвитку правового регулювання.

Одержані в процесі наукового дослідження результати дають підстави для висновків, які мають як теоретичне, так і практичне значення в роботі фінансових інституцій та інших суб'єктів приватного права, чия діяльність тісно пов'язана з функціонуванням в кіберпросторі.

Враховуючи наведене вище, слід зазначити, що матеріали дисертаційної роботи Поліщука В.П. є актуальними, мають вагоме теоретичне і практичне значення в діяльності, спрямованій на забезпечення правових основ функціонування глобальної кібербезпеки, зокрема в частині діяльності суб'єктів приватного права, спрямованій на забезпечення конфіденційності фінансових операцій, банківської таємниці та додержання інших конституційних прав і свобод громадян а також суб'єктів господарської діяльності.

Заступник директора РЦ у м. Львів Хода О.М.

23.12.2024 року

НАЦІОНАЛЬНА СПІЛКА ПРИВАТНИХ ВИКОНАВЦІВ
44052917 м.Київ

ДОВІДКА

про впровадження результатів дисертаційного дослідження Поліщука Володимира Павловича на тему «Адміністративно-правові засади забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України»

Наукове дослідження, проведене Поліщуком Володимиром Павловичем, є одним з перших в державі комплексним вивченням адміністративно- правових засад забезпечення кібербезпеки в умовах воєнного стану та повоєнної відбудови України.

Дисертантом проведено вивчення та глибокий науковий аналіз на згадану вище тему, вивчено позитивні та негативні аспекти сучасного стану адміністративно-правового забезпечення кібербезпеки, розглянуто концептуальні основи її формування та розвитку правового регулювання.

Одержані в процесі наукового дослідження результати дають підстави для висновків, які мають як теоретичне, так і практичне значення в роботі як державних органів, зокрема, правоохоронних структур, так і суб'єктів приватного права, чия діяльність тісно пов'язана з функціонуванням в кіберпросторі.

Враховуючи наведене вище, слід зазначити, що матеріали дисертаційної роботи Поліщука В.П. є актуальними, мають вагоме теоретичне і практичне значення в діяльності, спрямованій на забезпечення правових основ функціонування глобальної кібербезпеки, зокрема в частині діяльності суб'єктів приватного права, спрямованій на забезпечення конфіденційності та додержання конституційних прав і свобод громадян і суб'єктів господарської діяльності.

Голова
Всеукраїнської професійної спілки
«Національна спілка приватних виконавців»
доктор юридичних наук **Сергій ЛИСЕНКО**

Додаток В

ПРОЕКТ

вноситься _____

Закон України

Про внесення змін до деяких законодавчих актів України щодо вдосконалення деяких аспектів забезпечення кібербезпеки України

Верховна Рада України **п о с т а н о в л я є :**

І. Внести зміни до таких законодавчих актів України:

1. У статті 361 Кримінального кодексу України (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131 із наступними змінами):

1) частину другу доповнити новим абзацом такого змісту:

«Ті самі дії, вчинені через анонімні мережі або VPN, караються позбавленням волі строком від 5 до 10 років із конфіскацією обладнання та забороною займати певні посади строком до 5 років.»;

2) примітку доповнити новою частиною такого змісту:

«2. Значною шкодою у статтях 361-363[1] вважається шкода, незалежно від її розміру, яка завдана об’єкту критичної інфраструктури або державній установі.».

2. У Законі України «Про захист прав споживачів» (Відомості Верховної Ради УРСР (ВВР), 1991, № 30, ст. 379 із наступними змінами):

1) статтю 15 доповнити новою частиною такого змісту:

«10. Виробники зобов’язані надавати споживачам інформацію про:

1) можливі ризики використання пристроїв Інтернету речей (IoT);

2) необхідність регулярного оновлення програмного забезпечення пристроїв Інтернету речей (IoT);

3) рекомендовані налаштування щодо забезпечення кібербезпеки при використанні пристроїв Інтернету речей (IoT).»;

2) статтю 17 доповнити новою частиною такого змісту:

«6. Кожен споживач має право на компенсацію збитків, спричинених витоком персональних даних або шахрайством, за рахунок кіберстрахового полісу відповідного суб’єкта господарювання.».

3. Частину першу статті 8 Закону України «Про оперативно-розшукову діяльність» (Відомості Верховної Ради України (ВВР), 1992, № 22, ст. 303 із наступними змінами) доповнити новим підпунктом такого змісту:

«22) використовувати спеціалізоване програмне забезпечення для відстеження та аналізу трафіку з метою ідентифікації джерел кібератак.».

4. Частину першу статті 6 Закону України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650 із наступними змінами) доповнити новим абзацом шостим такого змісту:

«обов’язком Інтернет-провайдерів розміщувати рекомендації щодо безпечного користування інтернетом на своїх веб-сайтах, а також надсилати клієнтам електронні листи з порадами з кібербезпеки;».

5. Статтю 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України (ВВР), 1994, № 31, ст. 286 із наступними змінами) доповнити новими частинами такого змісту:

«Суб’єкти критичної інфраструктури зобов’язані застосовувати багатофакторну автентифікацію, що включає комбінацію пароля та біометричних даних, для доступу до інформаційно-телекомунікаційних систем, які забезпечують функціонування таких об’єктів.

Користувачі пристроїв Інтернету речей (IoT) зобов’язані забезпечувати регулярне оновлення їх програмного забезпечення відповідно до рекомендацій виробника для усунення вразливостей.

Провайдери хмарних послуг зобов’язані:

1) використовувати системи шифрування даних під час їх зберігання та передачі;

2) забезпечувати можливість багатофакторно автентифікації для доступу до даних;

3) проводити регулярний аудит щодо стану кібербезпеки.

Провайдери хмарних сервісів, що працюють з державними установами, повинні кожні два роки проходити сертифікацію на відповідність стандартам кібербезпеки (ISO/IEC 27017, ISO/IEC 27018).

Усі державні установи та об’єкти критичної інфраструктури зобов’язані забезпечувати регулярне резервне копіювання даних на захищені сервери. Копії повинні зберігатися щонайменше на трьох фізично розподілених носіях.

Підприємства, які обробляють персональні або конфіденційні дані, зобов’язані використовувати сертифіковані системи резервного копіювання з можливістю шифрування даних.

Провайдери інтернет-послуг зобов’язані моніторити використання VPN, анонімних проксі-серверів та виявляти підозрілу активність, що може свідчити про підготовку або здійснення кібератаки.

У системах кібербезпеки державних органів та суб’єктів критичної інфраструктури впроваджуються алгоритми штучного інтелекту для аналізу мережевого трафіку, виявлення аномалій та визначення ймовірних джерел атак.

Усі суб’єкти, які використовують блокчейн для зберігання конфіденційних даних, зобов’язані:

1) використовувати сертифіковані апаратні засоби для зберігання приватних ключів;

2) забезпечувати резервне копіювання ключів у зашифрованому вигляді;

3) дотримуватися міжнародних стандартів кібербезпеки при роботі з блокчейн-системами.».

6. Статтю 2^1 Закону України «Про державну підтримку сільського господарства України» (Відомості Верховної Ради України (ВВР), 2004, № 49, ст. 527 із наступними змінами) доповнити новою частиною такого змісту:

«2^1.7. Державна підтримка сільського господарства включає компенсацію витрат на впровадження кіберзахисних технологій, проведення аудитів кібербезпеки та навчання персоналу.».

7. У Законі України «Про захист персональних даних» (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481):

1) доповнити статтю 6 новими частинами такого змісту:

«11. Суб'єкти, що обробляють персональні дані, зобов'язані надавати користувачам рекомендації з кібергігієни, які сприяють захисту персональної інформації.

12. Суб'єкти господарювання, що обробляють персональні дані, зобов'язані застосовувати багатофакторну автентифікацію для користувачів і адміністраторів всіх інформаційних систем, які використовуються для обробки та зберігання даних клієнтів.

13. Мобільні додатки, що обробляють персональні дані користувачів, зобов'язані:

1) забезпечувати шифрування даних;

2) застосовувати механізми багатофакторної автентифікації;

3) регулярно проходити аудит кібербезпеки.

Державні установи можуть використовувати лише мобільні додатки, які пройшли перевірку на відповідність стандартам кібербезпеки, затвердженим Держспецзв'язку.

14. Усі державні реєстри, які зберігають персональні дані або критичну інформацію, повинні використовувати блокчейн-системи, що відповідають стандартам безпеки ISO 27001 та NIST SP 800-57.»;

2) статтю 12 доповнити новою частиною такого змісту:

«3. Підприємства, що обробляють персональні дані, зобов'язані забезпечити проходження своїми працівниками щорічних тренінгів із кібергігієни.»;

3) статтю 24 доповнити новою частиною такого змісту:

«5. Провайдери хмарних сервісів зобов’язані повідомляти користувачів про витоки персональних даних не пізніше 48 годин після виявлення інциденту.»;

4) доповнити статтю 28 новими частинами такого змісту:

«2. У разі витоку персональних даних підприємства зобов’язані:

повідомити постраждалих осіб протягом 72 годин після виявлення витоку;

сплатити штраф у розмірі 5% від річного доходу компанії або до 5 мільйонів гривень (залежно від того, яка сума більша).

3. Компанії зобов’язані повідомляти про інциденти витоку даних до державного органу кібербезпеки протягом 24 годин після їх виявлення.

За невиконання цієї вимоги накладається штраф у розмірі до 1 мільйона гривень.».

8. У Законі України «Про державно-приватне партнерство» (Відомості Верховної Ради України (ВВР), 2010, № 40, ст. 524 із наступними змінами):

1) частину першу статті 4 доповнити новим абзацом такого змісту:

«кібербезпека;»;

2) частину першу статті 18 доповнити новим абзацом такого змісту:

«Проекти з кібербезпеки можуть фінансуватися на умовах державно-приватного партнерства з можливістю податкових пільг для приватного сектора.».

9. Частину другу статті 16 Закону України «Про розвиток та державну підтримку малого і середнього підприємництва в Україні» (Відомості Верховної Ради України (ВВР), 2013, № 3, ст. 23 із наступними змінами) доповнити новим підпунктом такого змісту:

«9) надання грантів для проведення аудитів кібербезпеки, навчання співробітників та впровадження інноваційних технологій захисту даних.».

10. Статтю 15 Закону України «Про зайнятість населення» (Відомості Верховної Ради (ВВР), 2013, № 24, ст. 243 із наступними змінами) доповнити новою частиною такого змісту:

«Держава компенсує витрати роботодавців на перепідготовку працівників у сфері кібербезпеки в рамках державних програм зайнятості.».

11. Статтю 16 Закону України «Про технічні регламенти та оцінку відповідності» (Відомості Верховної Ради (ВВР), 2015, № 14, ст. 96 із наступними змінами) доповнити новою частиною такого змісту:

«3. Всі пристрої Інтернету речей (IoT), які виробляються або імпортуються в Україну, повинні відповідати вимогам кібербезпеки, включаючи:

1) наявність можливості змінювати паролі за замовчуванням;

2) підтримку багатофакторної автентифікації;

3) шифрування даних під час передачі.

Сертифікація пристроїв Інтернету речей (IoT) на відповідність міжнародним стандартам кібербезпеки, включаючи ISO/IEC 27001 та ETSI EN 303 645, є обов’язковою умовою для їх реалізації в Україні.

Державні установи можуть використовувати лише сертифіковані пристрої Інтернету речей (IoT), які відповідають стандартам кібербезпеки. Контроль за виконанням цієї вимоги покладається на Держспецзв’язку.».

12. Статтю 14 Закону України «Про електронну комерцію» (Відомості Верховної Ради (ВВР), 2015, № 45, ст. 410 із наступними змінами) доповнити новими частинами такого змісту:

«5. Інтернет-магазини зобов’язані забезпечувати страхування ризиків, пов’язаних із витоком даних клієнтів, шляхом укладання договорів кіберстрахування.

6. Власники платформ електронної комерції зобов’язані проводити регулярний аудит кібербезпеки не рідше одного разу на рік, який поміж іншого має включати перевірку відповідності стандартам захисту даних ISO 27001, для забезпечення захисту даних клієнтів і безперебійної роботи платформ.».

13. Частину п’яту статті 48 Закону України «Про державну службу» (Відомості Верховної Ради (ВВР), 2016, № 4, ст. 43 із наступними змінами) доповнити новими абзацами такого змісту:

«Професійного навчання державного службовця має обов’язково включати навчання основ кібергігієни, щодо:

використання багатофакторної автентифікації;

розпізнавання фішингових атак;

безпечну роботу з конфіденційною інформацією.».

14. У статті 4 Закону України «Про публічні закупівлі» (Відомості Верховної Ради (ВВР), 2016, № 9, ст. 89 із наступними змінами):

1) абзац п’ятий підпункту 5 частини другої викласти у такій новій редакції:

«спрощена закупівля – для замовників, визначених у пункті 4 частини першої статті 2 цього Закону, а також для всіх замовників коли закупівлі, пов’язані з модернізацією систем кібербезпеки, якщо вартість предмета закупівлі товару (товарів), послуги (послуг) менше ніж 1 мільйон гривень, а робіт – 5 мільйонів гривень;»;

2) доповнити новими частинами такого змісту:

«5. Усі постачальники, які беруть участь у державних закупівлях, повинні мати діючий кіберстраховий поліс, що покриває ризики, пов’язані з обробкою державних даних.

6. При здійсненні публічних закупівель пристроїв Інтернету речей (IoT) замовник зобов’язаний враховувати відповідність продукції стандартам кібербезпеки, підтвердженим сертифікатом відповідності.

7. При здійсненні публічних закупівель послуг на користування сервісами хмарних послуг замовники зобов’язані враховувати рівень кіберзахисту даних. Провайдери повинні надати сертифікати відповідності міжнародним стандартам кібербезпеки.

8. При здійсненні публічних закупівель програмного забезпечення або послуг хмарних сервісів замовники зобов’язані вимагати наявність функціоналу резервного копіювання даних.

9. При здійсненні публічних закупівель програмного забезпечення замовники зобов’язані вимагати наявність функціоналу для управління правами доступу та ведення аудиту.

10. Закупівля програмних рішень для державних установ та критичної інфраструктури повинна передбачати наявність у таких рішеннях засобів аналізу джерел атак, виявлення загроз та реагування на інциденти.».

15. Статтю 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (Відомості Верховної Ради України (ВВР), 2017, № 45, ст. 400 із наступними змінами) доповнити новою частиною такого змісту:

«5. Смарт-контракти, що використовуються для фінансових операцій або державних реєстрів, повинні мати сертифіковане аудиторське підтвердження від спеціалізованих кібербезпекових компаній, що підтверджує їх відповідність стандартам безпеки.».

16. У Законі України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради України (ВВР), 2017, № 45, ст. 403 із наступними змінами):

1) статтю 6 доповнити новою частиною такого змісту:

«6. Об’єкти аграрного сектору, що використовують інформаційні технології для управління виробництвом, зберігання даних та логістики, вважаються критично важливими для національної безпеки та підлягають обов’язковому кіберзахисту.

Інформаційні системи, які використовуються в агротехнологіях, управлінні агропідприємствами та логістиці продукції, підлягають обов’язковій сертифікації та кіберзахисту.

Центральний орган виконавчої влади, що забезпечує формування та реалізує державну аграрну політику, державну політику у сферах сільського господарства та з питань продовольчої безпеки держави здійснює оцінку ризиків кіберзагроз та розробку рекомендацій для впровадження сучасних кіберзахисних технологій у сільськогосподарському секторі.»;

2) у статті 8:

частину другу статті доповнити новими абзацами такого змісту:

«Державні установи зобов’язані використовувати лише сертифіковане програмне та апаратне забезпечення, яке відповідає вимогам національної безпеки. Використання продуктів, розроблених у країнах, що представляють геополітичну загрозу, забороняється.

Суб’єкти критичної інфраструктури зобов’язані впроваджувати системи управління кіберризиками відповідно до стандартів ISO/IEC 27001 та забезпечувати щорічний аудит ефективності цих систем.»;

доповнити новими частинами такого змісту:

«7. Єдина державна платформа для обміну інформацією про кіберзагрози забезпечує:

1) реєстрацію всіх кіберінцидентів державного рівня;

2) оперативне сповіщення про нові загрози;

3) інтеграцію з приватними ініціативами у сфері кібербезпеки.

8. Суб’єкти господарювання зобов’язані розробляти, затверджувати та впроваджувати політики кібербезпеки, що включають заходи з протидії кібератакам, навчання співробітників основам кібергігієни та впровадження сучасних засобів захисту інформації.

9. Програмне забезпечення, що використовується державними органами, підлягає обов’язковій періодичній перевірці на відповідність вимогам кібербезпеки, включаючи аналіз коду на наявність вразливостей та шкідливого функціоналу.

10. Суб’єкти критичної інфраструктури зобов’язані підключитися до національної системи моніторингу кіберзагроз для автоматичного виявлення джерел атак та аналізу підозрілої активності.

Державні установи та приватні компанії, що працюють із критичною інформаційною інфраструктурою, зобов’язані передавати дані про кіберінциденти та джерела атак до національної системи моніторингу кібербезпеки.»;

3) частину першу статті 9 доповнити новим підпунктом 10 такого змісту:

«10) здійснення постійного моніторингу стану кібербезпеки об’єктів критичної інфраструктури та надає обов’язкові рекомендації для усунення виявлених недоліків.»;

4) доповнити новою статтею 9^1 такого змісту:

«Стаття 9^1. Національний центр міжнародної координації з кібербезпеки

1. Завданнями Національного центру міжнародної координації з кібербезпеки є:

1) обмін інформацією про кіберзагрози та атаки з НАТО, ЄС та іншими міжнародними організаціями;

2) співпраця з Interpol та Europol щодо розслідування міжнародних кіберзлочинів;

3) спільно з міжнародними експертами розробка рекомендацій та стандартів кіберзахисту.

2. Національний центр міжнародної координації з кібербезпеки забезпечує:

1) взаємодію України з міжнародними організаціями, зокрема NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) та European Union Agency for Cybersecurity (ENISA);

2) участь у міжнародних кібернавчаннях та обмін досвідом з провідними країнами у сфері кіберзахисту;

3) підготовку фахівців у галузі кібербезпеки через міжнародні програми навчання.»;

5) статтю 11 доповнити новою частиною такого змісту:

«Державні органи, що відповідають за забезпечення кібербезпеки, повинні здійснювати постійний моніторинг кіберзагроз та вживати заходів для запобігання кіберінцидентам. Це включає використання технологій штучного інтелекту для виявлення та запобігання атакам у режимі реального часу.»;

6) статтю 13 доповнити новою частиною такого змісту:

«Держава зобов’язана забезпечувати фінансування заходів з кібербезпеки для захисту державних установ, критичної інфраструктури та державних інформаційних ресурсів.».

17. Статтю 31 Закону України «Про національну безпеку України» (Відомості Верховної Ради України (ВВР), 2018, № 31, ст. 241 із наступними змінами) доповнити новою частиною такого змісту:

«4. Україна бере участь у міжнародних кіберопераціях, спрямованих на протидію ворожим кіберзагрозам, у співпраці з країнами-партнерами НАТО та ЄС. Для цього створюється Національний центр кібероборони, який здійснює стратегічне планування, аналіз загроз та кібероперації оборонного характеру.»

18. Статтю 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» (Відомості Верховної Ради України (ВВР), 2020, № 25, ст. 171 із наступними змінами) доповнити новою частиною такого змісту:

«16. Банки та фінансові установи, які проводять операції з використанням блокчейн-технологій, зобов’язані:

1) використовувати автоматизовані системи аналізу транзакцій для виявлення підозрілих операцій;

2) запровадити механізми ідентифікації учасників транзакцій;

3) здійснювати аудит безпеки своїх блокчейн-платформ не рідше одного разу на рік.».

19. У Законі України «Про електронні комунікації» (Офіційний вісник України, 2021, № 6, ст. 306 із наступними змінами):

1) статтю 31 доповнити новими частинами такого змісту:

«3. Мобільні оператори зобов’язані надавати клієнтам SMS-сповіщення про актуальні кіберзагрози та рекомендації щодо їх уникнення.

4. Провайдери хмарних сервісів повинні здійснювати щорічний аудит кібербезпеки з поданням звіту до Держспецзв’язку.

5. Оператори електронних комунікаційних мереж повинні використовувати лише програмне забезпечення, яке пройшло сертифікацію на відповідність вимогам кібербезпеки.

6. Мобільні оператори повинні впроваджувати засоби захисту від перехоплення сигналу, несанкціонованого доступу до мережі та атак типу man-in-the-middle.»;

2) статтю 104 доповнити новою частиною такого змісту:

«10. Провайдери інтернет-послуг зобов’язані надавати користувачам рекомендації з кібергігієни, включаючи:

1) поради щодо налаштування захищених з’єднань;

2) попередження про актуальні кіберзагрози.».

20. У Законі України «Про критичну інфраструктуру» (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13 із наступними змінами):

1) частину четверту статті 21 доповнити новим підпунктом такого змісту:

«3[1]) щороку проводити тестування на проникнення, що має підтверджувати захищеність інформаційних систем від актуальних кіберзагроз;»;

2) статтю 22 доповнити новими частинами такого змісту:

«8. Об’єкти критичної інформаційної інфраструктури зобов’язані щорічно брати участь у навчаннях, організованих Національним координаційним

центром кібербезпеки, для перевірки готовності до реагування на кібератаки.

9. Об’єкти критичної інфраструктури зобов’язані укладати договори кіберстрахування з акредитованими страховиками для покриття таких можливих ризиків кібератак:

1) використання шкідливого програмного забезпечення;

2) DDoS-атаки;

3) заподіяння збитків через витік конфіденційної інформації.

10. Об’єкти критичної інфраструктури зобов’язані впроваджувати:

1) системи моніторингу стану пристроїв Інтернету речей (IoT);

2) захист від DDoS-атак через пристрої Інтернету речей (IoT);

3) регулярний аудит безпеки підключених пристроїв Інтернету речей (IoT).

11. Хмарні сервіси, що обробляють дані критичної інформаційної інфраструктури, підлягають обов’язковій сертифікації та моніторингу.».

21. Частину першу статті 4 Закону України «Про страхування» (Відомості Верховної Ради України (ВВР), 2023, № 12-13, ст. 28 із наступними змінами) доповнити новим підпунктом такого змісту:

«9^{1}) клас 9.1 – кіберстрахування, що покриває збитки від кіберзагроз, включаючи витрати на відновлення даних, забезпечення безперервності бізнесу та компенсацію витрат клієнтам;».

22. Статтю 9 Закону України «Про віртуальні активи» (Відомості Верховної Ради України (ВВР), 2023, № 15, ст. 51 із наступними змінами) доповнити новою частиною такого змісту:

«8. Блокчейн-платформи, що використовуються для фінансових операцій, повинні відповідати стандартам безпеки, визначеним Національним банком

України та Держспецзв’язку, зокрема, забезпечувати криптографічний захист даних, безпечне зберігання приватних ключів та захист від несанкціонованого доступу.».

II. Прикінцеві положення

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування.

ПОРІВНЯЛЬНА ТАБЛИЦЯ

до проекту Закон України

«Про внесення змін до деяких законодавчих актів України щодо вдосконалення деяких аспектів забезпечення кібербезпеки України»

Чинна редакція	Редакція з урахуванням запропонованих змін
Кримінальний кодекс України (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131 із наступними змінами)	
Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж … 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або	**Стаття 361.** Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж … 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або

обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. *норма відсутня* … **Примітка.** Значною шкодою у статтях 361-363[1] вважається така шкода, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян. *норма відсутня*	обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. Ті самі дії, вчинені через анонімні мережі або VPN, караються позбавленням волі строком від 5 до 10 років із конфіскацією обладнання та забороною займати певні посади строком до 5 років. … **Примітка.** 1. Значною шкодою у 361-363[1] вважається така шкода, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян. 2. Значною шкодою у статтях 361-363[1] вважається шкода, незалежно від її розміру, яка завдана об’єкту критичної інфраструктури або державній установі.
Закон України «Про захист прав споживачів» (Відомості Верховної Ради УРСР (ВВР), 1991, № 30, ст. 379 із наступними змінами)	
Стаття 15. Право споживача на інформацію про продукцію …	**Стаття 15.** Право споживача на інформацію про продукцію …

норма відсутня	10. Виробники зобов’язані надавати споживачам інформацію про: 1) можливі ризики використання пристроїв Інтернету речей (IoT); 2) необхідність регулярного оновлення програмного забезпечення пристроїв Інтернету речей (IoT); 3) рекомендовані налаштування щодо забезпечення кібербезпеки при використанні пристроїв Інтернету речей (IoT).
Стаття 17. Права споживача у сфері торговельного та інших видів обслуговування … *норма відсутня*	**Стаття 17.** Права споживача у сфері торговельного та інших видів обслуговування … 6. Кожен споживач має право на компенсацію збитків, спричинених витоком персональних даних або шахрайством, за рахунок кіберстрахового полісу відповідного суб’єкта господарювання.
Закон України «Про оперативно-розшукову діяльність» (Відомості Верховної Ради України (ВВР), 1992, № 22, ст. 303 із наступними змінами)	

Стаття 8. Права підрозділів, які здійснюють оперативно-розшукову діяльність Оперативним підрозділам для виконання завдань оперативно-розшукової діяльності за наявності передбачених статтею 6 цього Закону підстав надається право: **…** *норма відсутня*	**Стаття 8.** Права підрозділів, які здійснюють оперативно-розшукову діяльність Оперативним підрозділам для виконання завдань оперативно-розшукової діяльності за наявності передбачених статтею 6 цього Закону підстав надається право: **…** 22) використовувати спеціалізоване програмне забезпечення для відстеження та аналізу трафіку з метою ідентифікації джерел кібератак.
Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650 із наступними змінами)	
Стаття 6. Гарантії права на інформацію 1. Право на інформацію забезпечується: … *норма відсутня*	**Стаття 6.** Гарантії права на інформацію 1. Право на інформацію забезпечується: … обов’язком Інтернет-провайдерів розміщувати рекомендації щодо безпечного користування інтернетом на своїх веб-сайтах, а також надсилати клієнтам електронні листи з порадами з кібербезпеки;

	….
Закон України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України (ВВР), 1994, № 31, ст. 286 із наступними змінами)	
Стаття 9. Забезпечення захисту інформації в системі … *норма відсутня*	**Стаття 9.** Забезпечення захисту інформації в системі … Суб’єкти критичної інфраструктури зобов’язані застосовувати багатофакторну автентифікацію, що включає комбінацію пароля та біометричних даних, для доступу до інформаційно-телекомунікаційних систем, які забезпечують функціонування таких об’єктів. Користувачі пристроїв Інтернету речей (IoT) зобов’язані забезпечувати регулярне оновлення їх програмного забезпечення відповідно до рекомендацій виробника для усунення вразливостей. Провайдери хмарних послуг зобов’язані: 1) використовувати системи шифрування даних під час їх зберігання та передачі; 2) забезпечувати можливість багатофакторно автентифікації для доступу до даних;

	3) проводити регулярний аудит щодо стану кібербезпеки. Провайдери хмарних сервісів, що працюють з державними установами, повинні кожні два роки проходити сертифікацію на відповідність стандартам кібербезпеки (ISO/IEC 27017, ISO/IEC 27018). Усі державні установи та об’єкти критичної інфраструктури зобов’язані забезпечувати регулярне резервне копіювання даних на захищені сервери. Копії повинні зберігатися щонайменше на трьох фізично розподілених носіях. Підприємства, які обробляють персональні або конфіденційні дані, зобов’язані використовувати сертифіковані системи резервного копіювання з можливістю шифрування даних. Провайдери інтернет-послуг зобов’язані моніторити використання VPN, анонімних проксі-серверів та виявляти підозрілу активність, що може свідчити про підготовку або здійснення кібератаки.

	У системах кібербезпеки державних органів та суб'єктів критичної інфраструктури впроваджуються алгоритми штучного інтелекту для аналізу мережевого трафіку, виявлення аномалій та визначення ймовірних джерел атак. Усі суб'єкти, які використовують блокчейн для зберігання конфіденційних даних, зобов'язані: 1) використовувати сертифіковані апаратні засоби для зберігання приватних ключів; 2) забезпечувати резервне копіювання ключів у зашифрованому вигляді; 3) дотримуватися міжнародних стандартів кібербезпеки при роботі з блокчейн-системами.
Закон України «Про державну підтримку сільського господарства України» (Відомості Верховної Ради України (ВВР), 2004, № 49, ст. 527 із наступними змінами)	
Стаття 2[1]. Принципи підтримки сільського господарства України … *норма відсутня*	**Стаття 2[1]**. Принципи підтримки сільського господарства України … 2[1].7. Державна підтримка сільського господарства включає компенсацію витрат на впровадження

	кіберзахисних технологій, проведення аудитів кібербезпеки та навчання персоналу.
Закон України «Про захист персональних даних» (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481 із наступними змінами)	
Стаття 6. Загальні вимоги до обробки персональних даних … *норма відсутня*	**Стаття 6.** Загальні вимоги до обробки персональних даних … 11. Суб'єкти, що обробляють персональні дані, зобов'язані надавати користувачам рекомендації з кібергігієни, які сприяють захисту персональної інформації. 12. Суб'єкти господарювання, що обробляють персональні дані, зобов'язані застосовувати багатофакторну автентифікацію для користувачів і адміністраторів всіх інформаційних систем, які використовуються для обробки та зберігання даних клієнтів. 13. Мобільні додатки, що обробляють персональні дані користувачів, зобов'язані:

	1) забезпечувати шифрування даних; 2) застосовувати механізми багатофакторної автентифікації; 3) регулярно проходити аудит кібербезпеки. Державні установи можуть використовувати лише мобільні додатки, які пройшли перевірку на відповідність стандартам кібербезпеки, затвердженим Держспецзв'язку. 14. Усі державні реєстри, які зберігають персональні дані або критичну інформацію, повинні використовувати блокчейн-системи, що відповідають стандартам безпеки ISO 27001 та NIST SP 800-57.
Стаття 12. Збирання персональних даних … *норма відсутня*	**Стаття 12.** Збирання персональних даних … 3. Підприємства, що обробляють персональні дані, зобов'язані забезпечити проходження своїми працівниками щорічних тренінгів із кібергігієни.
Стаття 24. Забезпечення захисту персональних дан**их** …	**Стаття 24.** Забезпечення захисту персональних даних …

норма відсутня	5. Провайдери хмарних сервісів зобов’язані повідомляти користувачів про витоки персональних даних не пізніше 48 годин після виявлення інциденту.
Стаття 28. Відповідальність за порушення законодавства про захист персональних даних … *норма відсутня*	**Стаття 28.** Відповідальність за порушення законодавства про захист персональних даних … 2. У разі витоку персональних даних підприємства зобов’язані: повідомити постраждалих осіб протягом 72 годин після виявлення витоку; сплатити штраф у розмірі 5% від річного доходу компанії або до 5 мільйонів гривень (залежно від того, яка сума більша). 3. Компанії зобов’язані повідомляти про інциденти витоку даних до державного органу кібербезпеки протягом 24 годин після їх виявлення. За невиконання цієї вимоги накладається штраф у розмірі до 1 мільйона гривень.

Закон України «Про державно-приватне партнерство» (Відомості Верховної Ради України (ВВР), 2010, № 40, ст. 524 із наступними змінами)	
Стаття 4. Сфери застосування державно-приватного партнерства 1. Державно-приватне партнерство застосовується в таких сферах: … *норма відсутня* ...	**Стаття 4.** Сфери застосування державно-приватного партнерства 1. Державно-приватне партнерство застосовується в таких сферах: … кібербезпека; …
Стаття 18. Державна підтримка здійснення державно-приватного партнерства 1. Державна підтримка здійснення державно-приватного партнерства може надаватися: … *норма відсутня*	**Стаття 18.** Державна підтримка здійснення державно-приватного партнерства 1. Державна підтримка здійснення державно-приватного партнерства може надаватися: … Проекти з кібербезпеки можуть фінансуватися на умовах державно-приватного партнерства з можливістю податкових пільг для приватного сектора.
Закон України «Про розвиток та державну підтримку малого і середнього підприємництва в Україні» (Відомості Верховної Ради України (ВВР), 2013, № 3, ст. 23 із наступними змінами)	

Стаття 16. Фінансова державна підтримка суб'єктів малого і середнього підприємництва … 2. Основними видами фінансової державної підтримки є: … *норма відсутня*	**Стаття 16.** Фінансова державна підтримка суб'єктів малого і середнього підприємництва … 2. Основними видами фінансової державної підтримки є: … 9) надання грантів для проведення аудитів кібербезпеки, навчання співробітників та впровадження інноваційних технологій захисту даних.
Закон України «Про зайнятість населення» (Відомості Верховної Ради (ВВР), 2013, № 24, ст. 243 із наступними змінами)	
Стаття 15. Принципи та мета, основні напрями державної політики у сфері зайнятості населення … *норма відсутня*	**Стаття 15.** Принципи та мета, основні напрями державної політики у сфері зайнятості населення … 2. Держава компенсує витрати роботодавців на перепідготовку працівників у сфері кібербезпеки в рамках державних програм зайнятості.
Закон України «Про технічні регламенти та оцінку відповідності» (Відомості Верховної Ради (ВВР), 2015, № 14, ст. 96 із наступними змінами)	

Стаття 16. Особливості розроблення проектів технічних регламентів і процедур оцінки відповідності … *норма відсутня*	**Стаття 16.** Особливості розроблення проектів технічних регламентів і процедур оцінки відповідності … 3. Всі пристрої Інтернету речей (IoT), які виробляються або імпортуються в Україну, повинні відповідати вимогам кібербезпеки, включаючи: 1) наявність можливості змінювати паролі за замовчуванням; 2) підтримку багатофакторної автентифікації; 3) шифрування даних під час передачі. Сертифікація пристроїв Інтернету речей (IoT) на відповідність міжнародним стандартам кібербезпеки, включаючи ISO/IEC 27001 та ETSI EN 303 645, є обов’язковою умовою для їх реалізації в Україні. Державні установи можуть використовувати лише сертифіковані пристрої Інтернету речей (IoT), які відповідають стандартам кібербезпеки. Контроль за виконанням цієї вимоги покладається на Держспецзв’язку.

Закон України «Про електронну комерцію» (Відомості Верховної Ради (ВВР), 2015, № 45, ст. 410 із наступними змінами)	
Стаття 14. Захист персональних даних у сфері електронної комерції … *норма відсутня*	**Стаття 14.** Захист персональних даних у сфері електронної комерції … 5. Інтернет-магазини зобов'язані забезпечувати страхування ризиків, пов'язаних із витоком даних клієнтів, шляхом укладання договорів кіберстрахування. 6. Власники платформ електронної комерції зобов'язані проводити регулярний аудит кібербезпеки не рідше одного разу на рік, який поміж іншого має включати перевірку відповідності стандартам захисту даних ISO 27001, для забезпечення захисту даних клієнтів і безперебійної роботи платформ.
Закон України «Про державну службу» (Відомості Верховної Ради (ВВР), 2016, № 4, ст. 43 із наступними змінами)	
Стаття 48. Підвищення рівня професійної компетентності державних службовців …	**Стаття 48.** Підвищення рівня професійної компетентності державних службовців …

5. Підвищення рівня професійної компетентності державних службовців проводиться протягом проходження служби, а підвищення кваліфікації - не рідше одного разу на три роки. Необхідність професійного навчання державного службовця визначається його безпосереднім керівником та службою управління персоналом державного органу за результатами оцінювання службової діяльності. ...	5. Підвищення рівня професійної компетентності державних службовців проводиться протягом проходження служби, а підвищення кваліфікації - не рідше одного разу на три роки. Необхідність професійного навчання державного службовця визначається його безпосереднім керівником та службою управління персоналом державного органу за результатами оцінювання службової діяльності. ***Професійного навчання державного службовця має обов'язково включати навчання основ кібергігієни, щодо:*** ***використання багатофакторної автентифікації;*** ***розпізнавання фішингових атак;*** ***безпечну роботу з конфіденційною інформацією.*** …
Закон України «Про публічні закупівлі» (Відомості Верховної Ради (ВВР), 2016, № 9, ст. 89 із наступними змінами)	
Стаття 4. Планування закупівель та інші передумови здійснення закупівель	**Стаття 4.** Планування закупівель та інші передумови здійснення закупівель

…	…
2. У річному плані повинна міститися така інформація:	2. У річному плані повинна міститися така інформація:
…	…
5) вид закупівлі та орієнтовний початок проведення:	5) вид закупівлі та орієнтовний початок проведення:
…	…
спрощена закупівля - для замовників, визначених у пункті 4 частини першої статті 2 цього Закону, якщо вартість предмета закупівлі товару (товарів), послуги (послуг) менше ніж 1 мільйон гривень, а робіт - 5 мільйонів гривень;	спрощена закупівля – для замовників, визначених у пункті 4 частини першої статті 2 цього Закону, ***а також для всіх замовників коли закупівлі, пов'язані з модернізацією систем кібербезпеки,*** якщо вартість предмета закупівлі товару (товарів), послуги (послуг) менше ніж 1 мільйон гривень, а робіт - 5 мільйонів гривень;
…	…
норма відсутня	5. Усі постачальники, які беруть участь у державних закупівлях, повинні мати діючий кіберстраховий поліс, що покриває ризики, пов'язані з обробкою державних даних. 6. При здійсненні публічних закупівель пристроїв Інтернету речей (IoT) замовник зобов'язаний враховувати

	відповідність продукції стандартам кібербезпеки, підтвердженим сертифікатом відповідності. 7. При здійсненні публічних закупівель послуг на користування сервісами хмарних послуг замовники зобов’язані враховувати рівень кіберзахисту даних. Провайдери повинні надати сертифікати відповідності міжнародним стандартам кібербезпеки. 8. При здійсненні публічних закупівель програмного забезпечення або послуг хмарних сервісів замовники зобов’язані вимагати наявність функціоналу резервного копіювання даних. 9. При здійсненні публічних закупівель програмного забезпечення замовники зобов’язані вимагати наявність функціоналу для управління правами доступу та ведення аудиту. 10. Закупівля програмних рішень для державних установ та критичної інфраструктури повинна передбачати наявність у таких рішеннях засобів аналізу джерел атак, виявлення загроз та реагування на інциденти.

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (Відомості Верховної Ради України (ВВР), 2017, № 45, ст. 400 із наступними змінами)	
Стаття 15. Рівні довіри до засобів та схем електронної ідентифікації … *норма відсутня*	**Стаття 15.** Рівні довіри до засобів та схем електронної ідентифікації … 5. Смарт-контракти, що використовуються для фінансових операцій або державних реєстрів, повинні мати сертифіковане аудиторське підтвердження від спеціалізованих кібербезпекових компаній, що підтверджує їх відповідність стандартам безпеки.
Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради України (ВВР), 2017, № 45, ст. 403 із наступними змінами)	
Стаття 6. Об’єкти критичної інфраструктури … *норма відсутня*	**Стаття 6.** Об’єкти критичної інфраструктури … 6. Об’єкти аграрного сектору, що використовують інформаційні технології для управління виробництвом, зберігання даних та логістики, вважаються критично важливими для національної безпеки та підлягають обов’язковому кіберзахисту.

	Інформаційні системи, які використовуються в агротехнологіях, управлінні агропідприємствами та логістиці продукції, підлягають обов’язковій сертифікації та кіберзахисту. Центральний орган виконавчої влади, що забезпечує формування та реалізує державну аграрну політику, державну політику у сферах сільського господарства та з питань продовольчої безпеки держави здійснює оцінку ризиків кіберзагроз та розробку рекомендацій для впровадження сучасних кіберзахисних технологій у сільськогосподарському секторі.
Стаття 8. Національна система кібербезпеки … 2. Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які	**Стаття 8.** Національна система кібербезпеки … 2. Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які

відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання: … *норма відсутня*	відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання: … Державні установи зобов’язані використовувати лише сертифіковане програмне та апаратне забезпечення, яке відповідає вимогам національної безпеки. Використання продуктів, розроблених у країнах, що представляють геополітичну загрозу, забороняється. Суб’єкти критичної інфраструктури зобов’язані впроваджувати системи управління кіберризиками відповідно до стандартів ISO/IEC 27001 та забезпечувати щорічний аудит ефективності цих систем.
… *норма відсутня*	… 7. Єдина державна платформа для обміну інформацією про кіберзагрози забезпечує: 1) реєстрацію всіх кіберінцидентів державного рівня; 2) оперативне сповіщення про нові загрози; 3) інтеграцію з приватними ініціативами у сфері кібербезпеки.»;

	8. Суб’єкти господарювання зобов’язані розробляти, затверджувати та впроваджувати політики кібербезпеки, що включають заходи з протидії кібератакам, навчання співробітників основам кібергігієни та впровадження сучасних засобів захисту інформації. 9. Програмне забезпечення, що використовується державними органами, підлягає обов’язковій періодичній перевірці на відповідність вимогам кібербезпеки, включаючи аналіз коду на наявність вразливостей та шкідливого функціоналу. 10. Суб’єкти критичної інфраструктури зобов’язані підключитися до національної системи моніторингу кіберзагроз для автоматичного виявлення джерел атак та аналізу підозрілої активності. Державні установи та приватні компанії, що працюють із критичною інформаційною інфраструктурою, зобов’язані передавати дані про кіберінциденти та джерела атак до національної системи моніторингу кібербезпеки.

Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA 1. Завданнями CERT-UA є: … *норма відсутня*	**Стаття 9.** Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA 1. Завданнями CERT-UA є: … 10) здійснення постійного моніторингу стану кібербезпеки об'єктів критичної інфраструктури та надає обов'язкові рекомендації для усунення виявлених недоліків.
норма відсутня	**Стаття 9[1].** Національний центр міжнародної координації з кібербезпеки 1. Завданнями Національного центру міжнародної координації з кібербезпеки є: 1) обмін інформацією про кіберзагрози та атаки з НАТО, ЄС та іншими міжнародними організаціями; 2) співпраця з Interpol та Europol щодо розслідування міжнародних кіберзлочинів; 3) спільно з міжнародними експертами розробка рекомендацій та стандартів кіберзахисту.

	2. Національний центр міжнародної координації з кібербезпеки забезпечує: 1) взаємодію України з міжнародними організаціями, зокрема NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) та European Union Agency for Cybersecurity (ENISA); 2) участь у міжнародних кібернавчаннях та обмін досвідом з провідними країнами у сфері кіберзахисту; 3) підготовку фахівців у галузі кібербезпеки через міжнародні програми навчання.
Стаття 11. Сприяння суб'єктам забезпечення кібербезпеки України … *норма відсутня*	**Стаття 11.** Сприяння суб'єктам забезпечення кібербезпеки України … Державні органи, що відповідають за забезпечення кібербезпеки, повинні здійснювати постійний моніторинг кіберзагроз та вживати заходів для запобігання кіберінцидентам. Це включає використання технологій штучного інтелекту для виявлення та запобігання атакам у режимі реального часу.

Стаття 13. Фінансове забезпечення заходів кібербезпеки … *норма відсутня*	**Стаття 13.** Фінансове забезпечення заходів кібербезпеки … Держава зобов’язана забезпечувати фінансування заходів з кібербезпеки для захисту державних установ, критичної інфраструктури та державних інформаційних ресурсів.
Закон України «Про основні національну безпеку України» (Відомості Верховної Ради України (ВВР), 2018, № 31, ст. 241 із наступними змінами)	
Стаття 31. Стратегія кібербезпеки України … *норма відсутня*	**Стаття 31.** Стратегія кібербезпеки України … 4. Україна бере участь у міжнародних кіберопераціях, спрямованих на протидію ворожим кіберзагрозам, у співпраці з країнами-партнерами НАТО та ЄС. Для цього створюється Національний центр кібероборони, який здійснює стратегічне планування, аналіз загроз та кібероперації оборонного характеру.

Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» (Відомості Верховної Ради України (ВВР), 2020, № 25, ст. 171 із наступними змінами)	
Стаття 18. Повноваження та обов'язки суб'єктів державного фінансового моніторингу … *норма відсутня*	**Стаття 18.** Повноваження та обов'язки суб'єктів державного фінансового моніторингу … 16. Банки та фінансові установи, які проводять операції з використанням блокчейн-технологій, зобов'язані: 1) використовувати автоматизовані системи аналізу транзакцій для виявлення підозрілих операцій; 2) запровадити механізми ідентифікації учасників транзакцій; 3) здійснювати аудит безпеки своїх блокчейн-платформ не рідше одного разу на рік.
Закон України «Про електронні комунікації» (Офіційний вісник України, 2021, № 6, ст. 306 із наступними змінами)	
Стаття 31. Забезпечення безпеки електронних комунікаційних мереж …	**Стаття 31.** Забезпечення безпеки електронних комунікаційних мереж …

норма відсутня	3. Мобільні оператори зобов’язані надавати клієнтам SMS-сповіщення про актуальні кіберзагрози та рекомендації щодо їх уникнення. 4. Провайдери хмарних сервісів повинні здійснювати щорічний аудит кібербезпеки з поданням звіту до Держспецзв’язку. 5. Оператори електронних комунікаційних мереж повинні використовувати лише програмне забезпечення, яке пройшло сертифікацію на відповідність вимогам кібербезпеки. 6. Мобільні оператори повинні впроваджувати засоби захисту від перехоплення сигналу, несанкціонованого доступу до мережі та атак типу man-in-the-middle
Стаття 104. Загальні засади надання електронних комунікаційних послуг кінцевим користувачам … *норма відсутня*	**Стаття 104.** Загальні засади надання електронних комунікаційних послуг кінцевим користувачам … 10. Провайдери інтернет-послуг зобов’язані надавати користувачам рекомендації з кібергігієни, включаючи: 1) поради щодо налаштування захищених з’єднань;

	2) попередження про актуальні кіберзагрози.
Закон України «Про критичну інфраструктуру» (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13 із наступними змінами)	
Стаття 21. Завдання, права та обов'язки операторів критичної інфраструктури … 4. Оператори критичної інфраструктури зобов'язані: … *норма відсутня* …	**Стаття 21.** Завдання, права та обов'язки операторів критичної інфраструктури … 4. Оператори критичної інфраструктури зобов'язані: … 3[1]) щороку проводити тестування на проникнення, що має підтверджувати захищеність інформаційних систем від актуальних кіберзагроз; …
Стаття 22. Планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури … *норма відсутня*	**Стаття 22.** Планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури … 8. Об'єкти критичної інформаційної інфраструктури зобов'язані щорічно брати участь у навчаннях, організованих Національним координаційним центром

	кібербезпеки, для перевірки готовності до реагування на кібератаки. 9. Об’єкти критичної інфраструктури зобов’язані укладати договори кіберстрахування з акредитованими страховиками для покриття таких можливих ризиків кібератак: 1) використання шкідливого програмного забезпечення; 2) DDoS-атаки; 3) заподіяння збитків через витік конфіденційної інформації. 10. Об’єкти критичної інфраструктури зобов’язані впроваджувати: 1) системи моніторингу стану пристроїв Інтернету речей (IoT); 2) захист від DDoS-атак через пристрої Інтернету речей (IoT); 3) регулярний аудит безпеки підключених пристроїв Інтернету речей (IoT).

	11. Хмарні сервіси, що обробляють дані критичної інформаційної інфраструктури, підлягають обов'язковій сертифікації та моніторингу.
Закон України «Про страхування» (Відомості Верховної Ради України (ВВР), 2023, № 12-13, ст. 28 із наступними змінами)	
Стаття 4. Класи страхування 1. До класів страхування іншого, ніж страхування життя, належать: … *норма відсутня* **…**	**Стаття 4.** Класи страхування 1. До класів страхування іншого, ніж страхування життя, належать: … 9^{1}) клас 9.1 – кіберстрахування, що покриває збитки від кіберзагроз, включаючи витрати на відновлення даних, забезпечення безперервності бізнесу та компенсацію витрат клієнтам; **…**
Закон України «Про віртуальні активи» (Відомості Верховної Ради України (ВВР), 2023, № 15, ст. 51 із наступними змінами)	
Стаття 9. Права та обов'язки учасників ринку віртуальних послуг …	**Стаття 9.** Права та обов'язки учасників ринку віртуальних послуг …

норма відсутня	8. Блокчейн-платформи, що використовуються для фінансових операцій, повинні відповідати стандартам безпеки, визначеним Національним банком України та Держспецзв'язку, зокрема, забезпечувати криптографічний захист даних, безпечне зберігання приватних ключів та захист від несанкціонованого доступу.