

**ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

Кваліфікаційна наукова
праця на правах рукопису

ДЕМЕДЮК СЕРГІЙ ВАСИЛЬОВИЧ

УДК 343.9.01:004.056(477)

**ДИСЕРТАЦІЯ
ОРГАНІЗАЦІЙНО-ПРАВОВІ ТА КРИМІНОЛОГІЧНІ ЗАСАДИ
КІБЕРСТІЙКОСТІ В УКРАЇНІ**

12.00.07 «Адміністративне право і процес; фінансове право;
інформаційне право»

12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право»

Юридичні науки

Подається на здобуття наукового ступеня доктора юридичних наук

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

С.В. Демедюк

Одеса – 2026

АНОТАЦІЯ

Демедюк С.В. Організаційно-правові та кримінологічні засади кіберстійкості в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальностями: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право»; 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». – Одеський державний університет внутрішніх справ, Одеса, 2026.

У дисертації здійснено комплексне теоретико-правове та кримінологічне дослідження кіберстійкості як новітньої парадигми забезпечення національної безпеки України в умовах цифрової трансформації та гібридної агресії. Обґрунтовано, що традиційна модель кібербезпеки, орієнтована на запобігання інцидентам і захист периметра, є обмежено ефективною в умовах зростання складності, масштабності та багатовекторності кіберзагроз, що зумовлює необхідність переходу до концепції кіберстійкості як здатності соціотехнічних систем передбачати, протидіяти, витримувати, відновлюватися та адаптуватися до деструктивних впливів.

Розкрито генезис і еволюцію поняття «стійкість» у міждисциплінарному вимірі, що дозволило сформулювати сучасне розуміння кіберстійкості як емерджентної властивості складних адаптивних систем. Запропоновано авторське визначення кіберстійкості та здійснено теоретичне розмежування категорій «кібербезпека» і «кіберстійкість». Доведено доцільність зміщення акцентів державної політики з протидії загрозам на забезпечення безперервності функціонування критичних процесів та мінімізацію каскадних ефектів ураження.

На основі компаративного аналізу здійснено поглиблене дослідження міжнародного досвіду формування кіберстійкості, що дозволило виявити концептуальні, нормативні та інституційні особливості відповідних моделей у

провідних юрисдикціях. Зокрема, встановлено, що підхід Європейського Союзу характеризується високим рівнем нормативної деталізації та гармонізації через систему обов'язкових директив і регламентів, орієнтованих на забезпечення безперервності функціонування критичних сервісів, управління ризиками, підвищення відповідальності постачальників цифрових продуктів і послуг, а також інтеграцію кіберстійкості у життєвий цикл ІКТ-рішень. Американська модель вирізняється гнучкістю та значною роллю ринкових механізмів і стандартів, зокрема через використання рекомендаційних рамок, публічно-приватного партнерства та стимулювання добровільного дотримання стандартів кібербезпеки, що забезпечує адаптивність до динамічних загроз. Підхід Великої Британії поєднує централізоване стратегічне управління з розвитком секторальних моделей кіберстійкості та активною роллю держави у координації суб'єктів критичної інфраструктури. Водночас модель НАТО акцентує увагу на колективній кіберобороні, оперативній сумісності, стандартизації процедур реагування та інтеграції кіберпростору як повноцінного домену безпеки.

У результаті узагальнення зазначених підходів обґрунтовано, що ключовими трендами розвитку кіберстійкості є: перехід від реактивних до проактивних моделей управління ризиками; інтеграція кіберстійкості у всі етапи життєвого циклу цифрових продуктів і послуг; посилення ролі держави як регулятора та координатора при одночасному збереженні активної участі приватного сектору; розвиток стандартів та сертифікаційних механізмів; формування культури кіберстійкості як складової національної безпеки.

Обґрунтовано напрями гармонізації національного законодавства України з євроатлантичними стандартами, що включають: імплементацію ризик-орієнтованого підходу до регулювання кібербезпеки; запровадження обов'язкових вимог до управління ризиками для суб'єктів критичної інфраструктури; розвиток системи національних і галузевих стандартів кіберстійкості, узгоджених із міжнародними; встановлення вимог до безпеки цифрових продуктів на всіх етапах їх життєвого циклу; удосконалення

механізмів обміну інформацією про кіберінциденти; запровадження ефективних інструментів нагляду та відповідальності.

Розроблено концептуальну модель інституціоналізації кіберстійкості, що ґрунтується на інтеграції державного, приватного та громадянського секторів у межах єдиної системи кіберуправління на засадах спільної відповідальності, взаємодії та обміну інформацією. Модель передбачає чіткий розподіл ролей і функцій між суб'єктами, водночас забезпечуючи їх координацію через горизонтальні та вертикальні зв'язки. Запропоновано трикомпонентну модель забезпечення кіберстійкості, яка охоплює регуляторний компонент (формування обов'язкових правових вимог і політик), стандартизаційний (уніфікація процедур, впровадження стандартів і сертифікації) та стимулюючий (економічні й організаційні механізми заохочення до підвищення рівня безпеки). Обґрунтовано доцільність трансформації координаційних органів у стратегічні хаби, що виконують функції інтеграції даних, аналітичної обробки інформації, управління ризиками та забезпечення міжсекторальної взаємодії, підвищуючи адаптивність і стійкість національної системи кібербезпеки.

Важливе місце у дослідженні посідає обґрунтування необхідності розвитку цивільно-військового співробітництва у кіберпросторі як ключового елементу забезпечення кіберстійкості держави. Запропоновано концепцію «Cyber-CIMIC», яка розглядається як багаторівнева модель інтеграції спроможностей сектору безпеки і оборони, приватного сектору та громадянського суспільства на основі координації, довіри та обміну інформацією. Модель передбачає формування спільних операційних механізмів реагування на кіберзагрози, залучення експертного потенціалу недержавних суб'єктів, а також розвиток партнерських платформ взаємодії. Обґрунтовано доцільність створення інституту цивільного кіберрезерву як інструменту мобілізації висококваліфікованих фахівців для виконання завдань кібероборони в умовах кризових ситуацій. Запропоновано впровадження регуляторних «пісочниць», що забезпечують апробацію інноваційних рішень

у контрольованому правовому середовищі, сприяють розвитку технологій та легітимізації участі приватного сектору у забезпеченні національної кібербезпеки.

Окремий блок дослідження присвячено розвитку методології аналітичної розвідки у сфері кіберстійкості як ключового інструменту стратегічного управління кіберризиками. Обґрунтовано, що ефективність управлінських рішень у цій сфері визначається рівнем інтеграції методів OSINT, стратегічного форсайту та ризик-орієнтованого підходу, які у сукупності забезпечують системне виявлення, оцінювання та прогнозування кіберзагроз. Запропоновано модель інтелектуальної стійкості, що передбачає багаторівневу обробку даних – від збору та верифікації до аналітичної інтерпретації і формування сценаріїв розвитку загроз. Модель орієнтована на забезпечення безперервного аналітичного циклу, підвищення якості стратегічного прогнозування та підтримку прийняття управлінських рішень в умовах високої невизначеності, динамічності середовища та інформаційної надлишковості.

На основі емпіричного аналізу здійснено системну ідентифікацію та ранжування кіберзагроз за рівнем їх ризику поширення в Україні з урахуванням ймовірності реалізації, потенційних наслідків та вразливостей ключових секторів. Визначено пріоритетні напрями зміцнення кіберстійкості, насамперед у сферах критичної інфраструктури, де зосереджені найбільш чутливі до деструктивних впливів функціональні системи. Запропоновано комплексну матричну модель діагностики кіберстійкості, яка інтегрує функціональні етапи управління інцидентами (передбачення, витримування, відновлення, адаптація) з операційними доменами (фізичним, інформаційним, когнітивним, соціальним). Така модель забезпечує багатовимірну оцінку стану системи, дозволяє виявляти критичні точки вразливості, визначати рівень готовності до реагування та відновлення, а також формувати обґрунтовані управлінські рішення щодо підвищення загального рівня кіберстійкості.

У дисертації здійснено комплексний кримінологічний аналіз кіберзлочинності як складного багаторівневого явища, що функціонує в умовах глобалізованого цифрового середовища, і протидія якому є одним із ключових напрямів забезпечення кіберстійкості в суспільстві. Визначено сучасні тенденції кіберзлочинності, зокрема зростання організованих форм кіберзлочинної діяльності, професіоналізацію учасників, транснаціональний характер злочинних мереж та активне використання цифрових платформ для координації протиправної діяльності. Розкрито інструментарій кіберзлочинності, включаючи шкідливе програмне забезпечення, фішингові кампанії, експлуатацію вразливостей інформаційних систем, а також механізми фінансової анонімізації. Особливу увагу приділено мотиваційним детермінантам, серед яких домінують економічні інтереси, політично вмотивовані дії та гібридні форми впливу, пов'язані з інформаційно-психологічними операціями.

Обґрунтовано доцільність переходу від реактивних до предиктивних моделей протидії кіберзлочинності, що передбачають використання стратегічного аналізу, технологій обробки великих масивів даних, поведінкових моделей та ризик-орієнтованого підходу. Такий підхід дозволяє не лише виявляти вже реалізовані загрози, але й прогнозувати їх розвиток, ідентифікувати потенційні вразливості та формувати проактивні заходи реагування. Виявлено особливості функціонування кримінальних екосистем у кіберпросторі, які характеризуються високим рівнем децентралізації, сервісною моделлю, використанням соціальної інженерії як ключового інструменту впливу, а також широким застосуванням анонімізаційних технологій і цифрових фінансових інструментів, зокрема криптовалют.

Сформовано цілісну теоретико-методологічну концепцію кіберстійкості як вищого рівня кібербезпеки, що інтегрує правові, організаційні та аналітичні механізми управління кіберризиками. У межах цієї концепції кіберстійкість розглядається як системна здатність держави та суспільства забезпечувати безперервність функціонування, адаптацію та розвиток в умовах постійних

кіберзагроз. Розроблено інституціональні, організаційно-правові та кримінологічні засади забезпечення кіберстійкості, які охоплюють удосконалення нормативно-правової бази, розвиток міжсекторальної взаємодії, впровадження сучасних аналітичних інструментів та формування культури кібербезпеки. На цій основі сформовано пропозиції до удосконалення чинного законодавства. Запропоновано інноваційні моделі оцінювання та управління кіберризиками, що базуються на інтеграції кількісних і якісних показників, дозволяють здійснювати багаторівневу діагностику стану системи та забезпечують підґрунтя для прийняття обґрунтованих стратегічних рішень у сфері національної безпеки.

Ключові слова: кіберстійкість, кібербезпека, кіберзагрози, кіберзлочинність, ризик-орієнтований підхід, OSINT, форсайт, критична інфраструктура, національна безпека, правове регулювання.

SUMMARY

Demedyuk S.V. Organisational, legal and criminological foundations of cyber resilience in Ukraine. – Qualification scientific work on the rights of the manuscript.

Thesis for the degree of Doctor of Law in the following specialities: 12.00.07 «Administrative law and process; financial law; information law»; 12.00.08 «Criminal law and criminology; criminal enforcement law». – Odessa State University of Internal Affairs, Odessa, 2026.

The dissertation provides a comprehensive theoretical, legal, and criminological study of cyber resilience as a novel paradigm for ensuring Ukraine's national security in the context of digital transformation and hybrid aggression. It is substantiated that the traditional cybersecurity model, focused on incident prevention and perimeter protection, exhibits limited effectiveness against increasingly complex, large-scale, and multi-vector cyber threats. This necessitates a transition to the concept of cyber resilience, defined as the ability of socio-technical systems to anticipate, withstand, recover from, and adapt to disruptive influences.

The genesis and evolution of the "resilience" concept are revealed within an interdisciplinary dimension, allowing for the formulation of a modern understanding of cyber resilience as an emergent property of complex adaptive systems. An original author's definition of cyber resilience is proposed, and a theoretical distinction between the categories of "cybersecurity" and "cyber resilience" is established. The study proves the expediency of shifting public policy focus from merely countering threats to ensuring the continuity of critical processes and minimizing the cascading effects of compromises.

Based on comparative analysis, an in-depth study of international experience in building cyber resilience was conducted, identifying conceptual, regulatory, and institutional characteristics of respective models in leading jurisdictions. Specifically, it is established that the European Union's approach is characterized by a high level of regulatory detail and harmonization through a system of mandatory directives and regulations. These are aimed at ensuring the continuity of critical services, risk management, increasing the accountability of digital product and service providers, and integrating cyber resilience into the ICT solutions' lifecycle. The American model is distinguished by its flexibility and the significant role of market mechanisms and standards, particularly through the use of non-binding frameworks, public-private partnerships, and incentives for voluntary compliance with cybersecurity standards, ensuring adaptability to dynamic threats. The United Kingdom's approach combines centralized strategic management with the development of sectoral cyber resilience models and an active state role in coordinating critical infrastructure entities. Meanwhile, the NATO model emphasizes collective cyber defense, operational interoperability, standardization of response procedures, and the integration of cyberspace as a fully-fledged security domain.

By synthesizing these approaches, it is substantiated that the key trends in the development of cyber resilience include: a shift from reactive to proactive risk management models; the integration of cyber resilience into all stages of the digital product and service lifecycle; the strengthening of the state's role as a regulator and

coordinator while maintaining the active participation of the private sector; the development of standards and certification mechanisms; and the formation of a cyber resilience culture as a component of national security.

The study outlines directions for harmonizing Ukraine's national legislation with Euro-Atlantic standards, including: implementing a risk-oriented approach to cybersecurity regulation; introducing mandatory risk management requirements for critical infrastructure entities; developing a system of national and sectoral cyber resilience standards aligned with international ones; establishing security requirements for digital products throughout their entire lifecycle; improving mechanisms for cyber incident information sharing; and introducing effective oversight and accountability tools.

A conceptual model for the institutionalization of cyber resilience has been developed, based on the integration of the public, private, and civil sectors within a unified cyber governance system founded on the principles of shared responsibility, cooperation, and information exchange. This model provides a clear distribution of roles and functions among actors while ensuring coordination through horizontal and vertical linkages. A three-component model for ensuring cyber resilience is proposed, encompassing a regulatory component (formation of mandatory legal requirements and policies), a standardization component (unification of procedures, implementation of standards and certification), and an incentive component (economic and organizational mechanisms to encourage higher security levels). The study justifies the expediency of transforming coordination bodies into strategic hubs that perform data integration, analytical processing, risk management, and cross-sectoral interaction functions, thereby increasing the adaptability and resilience of the national cybersecurity system.

A significant focus of the study is the substantiation of the need to develop civil-military cooperation in cyberspace as a key element of ensuring state cyber resilience. The "Cyber-CIMIC" concept is proposed, viewed as a multi-layered model for integrating the capabilities of the security and defense sector, the private sector, and civil society based on coordination, trust, and information exchange. The

model envisages the formation of joint operational mechanisms for responding to cyber threats, leveraging the expert potential of non-state actors, and developing partnership-based interaction platforms. The study justifies the expediency of establishing a civilian cyber reserve as a tool for mobilizing highly qualified specialists to perform cyber defense tasks during crisis situations. Additionally, the introduction of regulatory sandboxes is proposed to provide a controlled legal environment for testing innovative solutions, fostering technological development, and legitimizing private sector involvement in ensuring national cybersecurity.

A separate block of the research is dedicated to the development of analytical intelligence methodology in the field of cyber resilience as a key tool for strategic cyber risk management. It is argued that the effectiveness of management decisions in this area is determined by the integration of OSINT methods, strategic foresight, and a risk-oriented approach, which collectively provide systematic detection, assessment, and forecasting of cyber threats. An intellectual resilience model is proposed, involving multi-level data processing—from collection and verification to analytical interpretation and threat scenario development. The model aims to ensure a continuous analytical cycle, improve the quality of strategic forecasting, and support decision-making under conditions of high uncertainty, dynamic environments, and information redundancy.

Based on empirical analysis, a systematic identification and ranking of cyber threats by their risk level in Ukraine was conducted, considering the probability of realization, potential consequences, and vulnerabilities of key sectors. Priority areas for strengthening cyber resilience are identified, primarily within critical infrastructure sectors where functional systems most sensitive to destructive impacts are concentrated. A comprehensive matrix model for cyber resilience diagnostics is proposed, integrating functional stages of incident management (anticipate, withstand, recover, adapt) with operational domains (physical, informational, cognitive, and social). This model provides a multi-dimensional assessment of the system's state, allows for the identification of critical vulnerabilities, determines

readiness for response and recovery, and facilitates the formulation of informed management decisions to enhance the overall level of cyber resilience.

The dissertation provides a comprehensive criminological analysis of cybercrime as a complex, multi-layered phenomenon operating within a globalized digital environment, where countering such activity is a pivotal direction for ensuring societal cyber resilience. Modern trends in cybercrime are identified, specifically the rise of organized cybercriminal activities, the professionalization of actors, the transnational nature of criminal networks, and the active use of digital platforms to coordinate illicit operations. The toolkit of cybercrime is revealed, including malware, phishing campaigns, the exploitation of information system vulnerabilities, and financial anonymization mechanisms. Particular attention is paid to motivational determinants, dominated by economic interests, politically motivated actions, and hybrid forms of influence associated with information and psychological operations.

The study substantiates the expediency of transitioning from reactive to predictive models of countering cybercrime, which involve the use of strategic analysis, big data processing technologies, behavioral models, and a risk-oriented approach. Such an approach allows not only for the detection of realized threats but also for forecasting their evolution, identifying potential vulnerabilities, and formulating proactive response measures. The research identifies the functional features of criminal ecosystems in cyberspace, characterized by a high level of decentralization, a "service-based" model (Cybercrime-as-a-Service), the use of social engineering as a primary influence tool, and the extensive application of anonymization technologies and digital financial instruments, including cryptocurrencies.

A cohesive theoretical and methodological concept of cyber resilience is formulated as a superior level of cybersecurity that integrates legal, organizational, and analytical mechanisms for cyber risk management. Within this framework, cyber resilience is viewed as the systemic capacity of the state and society to ensure operational continuity, adaptation, and development in the face of persistent cyber

threats. Institutional, legal, and criminological foundations for ensuring cyber resilience are developed, covering the improvement of the regulatory framework, the development of cross-sectoral interaction, the implementation of modern analytical tools, and the cultivation of a cybersecurity culture. Based on this, proposals for improving current legislation are formulated. Innovative models for cyber risk assessment and management are proposed, grounded in the integration of quantitative and qualitative indicators, enabling multi-level diagnostics of the system's state and providing a basis for making informed strategic decisions in the field of national security.

Keywords: cyber resilience, cybersecurity, cyber threats, cybercrime, risk-oriented approach, OSINT, foresight, critical infrastructure, national security, legal regulation.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації

Монографії

1. Демедюк С.В. Розділ 26. Кібервійна та форсайт кіберстійкості. Реалізація філософії ІЛР в системі кримінального аналізу Національної поліції України: монографія / О.Є. Користін, Б.А. Денисенко, С.В. Демедюк та ін. ; за заг. ред. д-ра юрид. наук, проф. О.Є. Користіна. Київ: ВАЙТЕ, 2024. С. 343-357. DOI: <https://doi.org/10.36486/978-966-2310-66-5-26>

2. Демедюк С.В. Розділ 1. Стратегічний ландшафт застосування OSINT в секторі національної безпеки. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. С. 21-36.

*Статті у наукових періодичних виданнях інших держав, у тому числі
проіндексованих у базах даних Web of Science Core Collection, Scopus*

1. Demedyuk S.V., Demedyuk T.S. Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. 2018. Vol. 68 № 6. P. 278-290. DOI: [10.33407/itlt.v68i6.2582](https://doi.org/10.33407/itlt.v68i6.2582) (WoS)

2. Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. *International Journal of Computer Network and Information Security*. 2024. Vol. 16. №. 1. P. 24-34. DOI: <https://doi.org/10.5815/ijcnis.2024.01.02> (Scopus Q3)

3. Korystin O., Demediuk S., Sviridyuk N., Mitina O., Aleksander M., Yuriy Kardashevskyy. Risk Forecasting of Information-content-security. *Cyber Hygiene & Conflict Management in Global Information Networks: Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks*. 2025. Vol. 3925. P. 273–280. (Scopus Q4)

4. Korystin O., Demediuk S., Likhovitsky Y., Kardashevsky Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns. *International Journal of Information Technology and Computer Science*. 2025. Vol. 17. No. 2. P. 24-35. DOI: <https://doi.org/10.5815/ijitcs.2025.02.03> (Scopus Q3)

5. Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*. (2025). Vol. 17. Is. 19. P. 8757. <https://doi.org/10.3390/su17198757> (Scopus Q1)

*Статті у наукових виданнях, включених до Переліку наукових фахових
видань України*

6. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона*. 2023. № 1(59). С.77-85. DOI: [https://doi.org/10.36486/np.2023.1\(59\).8](https://doi.org/10.36486/np.2023.1(59).8)

7. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона*. 2023. № 2(60). С.78-85. DOI: [https://doi.org/10.36486/np.2023.2\(60\).8](https://doi.org/10.36486/np.2023.2(60).8)

8. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59. DOI: <https://doi.org/10.32850/sulj.2023.3.10>

9. Демедюк С.В. Захист критично важливих послуг у цифрову епоху. *Наука і правоохорона*. 2023. № 3(61). С.26-34 DOI (Issue): [https://doi.org/10.36486/np.2023.3\(61\).3](https://doi.org/10.36486/np.2023.3(61).3)

10. Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет»*. 2023. №06. С. 708-713. DOI: <https://doi.org/10.24144/2788-6018.2023.06.122>

11. Демедюк С.В. Інституціоналізація кіберстійкості. *Наука і правоохорона*. 2023. № 4(62). С.31-41. DOI: [https://doi.org/10.36486/np.2023.4\(62\).4](https://doi.org/10.36486/np.2023.4(62).4)
12. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. *Наука і правоохорона*. 2024. № 1(63). С.133-141. DOI: [https://doi.org/10.36486/np.2024.1\(63\).13](https://doi.org/10.36486/np.2024.1(63).13)
13. Демедюк С.В. OSINT в контексті кібербезпеки. *Юридичний бюлетень*. 2024. № 34. С.200-207. DOI:10.32850/LB2414-4207.2024.34.26
14. Демедюк С.В. OSINT в контексті виявлення та запобігання кіберзлочинам. *Південноукраїнський правничий часопис*. 2024. № 4. С. 38-41. DOI: <https://doi.org/10.32850/sulj.2024.4.7>
15. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154. DOI: [https://doi.org/10.36486/np.2024.3\(65\).12](https://doi.org/10.36486/np.2024.3(65).12)
16. Демедюк С.В. Зміст та особливості експертної вибірки в оцінюванні кіберризиків. *Морська безпека та оборона*. 2025. №1. С.17-24. DOI: <https://doi.org/10.32782/msd/2025.1/03>
17. Демедюк С.В. Сучасні тенденції on-line шахрайства в Україні. *Право і суспільство*. 2025. №4. Т. 2. С. 186-194. DOI: <https://doi.org/10.32842/2078-3736/2025.4.2.28>
18. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. *Правові новели*. 2025. № 26. 157-166. DOI: <https://doi.org/10.32782/ln.2025.26.18>

Наукові праці, які засвідчують апробацію матеріалів дисертації

1. Демедюк С.В. Стійкість системи кібербезпеки та її правове забезпечення в Україні. *Закарпатські правові читання: збірник тез за матеріалами XV міжнародної науково-практичної конференції (Ужгород, 27 квітня 2023 р.)*. Ужгород: УЖНУ, 2023. С. 5-7.

2. Демедюк С.В. Захист критично важливої інформаційної інфраструктури в системі кібербезпеки. *Стратегії безпеки підприємництва в умовах воєнного стану: Збірник тез за матеріалами XIV міжнародної науково-практичної конференції «Безпекотворення: питання теорії, практики та правові аспекти»* (Київ, 06 квітня 2023 р.) / за ред. Тимошенко О.І., Київ: Видавництво Європейського університету», 2023. С. 26-27.

3. Демедюк С.В. Розбудова кіберстійкості на національному рівні. *Актуальність та особливості наукових досліджень в умовах воєнного стану: збірник матеріалів III Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки – 2023 в Україні* (Київ, 23 травня 2023 р.). Київ: ДНДІ МВС України, 2023. С. 133-134.

4. Демедюк С.В. Актуалізація сучасних методологій аналізу кіберзлочинності. *Стан та перспективи розвитку адміністративного права України: матеріали X міжнародної науково-практичної інтернет-конференції* (Одеса, 20 жовтня 2023 р.). Одеса: ОДУВС. С. 63-66.

5. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення: матеріали науково-практичного круглого столу* (Київ, 26 вересня 2023 р.) / [Редкол.: Вербенський М. Г., Опришко І. В., Кулик О. Г. та ін.]. Київ : ДНДІ МВС України, 2023. С. 168-170.

6. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України: матеріали міжвідомчої науково-практичної конференції*. (Київ, 17 листопада 2023 р.). Київ: НАВС. С.40-44.

7. Демедюк С.В. Захист критично важливих кібер-активів. *Кібербезпека в Україні: правові та організаційні питання: збірник матеріалів міжнародної науково-практичної конференції* (Одеса, 17 листопада 2023 р.). Одеса: ОДУВС. С.55-57.

8. Демедюк С.В. Показники кіберстійкості. *Актуальні питання забезпечення безпекового середовища в Україні: збірник тез наукових*

доповідей Всеукраїнської науково-практичної конференції (Київ, 19 квітня 2024 р.). Київ: ДНДІ МВС України, 2024. С.38-41.

9. Демедюк С.В. Щодо питань розвитку кіберстійкості. *Актуальність та особливості наукових досліджень в умовах воєнного стану*: збірник матеріалів IV Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки-2024 в Україні (Київ, 22 травня 2024 р.). Київ: ДНДІ МВС України, 2024. С.19-21.

10. Демедюк С.В. Використання злочинцями комп'ютерних систем та мереж. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки*: збірник матеріалів всеукраїнської науково-практичної конференції (Київ, 27 вересня 2024 р.). Київ: ДНДІ. С. 203-207.

11. Демедюк С.В. Особливості онлайн шахрайства в Україні. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (Київ, 01 листопада 2024 р.). Київ: НАВС, 2024. С. 35-38.

12. Демедюк С.В. Поширення та характерні складові кіберзалежних злочинів. *Протидія організованих злочинності і корупції в умовах збройного конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ*: збірник матеріалів Міжнародної науково-практичної конференції (Кропивницький, 04 жовтня 2024 року). Кропивницький: ДонДУВС, 2024. С. 268-273.

13. Демедюк С.В. Інтеграція OSINT в систему кібербезпеки держави: стратегічні та прикладні аспекти. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України*: матеріали круглого столу (Львів, 07 травня 2025 р.). Львів: ЛьвДУВС, 2025. С. 58-61.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	20
ВСТУП	23
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ РОЗБУДОВИ НАЦІОНАЛЬНОЇ КІБЕРСТІЙКОСТІ	42
1.1. Актуалізація кіберстійкості та історичні витoki концепції «стійкість»	42
1.2. Концептуальні основи та функціональні компоненти кіберстійкості	61
1.3. Нормативно-правове та стратегічне забезпечення національної кіберстійкості	79
Висновки до розділу 1	97
 РОЗДІЛ 2. ОРГАНІЗАЦІЙНО-ПРАВОВІ НАПРЯМИ ТА ЗМІСТ ІНСТИТУАЛІЗАЦІЇ КІБЕРСТІЙКОСТІ	101
2.1. Інституціоналізація кіберстійкості	101
2.2. Суб'єктний склад та міжнародний контекст формування системи кіберстійкості	126
2.3. Організаційно-правові механізми цивільно-військового співробітництва у формуванні національної системи кіберстійкості ...	165
Висновки до розділу 2	210
 РОЗДІЛ 3. АНАЛІТИЧНА РОЗВІДКА СТРАТЕГІЧНИХ НАПРЯМІВ КІБЕРСТІЙКОСТІ В УКРАЇНІ	213
3.1. Методологія та процес аналітичної розвідки стратегічних напрямів кіберстійкості в Україні	213
3.2. Обґрунтування стратегічних напрямів кіберстійкості на основі аналізу кіберзагроз.....	258
3.3. Методологічні засади та діагностика кіберстійкості національної інформаційної інфраструктури	289

3.4. Прикладний аналіз системних спроможностей та правові орієнтири забезпечення кіберстійкості інформаційної інфраструктури	313
Висновки до розділу 3	345

РОЗДІЛ 4. ПРІОРИТЕТИ СТРАТЕГІЧНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ 348

4.1. Сучасні методологічні засади виявлення та аналізу кіберзлочинності	348
4.2. Виклики та пріоритетні напрями стратегічного забезпечення протидії кіберзлочинності в Україні	360
4.3. Ризики поширення кримінальних загроз у кіберпросторі	380
4.3.1. Кримінальні on-line ринки та комунікації	394
4.3.2. Міжсекторальні фактори злочинності: соціальна інженерія, Інтернет речей	415
Висновки до розділу 4	421

ВИСНОВКИ 424

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 435

ДОДАТКИ 484

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ДССЗЗІ, Держспецзв’язку – Державна служба спеціального зв’язку та захисту інформації

ДКП – Департаменту кіберполіції

ДПП – державно-приватне партнерства

ЄРДР – Єдиний реєстр досудових розслідувань

ЄС – Європейський Союз

ЗКІ – захист критично важливої інформаційної інфраструктури

ЗСУ – Збройні Сили України

ІКТ – інформаційно-комунікаційні технології

ІПСО – інформаційно-психологічні операції

ІТ – інформаційні технології

к/п – кримінальні правопорушення

КІ – критична інфраструктура

КІІ – критична інформаційна інфраструктура

ККУ – Кримінальний кодекс України

НАТО – Організація Північноатлантичного договору

НКЦК – Національний координаційний центр кібербезпеки

НПУ – Національна поліція України

ОГ – організована група

ОЗУ – організоване злочинне угруповання

ОКІ – об’єкти критичної інфраструктури

ООН – Організація Об’єднаних Націй

ОТ – операційні технології

РНБО України - Рада національної безпеки і оборони України

СБУ – Служба безпеки України

СОУ – Сили оборони України

США – Сполучені Штати Америки

ЦВС – цивільно-військове співробітництво

ЦОВВ – центральні органи виконавчої влади

ІІІ – штучний інтелект

4V – Volume, Velocity, Variety, Validation (Обсяг, Швидкість, Різноманітність, Валідація)

APT – Advanced Persistent Threat (Складна постійна загроза)

CCDCOE – Cooperative Cyber Defence Centre of Excellence (Об'єднаний центр передових технологій із кібероборони)

CERT – Computer Emergency Response Team (Команда реагування на комп'ютерні надзвичайні події)

CERT-RMM – CERT Resilience Management Model (Модель управління стійкістю)

CERT-UA – Computer Emergency Response Team of Ukraine (Команда реагування на комп'ютерні надзвичайні події України)

CIMIC – Civil-military cooperation (Цивільно-військове співробітництво)

CISA – Cybersecurity and Infrastructure Security Agency (Агентство з питань кібербезпеки та захисту інфраструктури)

CRA – Cyber Resilience Act (Акт про кіберстійкість (ЄС))

CREF – Cyber Resiliency Engineering Framework (Рамкова модель інженерії кіберстійкості)

CSIRT – Computer Security Incident Response Team (Команда реагування на інциденти комп'ютерної безпеки)

Cyber-CIMIC – цивільно-військове співробітництво у сфері кібербезпеки

DORA – Digital Operational Resilience Act (Акт про цифрову операційну стійкість)

DSB – Defense Science Board (Наукова рада з питань оборони)

ENISA – European Union Agency for Network and Information Security (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки)

EU – European Union (Європейський Союз)

IACS – International Association of Classification Societies (Міжнародна асоціація класифікаційних товариств)

ICWR – Інституту досліджень кібервійни

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія)

IoT – Інтернет речей

IOCTA – Internet Organised Crime Threat Assessment (Оцінювання загроз організованої злочинності в інтернеті)

ISACs – Information Sharing and Analysis Centers (Центри обміну та аналізу інформації)

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації)

NCW – Network-Centric Warfare (Мережецентрична війна)

NIS – Directive on Network and Information Security (Директива про мережеву та інформаційну безпеку (ЄС))

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій (США))

OSINT – Open Source Intelligence (Розвідка з відкритих джерел)

SCADA – Supervisory Control and Data Acquisition (Система диспетчерського управління та збору даних)

SOC – Security Operations Centers (Центри оперативної безпеки)

ВСТУП

Обґрунтування вибору теми дослідження. На сучасному етапі розвитку інформаційного суспільства спостерігається фундаментальне зміщення акцентів у стратегіях забезпечення кіберзахисту. Традиційна модель «кібербезпеки», зосереджена переважно на створенні непроникних бар'єрів та запобіганні вторгненням, демонструє обмежену ефективність перед обличчям складних багатовекторних кібератак. Визнання концепції «неминучості компрометації» зумовило появу та розвиток парадигми кіберстійкості. На відміну від статичного захисту, кіберстійкість визначається як здатність соціотехнічних систем передбачати, протистояти, відновлюватися та адаптуватися до несприятливих умов, стресів або активних нападів на цифрові ресурси.

Актуальність дослідження на світовому рівні підтверджується прийняттям засадничих актів, що в одних випадках прямо вказують на кіберстійкість, зокрема в ЄС – Акт Європейського Союзу про кіберстійкість (*EU Cyber Resilience Act – 2024*), а в інших – містять окремі розділи цього спрямування, зокрема у Великій Британії – Національна кіберстратегія та розділ у ній «Кіберстійкість» (*National Cyber Strategy (Cyber Resilience) – 2023*) та США – Американська кіберстратегія Президента Трампа (*President Trump's Cyber Strategy for America – 2026*), з включенням змістовних складових кіберстійкості, а також правовим врегулюванням у цій сфері безпекових стандартів NIST, MITRE і NIS2, що також націлюють на застосування цієї концепції та спрямовують на забезпечення життєздатності систем навіть у стані часткового ураження.

Для України актуальність розбудови національної кіберстійкості набуває особливої гостроти, що детерміновано безпрецедентною інтенсивністю кібератак у межах гібридної агресії. Специфіка сучасного протистояння свідчить, що об'єктами атак стають не лише окремі бази даних, а цілісні екосистеми надання державних послуг, енергетичні мережі та

транспортні комунікації. У цьому контексті кіберстійкість виступає критичним компонентом національної безпеки, оскільки вона гарантує безперервність функціонування органів державної влади та об'єктів критичної інфраструктури. Необхідність теоретичного осмислення та практичного впровадження засад кіберстійкості в Україні зумовлена потребою створення механізмів, які б дозволили мінімізувати час відновлення після інцидентів та забезпечили гнучкість управління ризиками в умовах високої невизначеності.

Водночас, інституціоналізація кіберстійкості вимагає перегляду наявних організаційно-правових засад, оскільки існуюче нормативне регулювання часто орієнтоване на реагування, а не на проактивне вибудовування стійких архітектур. Актуальність теми підсилюється необхідністю адаптації українського законодавства до вимог європейських стандартів, що передбачає запровадження жорстких вимог до кіберстійкості продуктів із цифровими елементами протягом усього їхнього життєвого циклу. Створення ефективної системи управління кіберстійкістю на державному рівні потребує чіткого нормативного визначення функцій суб'єктів кібербезпеки, розробки метрик оцінювання здатності до відновлення та формування культури розбудови стійкості.

Окремим аспектом актуальності є стрімка трансформація кіберзлочинності, яка дедалі частіше використовує вразливості людського фактора та складні схеми онлайн-шахрайства для підриву довіри до цифрових інституцій. Водночас, протидія кіберзлочинності є одним із ключових напрямів забезпечення кіберстійкості суспільства і з врахуванням вимоги щодо комплексності дослідження, потребує адекватного, саме на основі сучасних кримінологічних підходів, обґрунтування змісту та пріоритетів відповідної державної політики.

Кримінологічний аналіз сучасних загроз свідчить про глибоку інтеграцію зловмисних практик у соціальні мережі та хмарні сервіси. Забезпечення кіберстійкості за таких умов неможливе без розробки новітніх методологічних засад виявлення злочинної діяльності, зокрема через

використання аналітичної розвідки (OSINT) та впровадження відповідних правоохоронних стратегій (Intelligence-Led Policing, ІОСТА). Дослідження кримінологічних детермінант кіберзагроз дозволяє сформувати пріоритети стратегічної протидії злочинності, що є невід'ємною частиною загальної кіберстійкості держави та її громадян.

Водночас, динамічність кіберпростору робить традиційні статистичні методи малоефективними для довгострокового прогнозування. Потреба у використанні інтелектуальних методів аналізу, експертних оцінок для форсайту кіберзагроз та оцінювання ризиків, є нагальною науковою проблемою. Розробка прогнозних моделей стійкості дозволить здійснювати превентивні інвестиції в найбільш вразливі ділянки цифрового простору, забезпечуючи перехід від боротьби з наслідками інцидентів до управління потенціалом адаптації та сталого розвитку національної кіберсистеми.

Викладені вище обставини у своїй сукупності засвідчують актуальність теми дисертаційного дослідження.

Ступінь наукової розробленості проблеми. Низка проблемних питань такої широкої палітри наукового пізнання достатньо поглиблено досліджувалися у роботах вітчизняних і зарубіжних вчених. Зокрема, доктринальні положення та окремі аспекти адміністративно-правового й інформаційно-правового характеру щодо формування та реалізації державної політики були предметом вивчення таких вчених як: В. Авер'янов, О. Баранов, К. Беляков, Ю. Битяк, Л. Веселова, В. Галунько, В. Грохольський, А. Денисова, І. Діордіца, Д. Дубов, Д. Калаянов, Р. Калюжний, В. Колпаков, М. Корнієнко, О. Коропатов, О. Крижановська, А. Марущак, В. Пилипчук, В. Пядишев, Н. Свиридюк, В. Стефанюк, С. Тімченко, Т. Тур, Т. Фулей, І. Цюприк, Ю. Шемшученко, Х. Ярмакі та ін. Водночас, кримінологічний ризик-орієнтований базис, а також сучасний кримінологічний інструментарій, зокрема і у сфері кібербезпеки із застосуванням інформаційних технологій, були предметом вивчення таких вчених як: А. Бабенко, Д. Балобанова, В. Бутузов, В. Дрьомін, С. Зибін, С. Казмірчук, М. Карчевський, О. Користін,

В. Конопельський, М. Корнієнко, О. Корченко, О. Костенко, О. Литвак, В. Литвиненко, В. Меркулова, В. Підгородинський, Г. Собко, П. Фріс, О. Шкута та ін.

Серед зарубіжних вчених важливо виділити доктринальні дослідження саме на рівні пізнання суспільства ризику таких вчених як: У. Бек, Ф. Фукуяма, А. Гідденс, а також щодо формування кіберстійкості у сучасному безпековому кіберпросторі: Г. Тірмаа-Клаар, Д. Бодо, Н. Вайлдінг, Л. Геррінгтон, Б. Дюпон, С. Муйє, Р. Олдріч, М. Тонхаузер, Й. Ріствей, С. Хассілл, Р. Екмаср, В. Фумі, Ж-П. Кемар, Н. Полемі, Р. Румпель Келлі, С. Леверетт, Е. Оутон, Дж. Копік, С. Такер, Р. Пант, Л. Прайор, Г. Кассара, Т. Еван, С. Дж. Раффл, М. Тувесон, А. Коберн, Д. Ральф та Дж. В. Голлта багато інших.

Попри численні дослідження, правове регулювання кіберстійкості стало ключовим чинником нацбезпеки України. В умовах гібридної війни, де кібератаки супроводжують воєнні дії, розбудова такої системи є стратегічним пріоритетом для стійкості суспільства. Саме тому, обране дослідження спрямоване на удосконалення національної доктрини кібербезпеки на основі розробки організаційно-правових та кримінологічних засад кіберстійкості, що є критично важливою науковою та практичною проблемою. Поєднання компаративістики з методологією стратегічного аналізу на основі оцінки ризиків дозволяє сформувати дієвий механізм протидії сучасним кіберзагрозам та забезпечити сталий розвиток цифрового суспільства в Україні.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційного дослідження узгоджується з положеннями: 1) п. 4 розділу 1 та 47 розділу 3 Стратегії національної безпеки України (Указ Президента України від 14.09.2020 р. № 392/2020); 2) п.п. 4 та 5 Стратегії кібербезпеки України (Указ Президента України від 26.08.2021 р. № 447/2021); 3) п. 1.2 розділу II Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027

роки (Указ Президента України від 11.05.2023 р. № 273/2023); 4) п. 16 Плану заходів на 2025 рік реалізації Стратегії кібербезпеки України (Розпорядження КМУ від 07.03.2025 р. № 204-р); 5) п.п. 3, 7, 11, 13 Тематики наукових досліджень та науково-технічних (експериментальних) розробок на 2025–2029 роки (наказ МВС від 21.05.2024 р. № 326); 6) темою науково-дослідних робіт Одеського державного університету внутрішніх справ «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (номер державної реєстрації 0123U103538).

Тему дисертації затверджено рішенням Вченої ради Одеського державного університету внутрішніх справ (протокол № 2 від 27.01.2026 року).

Мета і завдання дослідження. *Метою* дослідження є висвітлення організаційно-правових та кримінологічних засад кіберстійкості України та визначення пріоритетних напрямів розвитку вітчизняного законодавства.

Для досягнення цієї мети потрібно розв'язати наступні *завдання*:

- дослідити генезис та еволюцію концепції «стійкості» у міждисциплінарному розрізі для визначення теоретичного підґрунтя кіберстійкості;
- розмежувати поняття «кібербезпека» та «кіберстійкість», обґрунтувавши перехід до нової парадигми захисту в умовах високої невизначеності з визначенням ключових спроможностей системи кіберстійкості;
- проаналізувати міжнародний досвід та стратегічні моделі розбудови кіберстійкості (на прикладі НАТО, ЄС, США та Великобританії) для формування концептуальних засад та практичних рекомендацій щодо створення національної системи кіберстійкості України;
- обґрунтувати інституціональну модель кіберстійкості як інтегровану систему взаємодії ринкових, стандартизаційних та регуляторних механізмів у забезпеченні стійкості національної кіберсистеми;

- здійснити функціональний аналіз суб'єктного складу національної системи кібербезпеки України, визначити роль державних органів у впровадженні інституційної моделі стійкості та оцінити рівень міжнародної інтеграції України у глобальний кібербезпековий простір;
- розробити та обґрунтувати концептуальні засади цивільно-військового співробітництва як системоутворюючого компонента національної кіберстійкості України;
- проаналізувати та визначити сучасний методологічний підхід щодо аналітичної розвідки стратегічних напрямів кіберстійкості через інтеграцію методів стратегічного форсайту, OSINT-моніторингу та ризик-орієнтованого аналізу;
- здійснити комплексний аналіз та ранжування ключових кіберзагроз за рівнем ризику їх поширення в Україні, для обґрунтування пріоритетних стратегічних напрямів розбудови національної кіберстійкості;
- обґрунтувати методологічні засади діагностики кіберстійкості національної інформаційної інфраструктури через розробку та апробацію інтегрованої матричної моделі, що поєднує цикли управління інцидентами (планування, поглинання, відновлення, адаптація) з операційними доменами системи (фізичним, інформаційним, когнітивним, соціальним);
- провести прикладний аналіз інституційної спроможності суб'єктів кібербезпеки України на основі ризик-орієнтованого підходу та розробити стратегічні правові орієнтири для подолання виявлених системних розривів;
- обґрунтувати методологічні засади кримінологічного аналізу кіберзлочинності в Україні, що базується на синергії ризик-орієнтованого підходу та інструментарію стратегічного аналізу;
- на основі емпіричного аналізу ідентифікувати ключові виклики кіберзлочинності та актуальний інструментарій вчинення злочинів;
- проаналізувати фінансову екосистему кіберзлочинності, інструменти анонімізації та комунікації зловмисників, а також роль міжсекторальних

факторів (соціальна інженерія, IoT) у формуванні сучасного ландшафту кримінальних загроз в Україні.

Об'єктом дослідження є суспільні відносини у сфері забезпечення кібербезпеки в Україні.

Предметом дослідження є організаційно-правові та кримінологічні засади кіберстійкості України.

Методи дослідження. Багатоаспектність предмета гносеології обумовлює необхідність застосування цілісної системи методологічного інструментарію, що включає в себе:

- *генетико-морфологічний аналіз* використаний у підрозділі 1.1 для дослідження історичного походження терміна «стійкість»;

- *компаративний аналіз* застосований для розмежування понять «кібербезпека» та «кіберстійкість» та порівняння класичної парадигми «кібербезпеки» з новітньою концепцією «кіберстійкості» (2.1); зіставлення євроатлантичних стандартів (Директива NIS2, моделі CIMIC НАТО) із поточною нормативною базою та практичним досвідом України (2.2, 2.3); аналізу міжнародних інструментів співпраці (4.3) та розробки пропозицій щодо гармонізації українського законодавства;

- *системний підхід* застосований для дослідження національної системи кібербезпеки як складного соціотехнічного комплексу (2.1-2.3);

- *функціонально-структурний аналіз* використаний у підрозділі 1.2 для декомпозиції життєвого циклу стійкості на окремі фази (передбачення, витримування, відновлення, адаптація); для розмежування повноважень суб'єктів кібербезпеки України відповідно до їхніх ролей у забезпеченні стійкості (2.2) та визначення специфічних функцій «цивільних асистентів» та «кіберрезерву» у системі оборони держави;

- *контент-аналіз нормативно-правової бази* використаний у підрозділі 1.3 для вивчення стратегій кібербезпеки України та провідних держав світу, а також критичного аналізу Закону «Про основні засади забезпечення кібербезпеки України» та Директиви NIS2 (2.3);

- *метод термінологічного аналізу та дефініції* використаний для уточнення понятійно-категоріального апарату, виявлення «термінологічного розриву» у чинному законодавстві та формулювання авторського визначення понять «інституціоналізація кіберстійкості» (2.1) та «Cyber-CIMIC» (2.3);

- *метод моделювання* застосовано для розробки теоретичної моделі багаторівневої взаємодії суб'єктів, побудови моделі «координаційного хабу» на базі НКЦК та моделі цивільно-військового співробітництва, що охоплює стратегічний, тактичний та операційний рівні (2.2, 2.3);

- *метод екстраполяції та прогнозування* застосовано для визначення перспектив розвитку національної системи кіберстійкості (2.2, 2.3, 3.1);

- *соціологічний аналіз* використаний для переосмислення природи кіберзагроз не лише як технічних проблем, а як соціальних ризиків, що дозволило обґрунтувати необхідність залучення громадян як активних суб'єктів кіберстійкості (розділ 3);

- *ризик-орієнтований метод* застосований як наскрізний інструмент для обґрунтування пріоритетності інвестицій у кіберстійкість та протидії кіберзлочинності (розділи 3, 4);

- *метод стратегічного управління* застосований для визначення пріоритетів державної політики у сфері кібербезпеки, що дозволило сформулювати ієрархію цілей: від захисту індивідуального користувача до гарантування безпеки критичної інфраструктури держави (розділи 3, 4).

Емпіричну основу дослідження складають: дані державної статистичної звітності – матеріали Офісу Генерального прокурора щодо зареєстрованих кримінальних правопорушень; статистичні відомості Державної судової адміністрації України; інформаційні та аналітичні матеріали Національного координаційного центру кібербезпеки РНБО України, Держспецзв'язку та Національної поліції України; дані експертних та соціальних опитувань щодо кіберзагроз та кіберстійкості національної системи кібербезпеки (1013 осіб, які представляють фахове середовище в центральних та місцевих органах влади, на об'єктах критичної інформаційної інфраструктури та правоохоронних

органах), а також щодо протидії кіберзлочинності (764 співробітників Департаменту кіберполіції НПУ).

Правову основу дослідження склали конституційні норми, міжнародно-правові акти (міжнародні конвенції, директиви ЄС тощо), нормативно-правові акти Верховної Ради України, Кабінету Міністрів України, Президента України, РНБО України, Держспецзв'язку України, Національної поліції України, Служби безпеки України, Офісу Генерального прокурора України тощо.

Наукова новизна отриманих результатів пояснюється тим, що дисертація є першим комплексним дослідженням, у якому системно висвітлюється концепт кіберстійкості як вищий рівень кібербезпеки України та сформульовано низку нових положень, зокрема:

вперше:

- сформульовано дефініцію національної кіберстійкості як динамічної емерджентної властивості соціо-кібернетичної системи, що інтегрує не лише технічні параметри захисту, а й когнітивні та організаційні аспекти адаптації до умов високої невизначеності;

- запропоновано концептуальну модель «спільної відповідальності» в межах національної екосистеми кіберстійкості, де держава виступає фасилітатором та ризик-менеджером, надаючи бізнесу інструменти самооцінки та розвідувальні дані в обмін на прозору звітність, а стійкість держави розглядається як похідна від здатності окремих суб'єктів критичної інфраструктури до самовідновлення;

- обґрунтовано трикомпонентну інституціональну модель кіберстійкості (маркетинг – стандартизація – регулювання) як цілісну систему формування та реалізації політики кіберстійкості, що дозволяє інтегрувати економічні, організаційні та правові механізми в єдину архітектуру кіберменеджменту;

- сформульовано концептуальну модель «Cyber-CIMIC» як специфічну форму цивільно-військового співробітництва в цифровому просторі, що, на відміну від класичної моделі CIMIC НАТО (орієнтованої на підтримку

військових операцій у фізичних доменах), розглядається як безперервний процес соціотехнічної взаємодії державних, військових та приватних акторів для забезпечення національної кіберстійкості;

- обґрунтовано необхідність запровадження інституту «цивільного кіберрезерву» та правового режиму «регуляторних пісочниць» у сфері кібероборони, що дозволяє легітимізувати участь недержавних суб'єктів у відсічі збройній агресії в кіберпросторі без обов'язкової комбатантизації за класичними ознаками;

- сформульовано концептуальну модель «Стійкість через право», яка базується на переході від декларативного характеру норм кібербезпеки до жорсткої юридичної фіксації необхідних функціональних спроможностей суб'єктів (передбачення, витримування, відновлення, адаптація);

- обґрунтовано концептуальну модель «інтелектуальної стійкості», яка розглядає аналітичну розвідку як цілісний процес трансформації первинних даних у стратегічні рішення через синергію OSINT як джерела актуальної фактологічної бази, форсайту як інструменту предиктивного моделювання альтернативних сценаріїв і «слабких сигналів» та ризик-орієнтованого підходу як механізму пріоритезації ресурсів, що у сукупності забезпечує перехід від реактивного захисту до проактивного управління життєздатністю критичної інфраструктури в умовах гібридної агресії;

- сформовано ієрархічну модель кіберзагроз для України, яка інтегрує технічні вразливості з деструктивними наслідками гібридної агресії та кібертероризму в єдиному розрахунковому полі ризиків;

- експериментально встановлено та математично підтверджено залежність між профілем професійного досвіду експерта (стаж <3, 3–10, >10 років) та суб'єктивною оцінкою рівня ризику специфічних кіберзагроз;

- розроблено та апробовано комплексну діагностичну матрицю кіберстійкості національної інфраструктури, яка дозволяє вимірювати нелінійні зв'язки між технічною стабільністю фізичного домену та ефективністю ухвалення рішень у когнітивній і соціальній сферах;

- обґрунтовано та емпірично підтверджено існування «безпекового розриву» між центральним та регіональним рівнями управління кібербезпекою України, що потребує переходу від уніфікованого до диференційованого правового регулювання;

- здійснено комплексне зіставлення експертних оцінок на основі ризик-орієнтованого підходу з статистичними даними ЄРДР, що дозволило виявити розбіжності у обліку кіберзлочинів (зокрема за ст. 362 ККУ) та обґрунтувати необхідність вдосконалення системи кодування злочинів у цифровій сфері;

- обґрунтовано та реалізовано стратегічний аналіз кіберзлочинності в Україні, що базується на інтеграції ризик-орієнтованого підходу та методології Europol ІОСТА, що передбачає не лише аналіз статистичних даних ЄРДР, а й обов'язкове залучення експертної думки;

- ідентифіковано та класифіковано специфічний інструментарій кіберзлочинців за рівнем поширеності в українському сегменті, зокрема встановлено домінування операційної системи Kali Linux та використання методів Брутфорс і DoS-атак як ключових засобів вчинення кіберзлочинів;

- на основі емпіричних даних обґрунтовано вплив анонімізації на ефективність правоохоронної діяльності через оцінку популярності VPN-сервісів та мережі Tor, а також прогнозування майбутніх ризиків їх використання як засобів приховування злочинної діяльності в умовах цифровізації.

удосконалено:

- теоретичне розмежування категорій «кібербезпека» та «кіберстійкість» у контексті державного управління, що полягає у трактуванні кіберстійкості не як технічного стану, а як динамічної інституційної спроможності системи до адаптації та самовідновлення, що потребує інтеграції в загальну стратегію корпоративного та державного управління;

- підхід до формування національної екосистеми кіберстійкості шляхом синтезу трьох складників: нормативної обов'язковості (досвід ЄС), технологічної адаптивності (досвід США) та соціотехнічної синергії (досвід

Великобританії), що дозволяє перейти від фрагментарного захисту до створення «колективного імунітету» держави;

- механізм інтеграції метрик кіберстійкості, на основі ризик-орієнтованого підходу, у загальну систему управління державними ризиками, що забезпечує перехід від кількісного підрахунку інцидентів до оцінки реальної готовності інфраструктури до відновлення;

- підхід до інституційного забезпечення кіберстійкості на національному рівні шляхом визначення функціональної моделі розподілу повноважень між суб'єктами кібербезпеки, що забезпечує комплексність, уникнення дублювання функцій та підвищення ефективності управління кіберризиками

- функціональну схему розподілу повноважень суб'єктів національної системи кібербезпеки, де, на основі аналізу чинного законодавства, чітко розмежовано вектори впливу: регуляторний (Держспецзв'язку), стандартизуючий (НКЦК як методологічний хаб) та стимулюючий (Мінцифра), що усуває дублювання функцій та підвищує керованість системи;

- понятійно-категоріальний апарат щодо змісту терміна «цивільно-військове співробітництво у сфері кібербезпеки», який на відміну від існуючих підходів, трактується не як ситуативна взаємодія, а як сталий правовий та організаційний механізм інтеграції ресурсів волонтерських ІТ-спільнот та приватного сектору до загальнодержавної системи кібероборони;

- організаційно-функціональну структуру взаємодії суб'єктів кібербезпеки, де роль Національного координаційного центру кібербезпеки (НКЦК) трансформована із суто дорадчого органу в стратегічний «комунікаційний хаб», що забезпечує вертикальну та горизонтальну сумісність військових і цивільних стандартів обміну інформацією;

- методологію стратегічного аналізу кіберзагроз через інтеграцію інструментарію OSINT у структуру ризик-менеджменту, що перетворює відкриті дані на верифіковані індикатори для розрахунку ймовірності та впливу загроз;

- класифікацію кіберзагроз у контексті ІІСО та гібридної війни, де кібератака розглядається не лише як технічний акт, а як інструмент маніпуляції суспільною довірою та дискредитації військово-політичного керівництва;

- модель міждоменної комунікації в кіберсистемах, де когнітивний домен визначено як ключовий чинник «живучості» системи через його здатність перерозподіляти інформаційні потоки у разі руйнування фізичних вузлів;

- типологію on-line шахрайства через диференціацію загроз із використанням платіжних карток (фішинг, вішинг) та без них (торгівля віртуальними товарами, криптовалютні махінації), що дозволяє правоохоронним органам точніше фокусувати оперативні ресурси;

- типологію засобів анонімізації злочинців, де в системному аналізі розмежовано використання комерційних VPN, власноналаштованих серверів та децентралізованих мереж;

- типологію фінансової активності кіберзлочинців через розмежування платіжних інструментів за рівнем ризику: від традиційних банківських переказів до використання криптовалют (Bitcoin, USDT) та систем електронних грошей (EasyPay, PayPal), що сприяє розробці ефективніших механізмів фінансового моніторингу;

- систему джерел кримінологічної інформації про on-line шахрайства, де окрім матеріалів кримінальних проваджень, враховано значну питому вагу довідково-аналітичних матеріалів (близько 30%), що дозволяє нівелювати вплив високої латентності цього виду злочинів.

дістали подальшого розвитку:

- міждисциплінарна теорія стійкості через адаптацію екологічних та інженерних принципів стійкості до специфіки функціонування сучасних кіберфізичних систем та ІТ-мереж;

- теоретичні підходи до розуміння кіберстійкості як складної адаптивної системи, в якій ключову роль відіграє не сукупність заходів, а їх узгодженість,

пріоритезація та здатність до динамічної трансформації в умовах невизначеності;

- концепція міжнародної суб'єктності України в глобальному кіберпросторі на основі подальшого розвитку та трансформації України з реципієнта міжнародної технічної допомоги у ключового донора унікального практичного досвіду для країн НАТО та ЄС, що легітимізує національні безпекові протоколи як основу для майбутніх міжнародних стандартів колективної стійкості;

- підходи до гармонізації національного законодавства із євроатлантичними вимогами, зокрема в частині адаптації стандартів ISO/IEC 27000 та положень Директиви NIS2, що забезпечує інституційну сумісність України з міжнародними мережами реагування на інциденти;

- наукові підходи до формування мережевої моделі кібероборони, що базується на принципах функціональної комплементарності та розподіленої відповідальності, що дозволяє ефективно масштабувати спроможності держави за рахунок гнучкого залучення цивільного інтелектуального капіталу в умовах гібридної війни;

- методика багаторівневої фільтрації експертних даних у сфері кібербезпеки на основі «тесту на логічну узгодженість», що дозволило статистично значущо підвищити надійність прогностичних моделей розвитку кіберзагроз;

- використання методів інтелектуального аналізу даних для моніторингу регіональних та галузевих особливостей поширення кіберризиків в Україні;

- кримінологічна теорія мотивації кіберзлочинців, доповнена факторами «гібридної війни» та «колабораційної співпраці», що виходить за межі класичного корисливого мотиву;

- кримінологічна характеристика способів комунікації в кіберпросторі, яку доповнено порівняльним аналізом використання месенджерів (Telegram – 66%, WhatsApp – 56,3%, Viber – 52,3%) як основних каналів взаємодії між

злочинцями та жертвами, а також прогнозуванням ризиків їх використання у післявоєнний період;

- розуміння впливу технологічних чинників на ландшафт кіберзлочинності, зокрема щодо експлуатації вразливостей Інтернету речей (IoT) для створення ботнетів та проведення DDoS-атак, що розглядається як критична загроза для стабільності цифрової інфраструктури в умовах масової цифровізації;

- теоретичні засади протидії соціальній інженерії, які розширено через аналіз динаміки поширення методів фішингу, вішингу та смішингу, а також обґрунтування того, що людський фактор залишається найбільш критичною ланкою в системі забезпечення кіберстійкості держави.

Практичне значення отриманих результатів. Загальні положення дослідження, отримані висновки та обґрунтовані пропозиції використані та можуть у подальшому бути використані за такими напрямками:

- *науково-дослідна робота* – для наукових розробок проблемних аспектів окремих напрямів удосконалення кібербезпеки та формування національної системи кіберстійкості в Україні (акт впровадження в наукову діяльність Одеського державного університету внутрішніх справ від 15.01.2026 року);

- *правотворча діяльність* – для удосконалення законодавства, що регулює відносини у сфері кібербезпеки (довідка №89д9/10-2025/251968 від 03.11.2025 про впровадження у діяльності ВРУ при розробленні законопроекту № 12207 «Проект Закону про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки»);

- *правозастосовна діяльність* – для впровадження моделі стійкого правопорядку, що забезпечує перехід від констатації вчинених злочинів до проактивного виявлення латентних загроз та ідентифікації складних кримінальних схем, та передбачає вдосконалення координації суб'єктів національної системи кібербезпеки через автоматизований обмін даними про

аномальну активність у реальному часі; методологія аналітичної розвідки має базуватися на інтеграції алгоритмів машинного навчання та предиктивного аналізу великих даних для виявлення транскордонних злочинних мереж, задіяних у гібридній війні, що посилює кіберстійкість суспільства шляхом підвищення інституційної спроможності органів правопорядку, впровадження стандартів безпеки на етапі проектування систем та мінімізації економічної привабливості кіберзлочинності;

– *освітній процес* – при викладанні навчальних дисциплін «Кримінально-правова та кримінологічна характеристика кіберзлочинності», «Інформаційна та кібернетична безпека», «Кримінальний аналіз», «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції», «Протидія кіберзлочинності», при підготовці відповідних розділів підручників, навчальних посібників, програм, проведенні занять з професійної підготовки працівників оперативних підрозділів Національної поліції України (акт впровадження в освітній процес Одеського державного університету внутрішніх справ від 15.01.2026 року).

Апробація матеріалів дисертації. Основні положення дисертації апробовано на: XIV Міжнародній науково-практичній конференції «Безпекотворення: питання теорії, практики та правові аспекти» (м. Київ, 06 квітня 2023 р.), XV міжнародній науково-практичній конференції «Закарпатські правові читання» (м. Ужгород, 27 квітня 2023 р.), III Міжнародній науково-практичній інтернет-конференції з нагоди відзначення Дня науки – 2023 в Україні «Актуальність та особливості наукових досліджень в умовах воєнного стану» (м. Київ, 23 травня 2023 р.), науково-практичному круглому столі «Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення» (м. Київ, 26 вересня 2023 р.), X Міжнародній науково-практичній інтернет-конференції «Стан та перспективи розвитку адміністративного права України» (м. Одеса, 20 жовтня 2023 р.), міжвідомчій науково-практичній конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, 17

листопада 2023 р.), Міжнародній науково-практичній конференції «Кібербезпека в Україні: правові та організаційні питання» (м. Одеса, 17 листопада 2023 р.), Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks «Management in Global Information Networks» (м. Велятино, 25 січня 2024 р.), Всеукраїнській науково-практичній конференції «Актуальні питання забезпечення безпекового середовища в Україні» (м. Київ, 19 квітня 2024 р.), IV Міжнародній науково-практичній інтернет-конференції з нагоди відзначення Дня науки-2024 в Україні «Актуальність та особливості наукових досліджень в умовах воєнного стану» (м. Київ, 22 травня 2024 р.), Всеукраїнській науково-практичній конференції «Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки» (м. Київ, 27 вересня 2024 р.), Міжнародній науково-практичній конференції «Протидія організованих злочинності і корупції в умовах збройного конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ» (м. Кропивницький, 04 жовтня 2024 р.), Міжвідомчій науково-практичній конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, 01 листопада 2024 р.), круглому столі «Роль OSINT-досліджень у підвищенні рівня національної безпеки України» (м. Львів, 07 травня 2025 р.), Міжнародній науково-практичній конференції «Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів» (м. Одеса, 23 травня 2025 р.), Київському міжнародному форумі кіберстійкості (м. Київ, 19-20 лютого 2026 р.).

Публікації. Основні положення дисертації опубліковані в 33 наукових працях, з яких: 2 – одноосібні розділи колективних монографій, 18 – наукові статті в фахових виданнях (з яких 5 – у періодичних виданнях іноземних держав (фахові видання, включені до наукометричних баз Scopus, зокрема 2 – Q3 і 1 – Q1) та Web of Science), 13 – тези доповідей.

Особистий внесок. Дисертаційна робота виконана здобувачем самостійно. Викладені у дисертації положення, що виносяться на захист,

розроблені ним особисто. У наукових працях, опублікованих у співавторстві, особистий внесок полягає у наступному:

- Demedyuk S.V., Demedyuk T.S. Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. 2018. Vol. 68 № 6. P. 278-290 (досліджено кримінально-правовий контент насильства над дітьми в інтернеті);

- Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Set Theory. *International Journal of Computer Network and Information Security*. 2024. Vol. 16. №. 1. P. 24-34 (сформовано та проаналізовано емпіричний матеріал дослідження, розкрито методологічні засади дослідження);

- Korystin O., Demediuk S., Sviridyuk N., Mitina O., Aleksander M., Yuriy Kardashevsky. Risk Forecasting of Information-content-security. *Cyber Hygiene & Conflict Management in Global Information Networks: Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks*. 2025. Vol. 3925. P. 273–280 (сформовано емпіричний матеріал дослідження, проаналізовано ризики поширення кіберзагроз та визначено пріоритетними ризики, пов'язані з інформаційною безпекою);

- Korystin O., Demediuk S., Likhovitsky Y., Kardashevsky Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns, *International Journal of Information Technology and Computer Science*. 2025. Vol. 17. No. 2. P. 24-35 (розкрито сутність окремих кіберзагроз, на основі інтерпретації статистичних та аналітичних даних обґрунтовано пріоритети стратегічного розвитку системи кібербезпеки в Україні);

- Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*. (2025). Vol. 17. Is. 19. P. 8757 (сформовано емпіричний матеріал дослідження кібербезпеки

критичної інформаційної інфраструктури, проаналізовано ризики та виділено пріоритетні кіберзагрози);

- Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона*. 2023. № 1(59). С.77-85 (досліджено методологічні засади та досвід і стандарти НАТО у сфері забезпечення кіберстійкості);

- Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59 (досліджено методологічні засади ІОСТА за матеріалами Європолу та інтерпретовано аналітичні висновки за окремими особливостями в описових статистиках);

- Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет»*. 2023. №06. С. 708-713 (проаналізовано окремі аспекти дослідженості концепції «стійкість» та щодо обґрунтування актуальності її розбудови в Україні);

- Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154 (проаналізовано ризики та інтерпретовано отримані статистичні результати й аналітичні висновки, що характеризують сучасні тенденції поширення on-line шахрайства в Україні).

Структура та обсяг дисертації визначені її метою і завданнями. Робота складається зі списку умовних позначень, анотації, вступу, чотирьох розділів, які об'єднують тринадцять підрозділів, висновків, списку використаних джерел (424 найменування на 49 сторінках), 4 додатків на 42 сторінках. Повний обсяг дисертації складає 525 сторінок, з яких основний текст – 412 сторінок.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ РОЗБУДОВИ НАЦІОНАЛЬНОЇ КІБЕРСТІЙКОСТІ

1.1. Актуалізація кіберстійкості та історичні витoki концепції «стійкість»

Витонченість та зростаючі частота й інтенсивність кібератак, спрямованих на установи у кіберпросторі, підкреслюють їх високу ризиковість та складність повноти захисту цілісності критично важливих об'єктів та систем. У цьому контексті кіберстійкість пропонує привабливу додаткову альтернативу існуючій парадигмі кібербезпеки.

Концепт кіберстійкості є результатом тривалого наукового пошуку та розвитку більш загальної концепції «стійкість», з різним досягненням та сприйняттям різноманітними науковими школами та широкої низки галузей та сфер суспільного буття. Тому важливо проаналізувати міждисциплінарні засади, що стосуються вивчення кіберстійкості, щоб зрозуміти як її численні виміри, так і критерії, які можуть бути використані для полегшення її впровадження та вимірювання. Для досягнення цієї мети варто звернути увагу на численні значення стійкості через її використання в різних дисциплінах, вказуючи на теоретичні аспекти, які є особливо актуальними для кібербезпеки.

Етимологічне коріння терміну «стійкість» сягає латинського дієслова «resilire», що буквально означає «відскакувати назад», «відбиватися» або «повертатися у вихідний стан» [152, с. 2]. В історичній ретроспективі це поняття тривалий час використовувалося переважно в матеріалознавстві та класичній механіці для опису властивості фізичних тіл поглинати енергію при деформації та відновлювати свою первісну форму після припинення зовнішнього тиску.

Однак у другій половині XX сторіччя зміст терміну зазнав суттєвої еволюційної трансформації, що була зумовлена ускладненням соціальних та технологічних процесів.

Наукові концепції стійкості сягають корінням у фізику та матеріалознавство, де стійкість позначає властивість матеріалу поглинати енергію, коли він піддається деформації, і зберігати або відновлювати свою початкову форму або положення після згинання, розтягування або стискання [63, 345]. У розширеному розумінні це значення застосовується в медичній та ветеринарній науках для визначення природної еластичності частин тіла, таких як шкіра, легені або грудна клітка. У цьому контексті стійкість відноситься до обмеженого набору вимірюваних параметрів, які визначаються їхньою передбачуваністю і мало змінюються в часі та просторі. У 1970-х роках ця концепція стала більш привабливою, особливо в межах двох дисциплін, які спричинили її нинішню популярність - екології та психології [63, с. 710].

Перехід від загальнофілософського та етимологічного розуміння стійкості до її наукової формалізації відбувся у 1970-х роках, насамперед у межах екології та теорії систем. Фундаментальний зсув у науковій парадигмі пов'язаний із працями канадського еколога Кроуфорда Стенлі Голлінга, який у 1973 році запропонував розрізняти два типи стійкості, що згодом стали основою для проектування будь-яких критичних інфраструктур, включаючи цифрові.

Голлінг запропонував розмежувати «інженерну» та «екологічну» стійкість. Цей поділ є критично важливим для розуміння сучасної кіберстійкості.

Згідно з підходом К. Голлінга [63, с.710; 280; 281] *інженерна стійкість* (engineering resilience) фокусується на стабільності поблизу стану рівноваги. Вона вимірюється швидкістю, з якою система повертається до свого первісного стану після зовнішнього збурення. Цей підхід домінував у класичній інженерії та ранній кібернетиці, де ідеалом вважалася система з

високим рівнем передбачуваності та мінімальними відхиленнями від норми [269, с. 499]. Проте Голлінг зауважив, що така «стабільність» може бути оманливою: прагнення зробити систему максимально жорсткою та захищеною від будь-яких змін часто робить її крихкою перед обличчям непередбачуваних, катастрофічних впливів.

Натомість екологічна стійкість (ecological resilience) визначається як здатність системи поглинати зміни та потрясіння, зберігаючи при цьому базову структуру та функції. Тут акцент зміщується з ефективності на витривалість. Екологічно стійка система не обов'язково швидко повертається до попереднього стану, вона може змінювати свій стан, адаптуватися, переходити у нові режими функціонування, але вона продовжує виконувати свою місію. У термінах системної інженерії це породило перехід від філософії «fail-safe» (проектування систем, що не ламаються) до «safe-to-fail» (проектування систем, що ламаються безпечно та продовжують функціонувати в обмеженому режимі) [351, с. 361]. Саме цей підхід став ідейним прообразом «стійкості кіберсистем», де головною метою є не відсутність інцидентів (що у сучасному світі неможливо), а здатність продовжувати операції у скомпрометованому середовищі.

В екології основоположна стаття Голлінга представила більш динамічне розуміння поняття стійкості, застосовуючи його до ситуацій коли система стикається з глибокими та неочікуваними змінами не може, на відміну від матеріалів, підтримувати постійний стан рівноваги [280, с. 3-4]. Натомість Голлінг стверджував, що вивчення стійкості має зосередитися на «стійкості систем та їхній здатності поглинати зміни і збурення, зберігаючи при цьому незмінними взаємозв'язки між популяціями або змінними стану» [63, с 710; 280, с. 3-4]. На практиці персистентність є протилежністю стабільності, яка означає здатність системи повертатися до стану рівноваги після збурення. Персистентність, наприклад, може бути досягнута у випадках екстремальних коливань чисельності популяції і забезпечує меншу ймовірність її вимирання порівняно з популяціями, які є більш стабільними, але менш гнучкими у своїй

здатності поглинати екстремальні зміни навколишнього середовища. Важливо пам'ятати, що такий погляд на стійкість є характерним для екології, де, на відміну від організацій, головною метою не є обов'язковим максимізувати ефективність, а просто залишитися в грі. Коли ця концепція переноситься в організаційне середовище, вона створює напруженість, оскільки, на відміну від стійких екологічних систем, які покладаються на різноманітність і мінливість, гомогенність, яка сприяє організаційній ефективності, не терпить високих коливань, а отже, демонструє меншу стійкість. У наступній статті, Голлінг формалізував свої міркування щодо ознак – ефективності, постійності та передбачуваності – які відрізняють інженерну (або економічну) стійкість від екологічної стійкості, яка зосереджена на стійкості, змінах і непередбачуваності [63, с 711; 281]. Виходячи за межі теоретичних тонкощів одно- та багатостабільних рівноваг, практичним наслідком цього напрямку міркувань є те, що ефективність і стійкість не завжди узгоджуються між собою. Умови, які призводять до короткострокової економічної продуктивності (наприклад, зменшення різноманітності і надмірність, які дозволяють досягти економії на масштабах і оптимізації ресурсів), можуть бути шкідливими для стійкості і підвищувати вразливість [281, с. 33–34]. Хоча Голлінг не мав наміру узагальнювати свою роботу за межами управління екологічними системами, його розуміння є важливим для осіб, які приймають рішення в інших сферах, які повинні усвідомлювати, що досягнення стійкості вимагає від них балансу між суперечливими пріоритетами. Його новаторський внесок знайшов відгук, зокрема, серед екологів, містобудівників та експертів з управління катастрофами, які розширили їх для концептуалізації та картографування адаптаційних стратегій, доступних для сучасних суспільств та їхніх складних, але крихких соціально-технічних систем, з особливим акцентом на катастрофічні наслідки прискореної зміни клімату [217; 229]. Дехто навіть стверджує, що ця концепція є настільки універсальною і стала настільки помітною, що «вона допомогла уніфікувати екологію як дисципліну» [63; 346].

Психологія є другою дисципліною, яка зробила значний внесок у популяризацію стійкості. У 1970-х роках, коли екологія розглядала стабільність, стійкість і адаптацію екологічних систем, психологія намагалася зрозуміти, чому деякі люди і сім'ї, які опинилися в зоні ризику або зіткнулися з широким спектром несприятливих обставин (таких як бідність, розпад сім'ї, травматична втрата або стихійне лихо), здаються відносно не зачепленими і здатні впоратися з ними і нормально функціонувати [329], а в деяких випадках стають навіть сильнішими [412]. Психологія розробила концепцію життестійкості як спосіб вийти за межі своєї природної тенденції зосереджуватися на факторах ризику та їхніх негативних наслідках для психічного здоров'я, розширивши свої перспективи до вивчення особистісної сили, позитивних форм адаптації, пом'якшувальних факторів та захисних впливів [329; 369]. Річардсон виокремлює три хвилі психологічних досліджень життестійкості [369]. Перша хвиля визначила особистісні характеристики та захисні фактори, які підтримують людей під час несприятливих життєвих подій, створивши довгий список індивідуальних, сімейних, громадських та культурних факторів, таких як самооцінка, ефективність, навички вирішення проблем, турбота, гумор або теплі особисті стосунки, якщо назвати лише деякі з них [412]. Друга хвиля намагалася зрозуміти, як ці якості набуваються, тоді як третя хвиля намагалася змодельовати силу або мотивацію, яка спонукає людину до розвитку або посилення цих якостей [63, с. 711].

Ці дослідження стали інструментом у розвитку позитивної психології, яка відмовляється від патологізації ризиків на користь більш цілісного підходу, в якому розуміється, що найнесприятливіші ситуації можуть дозволити людям процвітати і знаходити креативні рішення [378, с. 9]. Така перспектива може бути відкинута як занадто оптимістична для суворих реалій нашого складного світу, але, навпаки, психологічні дослідження виявили, що життестійкість трапляється набагато частіше, ніж прийнято вважати. Основним висновком є те, що життестійкість – це далеко не виключна сфера

компетенції невеликої групи «невразливих» або «непереможних» людей, є дуже поширеним набором здібностей і практик, які демонструє значна частина населення [63; 173; 369; 414]. Психології вдалося демістифікувати надзвичайну силу життєстійкості та виділити її «звичайну магію» [328].

Третя, більш розрізнена, група вчених, які вивчали управління катастрофами та стійкість міст, також знайшла концепцію стійкості дуже привабливою.

Історична актуалізація цього терміну на початку ХХІ століття пов'язана із концепцією «суспільства ризику» [160] де неможливо прорахувати всі сценарії загроз. Отже, єдиним раціональним шляхом забезпечення безпеки стає розбудова внутрішньої стійкості, яка дозволяє системі бути готовою до «невідомих невідомих» (unknown unknowns). Це робить стійкість центральною категорією не лише технічних наук, а й стратегічного менеджменту та національної безпеки, де здатність до швидкого відновлення критичних послуг є пріоритетнішою за будь-які статичні бар'єри.

У «суспільстві ризику», в якому ми живемо [160], антропогенні фактори спричиняють дедалі частіші та сильніші стихійні лиха (посухи, пожежі, повені, спеку), які є надзвичайно руйнівними і впливають на наші складні технологічні та міські системи. Крім того, «штучні ризики», категорія ризиків, створених наукою і технікою і щодо яких є обмеженими знання, стали повсюдними [255, с. 2]. Штучні ризики, такі як фінансові крахи, ядерні катастрофи, розливи нафти чи скандали у сфері охорони здоров'я, зазвичай розгортаються в глобальному масштабі і завдають надзвичайної шкоди. Враховуючи такий радикально ворожий і невизначений контекст, не дивно, що дослідники як антропогенних, так і техногенних ризиків прийняли концепцію стійкості. Зокрема, у розробці та застосуванні концепції стійкості були задіяні дві сфери, що перетинаються, а саме: стійкість міст та стійкість до стихійних лих. У той час як перша стосується спроможності міст протистояти широкому спектру стресів і потрясінь, друга фокусується на конкретних великомасштабних несприятливих подіях і на тому, як з ними справляються

організації та місцеві громади. Обидва напрями висвітлені у численних публікаціях, в яких варто виділити два висновки [63, с. 712].

По-перше, складні організації та соціоекологічні системи по-різному інтерпретують поняття стійкості, залежно від рівня їхньої зрілості. На базовому рівні стійкість передбачає спроби зберегти статус-кво і зменшити виникнення або вплив збурень шляхом поглинання, тоді як більш адаптивна форма стійкості спирається на здатність до самоорганізації та прийняття нових практик без шкоди для структури та функцій. Найбільш просунутою формою стійкості є трансформаційна, яка передбачає перехід до нового набору функцій, структур, зворотного зв'язку та результатів, які краще відповідають мінливому середовищу [217]. Друге розуміння полягає в тому, що неможливо зрозуміти – і, відповідно, сприяти підвищенню – стійкості складних систем, не звертаючи уваги на міжмасштабну взаємодію між низкою географічних, часових, функціональних і технологічних вимірів [150]. Обидва висновки видаються особливо актуальними для нової сфери кіберстійкості [63, с. 712].

Подальша інтеграція концепції стійкості у науковий обіг відбувалася через її глибоке переосмислення в межах теорії надійності та сучасного ризик-менеджменту. Протягом останніх десятиліть стало очевидним, що традиційні підходи до управління ризиками, які базуються на лінійній детермінації та спробах нівелювати ймовірність настання негативної події, вичерпують свій ресурс у складних, взаємопов'язаних системах [153].

Протягом 1980-х та 1990-х років стало очевидним, що традиційний аналіз ризиків, який базується на формулі *«ймовірність × наслідки»*, виявляється неспроможним у складних взаємопов'язаних системах (Normal Accidents за Ч. Перроу [356, с. с. 205]). Складність сучасних технологічних систем (зокрема енергомереж, транспортних вузлів та інформаційних магістралей) породжує каскадні ефекти, де локальний збій може призвести до системного колапсу [323, с. 473].

У цьому контексті стійкість почала розглядатись як четверта лінія оборони після запобігання, захисту та пом'якшення наслідків. Як

підкреслюють зарубіжні вчені [174, с. 20], стійкість у цивільній інфраструктурі вимагає не лише технічних рішень, а й організаційної гнучкості. Управління катастрофами (disaster management) запозичило у психології та соціології розуміння того, що стійкість системи значною мірою залежить від її здатності до самоорганізації та наявності надлишкових ресурсів (redundancy).

Ключовим поштовхом до зміни фокусу з «ризиків» на «стійкість» стала праця Ч. Перроу про «нормальні аварії» (Normal Accidents), де обґрунтовано, що у високотехнологічних системах з жорсткими зв'язками локальні збої є неминучими і, в силу каскадного ефекту, призводять до системних катастроф [356, с. 203]. Це усвідомлення змусило наукову спільноту шукати відповідь не у питанні «як запобігти аварії?», а у площині «як вижити та відновитися, коли аварія вже сталася?». Відтак, стійкість почала розглядатись як динамічна характеристика, що дозволяє системі зберігати функціональність навіть за умови часткового руйнування [157].

Розвиток теорії ризиків продемонстрував, що стійкість є вимірюваною величиною. Концепція «трикутника стійкості» (resilience triangle) дозволила візуалізувати втрату функціональності системи після удару та траєкторію її відновлення [324]. Це заклало математичне підґрунтя для сучасних метрик кіберстійкості, де час відновлення (Recovery Time Objective) та точка відновлення (Recovery Point Objective) стали базовими показниками ефективності стратегій безпеки.

Таким чином, важливим внеском у теорію ризиків стала розробка метрик стійкості, що базуються на аналізі часових та ресурсних витрат на відновлення. На відміну від класичної надійності, яка оперує середнім часом між відмовами (MTBF), стійкість акцентує увагу на траєкторії відновлення (resilience triangle) – зоні між нормальним рівнем функціонування системи та її деградованим станом після удару [324, с. 473]. Що меншою є площа цієї зони, то вищою вважається стійкість системи. Ця концепція дозволила формалізувати стійкість як вимірювану величину, що є критичним для

прийняття управлінських рішень у сфері національної безпеки та захисту критичної інфраструктури [174].

Окремої уваги заслуговує соціотехнічний аспект еволюції ризиків. Управління катастрофами (disaster management) запозичило у психології та соціології розуміння того, що стійкість системи значною мірою залежить від її здатності до самоорганізації та наявності надлишкових ресурсів (redundancy). Як стверджує Я. Хаймс [269, с. 498], стійкість не є альтернативою управлінню ризиками, а є його вищим рівнем, що враховує фактори невизначеності та «чорних лебедів». У складних інфраструктурах, таких як енергомережі чи цифрові магістралі, стійкість забезпечується через децентралізацію та автономність окремих вузлів, що запобігає повному системному колапсу при ураженні одного з них.

На зламі тисячоліть концепція стійкості остаточно трансформувалася у стратегічну категорію державної політики. Зокрема, у звітах National Research Council [225] підкреслюється, що стійкість – це національний імператив, який вимагає переходу від культури «реагування на події» до культури «постійної адаптивності». Це заклало ідейний фундамент для виникнення власне «кіберстійкості», де цифрові активи розглядаються не як статичні об'єкти захисту, а як динамічні середовища, що перебувають у стані постійної боротьби за виживання та розвиток [165, с. 47].

Таким чином, еволюція поняття у контексті теорії ризиків продемонструвала неспроможність суто превентивних методів у волатильному середовищі. Стійкість стала науковою відповіддю на складність сучасного світу, запропонувавши інтегрований підхід, де здатність до швидкого відновлення та навчання на помилках стає головним показником успішності системи.

Важливим етапом стала формалізація поняття *абсорбційної спроможності* технічних систем. У роботах Я. Хаймса [269, с. 499] доводиться необхідність переходу від аналізу ймовірності відмови до аналізу здатності системи до «граціозної деградації» (graceful degradation) – здатності

відключати другорядні функції для порятунку життєво важливого ядра [153, с. 3; 269]. Це означає, що при отриманні критичних пошкоджень система не припиняє роботу миттєво, а відключає другорядні функції, зберігаючи працездатність життєво важливого ядра. Такий підхід став ключовим для сучасного розуміння кіберстійкості, де ізоляція зараженого сегмента мережі дозволяє зберегти контроль над усією інфраструктурою. У фундаментальних дослідженнях ризиків Я. Хаймс зазначає [269, с. 499], що стійкість є невід’ємним доповненням до вразливості: якщо вразливість вказує на «слабкі місця» системи, то стійкість визначає її «життєву силу» та здатність до відновлення після того, як ці слабкі місця були експлуатовані. Це зумовлює перехід від стратегій «запобігання відмовам» до проактивних стратегій «забезпечення виживання при відмовах» [174, с.22].

Варто зауважити, що у межах системного підходу стійкість часто протиставляється крихкості. Якщо крихка система руйнується повністю при досягненні критичного порогу навантаження, то стійка система демонструє властивість «граціозної деградації» – поступового зниження якості функцій при збереженні найбільш життєво важливих вузлів [252]. Як зазначають дослідники [165] у соціальних та психологічних контекстах стійкість – це не просто відсутність патології після травми, а активний процес підтримки нормального функціонування.

На початку ХХІ сторіччя, особливо після подій 11 вересня та низки масштабних техногенних аварій, концепція стійкості остаточно вийшла за межі академічних дискусій і стала частиною національних стратегій безпеки провідних країн світу. Зокрема, у США Presidential Policy Directive 21 (Директива президента США №21 «Безпека та стійкість критичної інфраструктури») визначила стійкість як здатність готуватися до адаптації до змінних умов, а також протистояти та швидко відновлюватися після збоїв [225].

Розглядаючи етимологію «стійкості» (англ. resilience) та міждисциплінарний характер, важливо зазначити щодо трансформації цього

терміну з вузькоспеціалізованого екологічного, технічного, біологічного, медичного та психологічного тощо терміну на фундаментальну міждисциплінарну парадигму, що визначає стратегію виживання складних систем у критичних умовах.

У другій половині XX сторіччя зміст терміну «стійкість» зазнав суттєвої еволюційної трансформації. Сучасна наукова думка розглядає стійкість не просто як статичну опірність матеріалу, а як динамічну здатність системи до збереження функціональної цілісності [269, с. 499], що обґрунтовано адаптується і до сфери безпеки інформаційних систем – перехід від статичних моделей захисту до динамічних стратегій виживання. Як зазначається у наукових розвідках щодо актуалізації кіберстійкості та її історичних витоків, поняття стійкості не є продуктом суто цифрової епохи, а має глибоке міждисциплінарне коріння [63].

Тривалий час у матеріалознавстві та класичній механіці стійкість розглядалася як пасивна здатність матеріалу поглинати енергію деформації. Однак системне ускладнення людської діяльності у другій половині XX сторіччя вимагало розширення цієї дефініції. Сьогодні стійкість трактується як інтегральна здатність складних соціотехнічних систем не лише протистояти зовнішнім шокам, а й зберігати функціональну цілісність в умовах тривалого деструктивного впливу. Міждисциплінарність терміну виявляється у тому, що він став спільним знаменником для екології, психології, інженерії та кібернетики, де ключовим є питання виживання системи у критичних фазах її життєвого циклу. Спільним знаменником для всіх цих сфер є фокус на поведінці системи в моменти екстремального стресу, коли традиційні методи захисту виявляються недостатніми або повністю нівелюються [324, с. 473].

Таким чином, у загальнонауковому розумінні стійкість характеризується як системна властивість, що дозволяє суб'єкту (об'єкту) протистояти деструктивному впливу та повертатися до стабільного функціонування. Центральним елементом цієї характеристики є не лише швидкість відновлення, а й здатність системи до адаптації – тобто

трансформації внутрішньої структури для запобігання подібним кризам у майбутньому [232, с. 6].

Тож, поняття «стійкість» (англ. *resilience*) на сучасному етапі наукового дискурсу трансформувалося з вузькоспеціалізованого технічного терміну на фундаментальну міждисциплінарну парадигму, що визначає стратегію життєздатності складних систем у критичних умовах.

У кібервимірах концепція *resilience* тісно переплітається з поняттям живучості (*survivability*). Згідно з підходами MITRE (2013–2018), стійкість системи не є бінарним станом (стійка/нестійка), а є континуумом спроможностей, які вимірюються через здатність передбачати загрози, витримувати їхній вплив, відновлювати сервіси та адаптувати архітектуру. Це дозволяє стверджувати, що стійкість є динамічною характеристикою, яка потребує постійного управління та інвестицій.

Це заклало підґрунтя для формування сучасних інженерних фреймворків, таких як CREF (Cyber Resiliency Engineering Framework) від корпорації MITRE. Історичний досвід екології навчив нас, що статичний захист – це шлях до стагнації та вразливості, тоді як динамічна адаптивність є єдиним способом забезпечити довгострокове виживання в агресивному та мінливому середовищі [165].

Таким чином, генезис концепції стійкості демонструє послідовний рух від вивчення фізичних властивостей матерії до створення складних адаптивних стратегій управління глобальними ризиками. Сучасна кіберстійкість є прямим спадкоємцем екологічної стійкості Голлінга, адаптованою до цифрових швидкостей та масштабів сучасного світу.

Кіберстійкість останнім часом стала однією з найбільш розкручених концепцій в дискусіях про кібербезпеку, незважаючи на її розпливчасте значення, що ускладнює її точне визначення та вимірювання, а можливо, і завдяки йому. Її популярність, безсумнівно, пов'язана з численними заголовками про кібератаки і витоки даних, які рясніють на перших шпальтах ЗМІ і веб-сайтах, повідомляючи про нові і масові зломи, що свідчать про

вразливість цифрових інфраструктур і нездатність організацій захистити персональні дані, які ми їм довіряємо. Навіть найбільш технічно підковані та обізнані в питаннях безпеки організації не застраховані від катастрофічних збоїв у кібербезпеці [63, с. 710].

Свого часу, у жовтні 2017 року газети New York Times і Washington Post опублікували історію прямо з роману Джона Ле Карре, в якій повідомлялося, що ізраїльські шпигуни проникли в системи компанії з кібербезпеки «Касперський» і ніби-то змогли відстежувати хакерські дії своїх російських колег, які використовували телеметричні можливості антивірусного продукту компанії для пошуку конфіденційних документів американських спецслужб [335; 355]. Витоки, що стосуються хакерських інструментів, розроблених Центральним розвідувальним управлінням та Агентством національної безпеки, хоча і не пов'язані з цим конкретним інцидентом, але, здається, підтверджують, що такий підхід іноді буває успішним. Кілька місяців потому, у менш розголошеній доповіді, голландське агентство внутрішньої розвідки повідомило, що воно зламало комп'ютерну мережу будівлі, з якої команда російських хакерів зі Служби зовнішньої розвідки їхньої країни проникла в електронні поштові скриньки співробітників Державного департаменту США та Національного комітету Демократичної партії. Цифрове проникнення, яке тривало близько року, було настільки повним, що рік голландська команда змогла отримувати доступ до відеозаписів камер відеоспостереження будівлі та ідентифікувати осіб, які заходили до кімнати, з якої працювали хакери [251]. Ці дві історії ілюструють неможливість гарантувати цілісність комп'ютерних систем навіть для організацій, які підтримують найвищі стандарти операційної безпеки і мають, можливо, найдосконаліші програми кібербезпеки [63, с. 709].

У цьому контексті концепція кіберстійкості пропонує привабливе доповнення до підходу «передбачити і захистити», який домінував в інформаційній безпеці протягом останніх кількох десятиліть. Зіткнувшись з усвідомленням того, що жодна цифрова система не може гарантувати неприступність перед обличчям постійних атак, організації приходять до

висновку щодо необхідності розробляти процеси і технології, які надають допомогу після катастрофічних атак. Відповіддю є стійкість, яку на даний момент визначатимемо як здатність протистояти, відновлюватися після та адаптуватися до зовнішніх шоків. За словами одного із засновників концепції (К. Голлінга, канадського еколога), така зміна перспективи «не вимагає точної здатності передбачати майбутнє, а лише якісної здатності розробляти системи, які можуть поглинати і пристосовуватися до майбутніх подій, яких би несподіваних форм вони не набули» [63, с. 709; 280, с. 15].

У контексті того, про що ми вже зазначали, тобто про концептуальний розвиток «від ризику до стійкості», важливо відрізнити стійкість від управління ризиками, хоча вони взаємопов'язані. Управління ризиками передбачає кількісну оцінку ймовірності та серйозності ризиків, що дозволяє підтримувати рішення про найбільш відповідну стратегію реагування на них, наприклад, таких як бездіяльність, уникнення, зменшення, передача або страхування [184, с. 133]. Стійкість є ширшим поняттям і «має важливе значення, коли ризик не піддається обчисленню, наприклад, коли небезпечні умови є повною несподіванкою, або коли аналітичні параметри ризику виявилися неефективними» [63, с. 710; 323]. Стійкість приходить на зміну управлінню ризиками, коли останній виявився неефективним у захисті організації від руйнівних загроз і передбачає постійний цикл дій та реагування – починаючи задовго до несприятливої події і закінчуючи задовго після завершення події, щоб впровадити адаптивні заходи необхідні для протидії наступному непередбачуваному шоку. Іншими словами, в той час як управління ризиками в кібербезпеці спрямоване на мінімізацію загроз, кіберстійкість прагне підтримувати високий рівень продуктивності незалежно від наявності або відсутності загроз [156]. Це пояснює, чому «організація може мати кібербезпеку не будучи стійкою, але не навпаки» [203].

Потреба в застосуванні мислення та практик стійкості до цифрової екосистеми може здатися зайвою, оскільки інтернет був створений як стійка розподілена система, яка може продовжувати працювати в найгірших

можливих ситуаціях, таких як ядерний удар [192, с. 157]. Але ця технічна стійкість, яка обмежується одним з базових рівнів, що складають Інтернет і гарантує, що маршрутизація пакетів даних може проходити декількома альтернативними шляхами [316], досягаючи одержувачів, навіть якщо нетривіальна кількість з'єднувальних вузлів видаляється, ніколи не мала на меті забезпечити надійний рівень безпеки для світу, в якому всі можливі види соціальної активності та бізнес-транзакцій перемістилися в онлайн, мільярди пристроїв підключені до мережі, а люди, процеси та політики регулярно і успішно використовуються зловмисниками [63, с.709-711]. Враховуючи безпрецедентні масштаби та серйозність кібер-ризиків, кіберстійкість повинна виходити за межі глобальної інфраструктури Інтернету, зосереджуючись на окремих організаціях, які стали залежати від неї у виконанні своєї ролі.

Хоча концепція кіберстійкості, безумовно, здається привабливою коли стикається з таким невизначеним і непередбачуваним середовищем, вона має важливі обмеження, які необхідно визнати і подолати, якщо ми хочемо зберегти її концептуальну перевагу. Основна проблема полягає в тому, що міждисциплінарне коріння стійкості може виявитися як прокляттям, так і перевагою: вона забезпечує багатий теоретичний інструментарій, пов'язаних концепцій, з яких суттєві позитивні складові можуть бути перенесені в кіберпростір, але відсутність єдиного визначення і різноманітність підходів, які вона тягне за собою, сприяє фрагментації, що заважає фахівцям з питань стійкості та політикам розробити узагальнюючий підхід [63; 156; 217; 323]. На фундаментальному рівні, наприклад, існують певні розбіжності щодо справжнього значення стійкості: для одних вона передбачає здатність системи витримати шок і повернутися до свого початкового стану, тоді як для інших – це еволюційний процес, що веде до адаптації та нового стану рівноваги [156, с.48]. На більш практичному рівні кіберстійкість, замість того, щоб розумітися як всеохоплююче поняття, іноді розглядається вузько. Наприклад, у звітах компаній, вихваляючи її переваги, часто плутають кіберстійкість з практиками та методологіями реагування на інциденти, з якими знайомі їхні автори і які

легше продати потенційним клієнтам. З тієї ж причини, галузеві стандарти, які намагалися формалізувати концепцію кіберстійкості переважно зосереджені на її інженерних аспектах і рідко приділяють когнітивним і соціальним аспектам стільки ж уваги. Стійкість занадто часто залишається «риторичним прийомом, який мало впливає на фактичне прийняття рішень» [63, с. 710-711; 161, с. 779].

Це частково пояснює, чому багато експертів скептично ставляться до концепції кіберстійкості, відкидаючи її як одну з останніх примх кібербезпеки, що має на меті привернути увагу довірливих клієнтів. Але мислення про стійкість може забезпечити дуже корисну теоретичну і практичну основу, яка допоможе нам вирватися з колії кібербезпеки, в якій ми опинилися [63].

Таким чином, концепт кіберстійкості є результатом тривалого наукового пошуку та розвитку більш загальної концепції «стійкість», з різним осягненням та сприйняттям різноманітними науковими школами та широкою низки галузей та сфер суспільного буття.

Процес перенесення принципів стійкості у кібервимір став закономірною відповіддю на зміну ландшафту цифрових загроз на початку XXI сторіччя. Якщо класична інформаційна безпека (information security) десятиліттями будувалася навколо тріади – конфіденційність, цілісність та доступність – та фокусувалася на створенні «стін» навколо активів, то поява складних, цілеспрямованих кібератак продемонструвала критичну вразливість таких статичних конструкцій. Трансформація поняття відбулася у момент, коли наукова та інженерна спільноти визнали: абсолютний захист у глобально мережевому світі є неможливим, а отже, фокус має зміститися з «недопущення інциденту» на «керування наслідками та виживання» [325].

Власне термін «кіберстійкість» (cyber resilience) почав активно впроваджуватися у 2010-х роках, знаходячи відображення у роботах таких провідних дослідницьких центрів, як MITRE та NIST. Відповідно до концептуальних засад NIST SP 800-160 [219], кіберстійкість визначається як здатність передбачати, протистояти, відновлюватися та адаптуватися до

несприятливих умов, стресів, атак або компрометацій систем, що використовують цифрові ресурси. У цьому визначенні закладено динамічну природу стійкості: система розглядається не як статичний об'єкт, а як складний організм, що перебуває у постійній взаємодії з агресивним середовищем [165, с. 47].

Сучасна інтерпретація кіберстійкості у міжнародних стандартах та інженерних фреймворках базується на кількох засадничих документах, що формалізували історичний досвід у конкретні технічні вимоги:

1. *Cyber Resiliency Engineering Framework (CREF) від MITRE*. Цей фреймворк став першою спробою структурувати цілі стійкості через набір конкретних технік (таких як адаптивне управління, сегментація, надлишковість та приховування). CREF наголошує, що стійкість досягається не через один інструмент, а через архітектурні рішення, які дозволяють системі «деградувати граціозно» (*graceful degradation*) без повної зупинки критичних процесів [165, с. 48–49].

2. *Підхід CERT Resilience Management Model (CERT-RMM)*. Розроблена SEI Carnegie Mellon University, ця модель розглядає кіберстійкість як конвергенцію безпеки, безперервності бізнесу та управління ІТ-операціями. Вона впроваджує поняття «управління операційною стійкістю», де головним показником успіху є здатність організації підтримувати життєво важливі сервіси незалежно від характеру деструктивного впливу [186, с. 18].

3. *Європейський вектор (EU Cyber Resilience Act)*. Сучасна інтерпретація в межах ЄС, що знайшла відображення у Cyber Resilience Act (2024), акцентує на відповідальності виробників за весь життєвий цикл цифрового продукту. Тут стійкість трактується як обов'язкова властивість «by design» та «by default», що включає автоматичне оновлення безпеки та постійний моніторинг вразливостей [238; 350; 396].

На національному рівні трансформація концепції стійкості призвела до виникнення стратегій «Cyber Power» (як UK National Cyber Strategy), де стійкість розглядається як здатність держави в цілому витримувати системні

кібершоки. Для країн, що перебувають у стані активного цифрового протистояння, кіберстійкість стає основою оборонної доктрини, інтегруючи цивільні та військові ресурси для захисту критичної інформаційної інфраструктури [404].

Особливого значення набуває соціально-технічний аспект: стійкість неможлива без «людського фактора». Як зазначає Wilding [417, с. 96], стійка організація – це та, де персонал володіє навичками розпізнавання аномалій та адаптивного реагування. Це підтверджує, що сучасна кіберстійкість – це не лише набір патчів чи алгоритмів, а комплексна культура управління ризиками, що поєднує правові норми, технічну досконалість та кримінологічну обізнаність щодо тактик противника.

Таким чином, сучасне розуміння терміну, закріплене у стандартах NIST SP 800-160 та фреймворках MITRE (CREF), визначає чотири ключові здатності системи, що формують зміст поняття «resilience» [165; 166; 219]:

1. *передбачення*: здатність системи підтримувати обізнаність про потенційні загрози та готуватися до них заздалегідь.

2. *протистояння*: спроможність поглинати удар, мінімізуючи наслідки або стрес, без втрати базової працездатності (в інженерному контексті це корелює з поняттям «запас міцності»);

3. *відновлення*: здатність оперативно повертатися до прийнятного режиму функціонування після інциденту, відновлюючи втрачені сервіси та дані (важливими показниками тут є час відновлення та ресурсомісткість цього процесу).

4. *адаптація*: найвищий рівень стійкості, що передбачає еволюцію системи на основі отриманого негативного досвіду; система не просто повертається до «статус-кво», а стає більш досконалою.

Особливого значення набуває інституціоналізація цих принципів. Наприклад, у межах НАТО та ЄС (через Cyber Resilience Act) стійкість розглядається як обов'язкова характеристика «by design» [350; 396]. Для України ця тема має особливу актуальність через умови постійної кібервійни.

Історичні витоки концепції доводять, що стійкість – це не лише технічне рішення, а й організаційна культура та правова готовність до функціонування в умовах постійного ризику [63, с. 711].

Аналіз генезису терміну «стійкість» дозволяє стверджувати, що воно пройшло шлях від опису фізичної пружності матеріалів до складної стратегії виживання націй у кіберпросторі. Сучасна кіберстійкість базується на філософії адаптивності, запозиченій з екології, та жорстких метриках відновлення, розроблених у теорії ризиків. Інтеграція цих знань є критичною для розбудови національної системи кібербезпеки України, де здатність системи до виживання та швидкого самовідновлення є головним критерієм її ефективності.

Хоча стійкість та управління ризиками є взаємопов'язаними, все ж вони відрізняються. Управління ризиками передбачає кількісну оцінку ймовірності та серйозності ризиків, що дозволяє підтримувати рішення про найбільш відповідну стратегію реагування на них, наприклад, таких як бездіяльність, уникнення, зменшення, передача або страхування. Стійкість є ширшим поняттям і має важливе значення, коли ризик не піддається обчисленню, наприклад, коли небезпечні умови є повною несподіванкою, або коли аналітичні параметри ризику виявилися неефективними [63, с. 711].

Хоча концепція кіберстійкості і здається привабливою, та коли стикається з невизначеним і непередбачуваним середовищем, вона має важливі обмеження, які необхідно визнати і подолати, якщо необхідно зберегти її концептуальну перевагу. Враховуючи безпрецедентні масштаби та серйозність кібер-ризиків, кіберстійкість повинна виходити за межі глобальної інфраструктури Інтернету, зосереджуючись на окремих організаціях. Мислення про стійкість може забезпечити дуже корисну теоретичну і практичну основу, яка допоможе вирватися з колії кібербезпеки. Тому важливо проаналізувати міждисциплінарні засади, що стосуються вивчення кіберстійкості, щоб зрозуміти як її численні виміри, так і критерії, які можуть

бути використані для полегшення її впровадження та вимірювання у кіберпросторі [63, с. 711].

1.2. Концептуальні основи та функціональні компоненти кіберстійкості

Сучасна парадигма забезпечення безпеки складних інформаційних систем зазнає фундаментальних трансформацій, переходячи від стратегії абсолютного захисту периметра до концепції забезпечення кіберстійкості. Актуальність цього переходу зумовлена неспроможністю традиційних методів кібербезпеки протидіяти складним цілеспрямованим кібератакам та каскадним збоям у взаємозалежних інфраструктурах [171; 324].

Перш за все, необхідно звернути увагу на інтерпретації самого терміну «стійкість», що є важливою методологічною характеристикою його змісту. Наразі, характеризуючи термін «стійкість», важливим є зазначити, що мова йде про відповідний стан об'єкта безпеки: критичної інфраструктури, певної системи, у цілому суспільства [5; 12; 32]. Так, термінологічний глосарій ООН формулює визначення стійкості як здатність систем, громад та суспільства абсорбувати зовнішні впливи та швидко відновлювати характеристики (базову структуру та функції), так і адаптивні можливості, гнучкість системи в умовах значних трансформацій, впливів зовнішнього середовища [94]. Водночас термін «стійкість» (англ., *resilience*) є достатньо вживаним в англomовних країнах та характеризується усталеними ознаками, які формують його сприйняття на рівні міжнародних нормативно-правових документів й практично їх значення формує основу сприйняття «стійкості» в стратегічних безпекових документах. Водночас, необхідним застереженням є певна проблема інтерпретації терміну «стійкість» при перекладі з англійської на інші мови. Як зазначають Тімоті Прайор та Йонас Хагманн, різноманіття смислу

поняття «стійкість» призводить до проблеми його уточнення для тих, хто формує державну політику [12; 362, с. 282].

Джонатан Джозеф з Великої Британії зазначає про «стійкість» як про неоліберальну форму державного управління, з наголосом на здатності суспільства адаптуватися до загроз [297, с. 45]. Водночас Джером Каган акцентує на тому, що термін «стійкість» системно використовується в стратегічних документах, є достатньо вживаним серед політиків в Сполучених Штатах щодо питань безпеки, часто виголошується у виступах політичних діячів, а Конгресом проголошуються «місяці стійкості» [300]. Наприклад, у Стратегії національної безпеки США (в редакції 2010 року) безпосереднє використання терміну «стійкість» здійснюється в контексті [338]: підвищення стійкості держави та національної економіки; дотримання послідовного політичного курсу країни на основі американських цінностей; здатності реагувати на надзвичайні ситуації; зменшення вразливості та підвищення стійкості критичної інфраструктури; протидії глобальним викликам. А у Стратегії національної безпеки Великої Британії стійкість використовується як одна з ключових частин забезпечення національної безпеки: метою державної політики у сфері нацбезпеки визначено розбудову оборони, стійкості та партнерства, а подальшому тексті акцентовано увагу на зміцненні внутрішньої стійкості у протистоянні глобальним викликам [12; 337].

Вітчизняні вчені також досліджують зазначені питання, зокрема Бірюков Д.С., виділяючи сутнісні ознаки, зазначає, що «стійкість» можна розглядати як суспільно-культурний феномен, який полягає у спроможності суспільства досягати та в надзвичайних ситуаціях демонструвати високий рівень культури безпеки [5, с. 223]. Наразі приклад героїзму і рішучості українського суспільства у протистоянні російській агресії також засвідчує про відповідний рівень стійкості нашої держави, в основі якої саме соціальний феномен, рівень свідомості та культури переважної більшості українських громадян. А якщо розглядати «українські майдани», на нашу думку, саме стійкість як суспільно-культурний феномен сформувала активну

громадянську позицію та об'єднала людей без підтримки держави взяти відповідальність за своє майбутнє на себе. Водночас дослідники з Великої Британії, посиляючись на американську пресу, після терактів у квітні 2003 року в Бостоні зазначали про характерні риси поведінки громадян: сміливі, швидко орієнтувалися, показували приклад щирого товариства, залишалися спокійними та слідували інструкціям представників правоохоронних органів [12; 177, с. 221].

Важливим акцентом щодо формування стійкості є розуміння того, що певна негативна подія, яка реалізується відповідною загрозою, є неминучою. Такий підхід і визначає об'єктивною необхідністю формування системи стійкості на основі заходів безпеки, що дозволять вистояти та відновитися. Водночас канадські фахівці вказують на допустимість збурень та відмов, які необхідно заздалегідь визначити і встановити рівень наслідків [347, с. 13]. Тобто, як зазначають автори безпекового діалогу [231, с. 4] ключовим є те, що безпека суб'єкта залежить не тільки від характеру й рівня загрози та його уразливості до загрози, а і від властивостей самого суб'єкта – його «стійкості» до подій [12].

Розуміючи важливість таких висновків, сутність зроблених акцентів, термін «стійкість» є не простим формальним контекстним використанням міжнародними організаціями, а є сучасною новацією щодо розбудови теорії безпеки, формування безпекових концепцій та стратегій, а також має ключове прикладне значення при реалізації державної політики щодо безпекового середовища. Не виключенням, а однією із ключових сьогодні в системі національної безпеки, саме щодо формування «стійкості», є і кібербезпека [12].

Продовжуючи аналіз стану дослідженості проблеми, важливо зазначити, що за останні десятиліття сформувався потужний теоретико-методологічний базис, який охоплює як системно-інженерні аспекти проектування стійких архітектур, так і управлінські стратегії операціоналізації стійкості для різних суб'єктів господарювання [189; 322].

У сучасних наукових працях закордонних дослідників спостерігається чітке розмежування між поняттями кібербезпеки та кіберстійкості. Фундаментальні роботи І. Лінкова та Я. Хаймеса детермінують кіберстійкість як здатність системи підтримувати критичні функції в умовах непередбачуваних деструктивних впливів, що виходить за межі класичного захисту периметра [269; 324]. Дослідники наголошують на необхідності переходу від оцінки вразливостей до вимірювання спроможностей «передбачати, витримувати, відновлюватися та адаптуватися» [164; 322]. У працях фахівців корпорації MITRE (D. Bodeau, R. Graubart) розроблено багаторівневу структуру Cyber Resiliency Engineering Framework (CREF), яка інтегрує цілі, завдання та конкретні інженерні техніки у єдину методологічну систему [164; 165; 166; 171]. Важливим науковим здобутком є перехід до кількісного аналізу через метрики стійкості, що дозволяють оцінювати ефективність архітектурних рішень ще на етапі проектування [170; 324]. Автори доводять, що стійкість не є статичним станом, а є динамічним процесом, який залежить від конфігурації системи та інтенсивності загроз [153; 157]. Особлива увага приділяється інтеграції ризик-орієнтованого підходу з концепцією «керованої деградації», де система свідомо жертвує другорядними функціями задля збереження життєво важливих сервісів [168; 169]. Огляд публікацій свідчить про домінування холістичного підходу, де кіберстійкість розглядається як емерджентна властивість складних систем, що потребує специфічних інструментів аналізу та моделювання [166; 222]. Таким чином, має місце надійний теоретичний базис для розуміння стійкості як здатності до виживання в агресивному цифровому середовищі.

Окремий напрям досліджень присвячений розробці прикладних інструментів кіберстійкості для організацій з обмеженими ресурсами. У роботах J. Carías та J. Hernantes обґрунтовано, що традиційні фреймворки (як-от NIST або ISO) часто є занадто складними для малого та середнього бізнесу (SME), що створює системні ризики для цілих галузей [189]. Дослідники пропонують методологію «операціоналізації стійкості», яка базується на

самооцінці (інструмент CR-SAT) та пріоритезації інвестицій у критичні контролі [188; 190]. Аналіз праць у контексті Індустрії 4.0 та промислового інтернету речей (IIoT) вказує на критичну важливість конвергенції інформаційних та операційних технологій (IT/OT) [190, с. 138]. Вчені доводять, що для промислових систем стійкість має вимірюватися через безперервність технологічних процесів, а не лише цілісність даних [222; 276]. У наукових розвідках останніх років акцентується увага на автоматизації оцінки стійкості, що дозволяє бізнесу оперативно реагувати на зміну ландшафту загроз [188; 189]. Важливим елементом досліджень є розробка стратегій інвестування, де математичні моделі допомагають знайти баланс між вартістю захисту та потенційними збитками від простою [190, с. 138; 274]. Автори підкреслюють, що успішна операціоналізація стійкості вимагає не лише технічних засобів, а й трансформації організаційної культури та управлінських процесів [174; 189]. Цей блок джерел демонструє перехід від абстрактних концепцій до конкретних алгоритмів дій для реального сектору економіки.

Сучасна наукова думка розглядає кіберстійкість не в ізоляції, а через призму взаємозалежностей між критичними інфраструктурами. Дослідження Cambridge Centre for Risk Studies вказують на ефект «каскадних збоїв», де атака на один цифровий актив призводить до колапсу фізичних систем (енергетика, логістика, охорона здоров'я) [306; 330]. Вчені аналізують стійкість у контексті «суспільного виміру», де цифрова інфраструктура виступає основою соціальної стабільності [234; 306]. У роботах MITRE (SCRAM) представлено методи структурованого аналізу, що дозволяють ідентифікувати «вузькі місця» у складних системах-систем (System-of-Systems) [166; 168]. Закордонні автори наголошують на ролі людського фактора та регуляторного середовища як критичних змінних у рівнянні стійкості [182; 256]. Аналіз сценаріїв розвитку кіберпростору до 2025 року (Microsoft) свідчить про необхідність формування нових моделей довіри та міжнародної координації для протидії масштабним кіберкризам [182, с. 17].

Наукові розвідки підкреслюють, що стійкість критичної інфраструктури безпосередньо залежить від швидкості обміну інформацією про інциденти між державою та операторами [210; 212]. Дослідники доводять, що в умовах гібридних загроз стійкість має стати частиною «національного імунітету», що об'єднує технічну міцність із соціальною адаптивністю [234; 322]. Таким чином, огляд підтверджує необхідність комплексного підходу до захисту держави як цілісної кіберфізичної екосистеми.

Результати проведеного аналізу публікацій закордонних авторів та звітів профільних організацій дозволяють сформулювати наступні узагальнення:

у науковій спільноті досягнуто консенсусу щодо трактування кіберстійкості як здатності системи не лише витримувати атаки, а й функціонувати в умовах часткового компрометування з подальшою адаптацією до нових умов загрозового середовища [164; 169];

розроблено низку прикладних фреймворків (CREF, SCRAM, CRR), які дозволяють декомпонувати абстрактні цілі стійкості до конкретних інженерних технік та засобів контролю. Проте залишається потреба у адаптації цих інструментів для специфічних секторів, зокрема для малого бізнесу та високоінтегрованих промислових систем (ІІТ) [168; 188; 189];

попри наявність значної кількості запропонованих індексів та метрик, ключовим викликом залишається їх емпірична валідація та здатність прогнозувати реальні наслідки кіберінцидентів у складних взаємозалежних мережах [157; 170];

кіберстійкість визнається емерджентною властивістю, що залежить не лише від технічних параметрів, а й від людського фактора, організаційної культури та регуляторної політики держави [182; 256].

Виявлені лакуни в існуючих дослідженнях, зокрема щодо автоматизації оцінки стійкості в режимі реального часу та оптимізації інвестиційних стратегій у кіберзахист, визначають вектор подальшого авторського дослідження. Це дозволить розробити більш гнучкі та ефективні моделі

управління кіберстійкістю, адаптовані до сучасних викликів цифрової трансформації суспільства.

Сучасний етап наукового пізнання стійкості кіберсистем характеризується множинністю теоретичних підходів, що зумовлено складністю самого об'єкта дослідження – глобального, взаємозалежного цифрового середовища. Наукова спільнота виокремлює три ключові парадигми, кожна з яких пропонує власну методологію забезпечення життєздатності систем: техноцентричну, екосистемну (біологічну) та соціотехнічну.

У межах *техноцентричної парадигми* – архітектурна стійкість та інженерія виживання – кіберстійкість розглядається як сукупність внутрішніх інженерних властивостей архітектури системи, що дозволяють їй витримувати деструктивні впливи та продовжувати виконання місії навіть у скомпрометованому стані. Науковий зміст цього підходу базується на концепції «стійкості за дизайном» (*resilience by design*), де стійкість є не додатковою функцією, а фундаментальною характеристикою побудови системи [219, с. 113–116].

Основними об'єктами вивчення тут є архітектурні принципи, що забезпечують «граціозну деградацію» (*graceful degradation*). Як зазначають дослідники корпорації MITRE [165], техноцентрична стійкість досягається через реалізацію набору спеціалізованих технік:

Надлишковість – дублювання критичних компонентів та даних для запобігання появі єдиної точки відмови. Теоретично обґрунтовується, що надлишковість має бути не просто кількісною, а й функціональною, щоб уникнути ідентичних вразливостей у дублюючих вузлах.

Модульність та сегментація – обмеження каскадних ефектів шляхом логічного та фізичного розділення системи. Це дозволяє ізолювати уражений сегмент, зберігаючи працездатність решти інфраструктури [324, с. 474].

Різноманітність – використання різноманітних апаратних засобів, операційних систем та алгоритмів. Наукове обґрунтування цього принципу

полягає у створенні гетерогенного середовища, де атака, успішна проти одного компонента, виявиться неефективною проти іншого.

Непостійність – стратегія частого оновлення або «скидання» ресурсів до відомого безпечного стану, що обмежує час перебування зловмисника в системі.

Центральною науковою проблемою в межах техноцентризму є розробка автоматизованих механізмів самовідновлення (self-healing). Вивчення концепції «виживання системи» фокусується на здатності мережі самостійно переконфігуруватися в режимі реального часу у відповідь на виявлені аномалії, що мінімізує втручання людини та прискорює повернення до штатного режиму функціонування [169].

Екосистемний підхід запозичує методологічний апарат з екології та еволюційної біології, розглядаючи кіберпростір не як статичну машину, а як динамічне, складне адаптивне середовище. Фундаментом цього підходу є праці К. Голлінга [280] про екологічну стійкість, адаптовані до цифрових реалій.

Наукове пізнання в межах екосистемного підходу концентрується на наступних аспектах:

Принципи імунізації мереж: аналогія між розповсюдженням комп'ютерних вірусів та біологічних патогенів дозволяє розробляти моделі «цифрового імунітету». Це включає вивчення здатності системи розпізнавати «чужорідні» патерни поведінки та формувати адаптивну відповідь, яка еволюціонує разом із загрозою [252].

Динамічна рівновага: на відміну від інженерного підходу, екосистемний розглядає стійкість як здатність системи переходити з одного стабільного стану в інший. Дослідження Linkov et al. [325, с. 172] підкреслюють, що система може втратити частину функцій, але адаптуватися до нових умов середовища, що є формою стратегічного виживання.

Популяційна різноманітність: вивчення кіберстійкості через призму виживання «популяцій» пристроїв. Це особливо актуально для Інтернету

речей (IoT), де стійкість всієї екосистеми залежить від здатності окремих автономних агентів взаємодіяти між собою для компенсації втрат [187, с. 7].

Ключовим змістом цієї парадигми є концепція адаптивної спроможності (adaptive capacity). Наукові дослідження спрямовані на те, щоб навчити кіберсистеми «вчитися» на кожному інциденті, інтегруючи отриманий досвід у майбутні механізми захисту, що робить їх більш стійкими до майбутніх стресів.

Соціотехнічна парадигма розглядає кіберстійкість як результат складної взаємодії між технічними компонентами, людським фактором та організаційними процесами. Цей підхід базується на засадах Resilience Engineering (Ерік Голльнагель), де стійкість визначається не через те, що система має, а через те, що вона робить [282].

Зміст наукового пізнання у цій сфері охоплює:

Когнітивні аспекти та людський фактор: вивчення того, як оператори та персонал приймають рішення в умовах високого стресу та невизначеності. Дослідження Gísladóttir et al. [256] демонструють, що надмірне регулювання (overregulation) може парадоксально знижувати стійкість, оскільки створює надмірне когнітивне навантаження на людину, яка є останньою лінією оборони при відмові автоматики.

Організаційна поведінка та культура безпеки: стійкість пізнається як здатність організації підтримувати критичні бізнес-функції через гнучке управління процесами. Модель CERT-RMM [186, с. 13] формалізує цей підхід, визначаючи стійкість як процес управління активами (людьми, інформацією, технологіями, об'єктами) для досягнення операційних цілей.

Управління репутацією та соціальною довірою: Як зазначає Wilding [417, с. 96], соціотехнічна стійкість включає здатність організації комунікувати під час кризи, зберігаючи довіру користувачів. Це перетворює кіберстійкість з суто технічної проблеми на проблему соціально-економічної стабільності.

Наукове пізнання в межах цієї парадигми фокусується на створенні систем, які б підтримували людську діяльність, а не лише обмежували її. Стійкість тут — це синергія технічної надійності та людської винахідливості, де здатність фахівців до імпровізації та нестандартного реагування під час «чорних лебедів» є вирішальною [153, с. 3].

Важливими аспектами наукових досліджень залишаються питання щодо методології оцінювання та вимірювання стійкості. У сучасній науковій літературі вимірювання стійкості кіберсистем розглядається як одна з найбільш складних та актуальних проблем, оскільки стійкість, на відміну від безпеки, є динамічною властивістю, що виявляється лише в процесі взаємодії системи з деструктивним середовищем. Наукове пізнання в цьому напрямі розвивається шляхом створення комплексних метрик, що інтегрують часові, функціональні та імовірнісні показники [324, с. 473].

Фундаментальним напрямом оцінювання стійкості є вивчення її через призму чотирьох функціональних цілей, що складають повний життєвий цикл протидії загрози: передбачення, протистояння, відновлення та адаптація.

Науковий зміст оцінювання за цими критеріями полягає у запровадженні чотирьох груп показників. Показники здатності до передбачення передбачають аналіз спроможності системи до раннього виявлення аномалій та ідентифікації потенційних векторів атак на основі проактивного моніторингу. Метрики цього етапу часто базуються на часі виявлення загрози (Time to Detect) та точності прогнозних моделей [164, с. 6]. Показники спроможності до протистояння передбачають вимірювання рівня деградації системи під час атаки. Ключовим параметром тут є «мінімально допустимий рівень функціонування», який система здатна підтримувати в умовах компрометації частини вузлів. Важливими є показники швидкості відновлення, тобто часові метрики, такі як Recovery Time Objective (RTO) та Recovery Point Objective (RPO), що описують здатність системи повернутися до цільового стану. Науковий аналіз траєкторії відновлення (Recovery Profile) дозволяє оцінити ефективність автоматизованих та ручних процедур

реагування [324, с. 474]. І ще один блок показників адаптивності, який передбачає кількісну оцінку змін у архітектурі системи після інциденту. Це найбільш складний для вимірювання блок, що включає аналіз «вивчених уроків» та їх вплив на зниження вразливості системи до майбутніх аналогічних атак [157, с. 1002].

Окремим потужним напрямом наукових досліджень є застосування теорії графів для аналізу стійкості комп'ютерних мереж. У межах цього підходу кіберсистема моделюється як сукупність вузлів та зв'язків, а стійкість пізнається через топологічні характеристики. До таких топологічних характеристик як правило відносять:

зв'язність та критичні вузли: ідентифікація «вузьких місць» та вузлів, видалення яких призводить до дефрагментації мережі, при цьому стійка архітектура теоретично обґрунтовується як така, що має високий ступінь децентралізації та надмірності шляхів передачі даних;

аналіз каскадних відмов: математичне моделювання процесів, коли вихід з ладу одного компонента провокує перевантаження та подальше руйнування суміжних вузлів, що дозволяє розробляти алгоритми автоматичного балансування навантаження як методу підвищення стійкості [252];

Оскільки кіберпростір характеризується високим рівнем стохастичності та неповнотою даних про наміри противника, сучасна наука дедалі частіше звертається до апарату нечіткої логіки (Fuzzy Logic) та теорії ігор.

Методологічний зміст цих досліджень полягає у переході від бінарних оцінок («система захищена / не захищена») до спектральних оцінок ступеня стійкості. Використання нечітких множин дозволяє інтегрувати якісні експертні оцінки з кількісними даними моніторингу, формуючи інтегральні індекси кіберстійкості [325, с. 172–173]. Такий підхід забезпечує моделювання стратегічної взаємодії, тобто розгляд протистояння «атакувальник – захисник» як гри з ненульовою сумою, де метою захисника є максимізація стійкості за обмежених ресурсів, та прогнозування в умовах невизначеності. А це вже

оцінювання ризиків, пов'язаних із «чорними лебедями» (малоймовірними, але критичними подіями), що є наріжним каменем менеджменту стійкості [153].

Наукове пізнання стійкості також включає розробку моделей зрілості (Maturity Models), таких як CERT-RMM, де стійкість вимірюється не лише технічними параметрами, а й рівнем стабільності організаційних процесів. Вимірювання «зрілості стійкості» дозволяє оцінити, наскільки здатність до відновлення є інституціоналізованою, а не залежить від випадкових факторів чи імпровізації персоналу [186, с. 13].

Таким чином, методологічні засади оцінювання кіберстійкості зміщують фокус з аналізу статичних вразливостей на аналіз динамічної реакції системи. Наукове поєднання часових метрик, топологічного аналізу мереж та апарату нечіткої логіки створює надійний фундамент для об'єктивного вимірювання та подальшого проектування стійких цифрових середовищ, здатних до адаптації в умовах глобальних кіберзагроз.

У межах сучасного наукового пізнання функціональні цілі кіберстійкості розглядаються не просто як сукупність технічних завдань, а як фундаментальні вектори спрямованості системи на збереження її життєздатності в умовах ворожого середовища. Концептуальний зміст цих цілей впливає з необхідності забезпечення безперервності критичних процесів через механізми адаптивного управління, контрольованої деградації та стратегічного введення противника в оману. Наукове обґрунтування цих напрямів дозволяє трансформувати теоретичні положення стійкості у конкретні архітектурні та операційні стратегії, що базуються на визнанні неминучості успішних атак та пріоритетності виживання системи.

Одним із центральних напрямів сучасних досліджень є адаптивне управління кіберсистемами. Наукове розуміння адаптивності базується на здатності системи динамічно змінювати свою конфігурацію, ресурси та поведінку у відповідь на виявлені зміни у стані середовища або виникнення аномалій. У теоретичному аспекті адаптивне управління реалізує концепцію «спритності» (agility), що дозволяє системі уникати статичних вразливостей.

На відміну від традиційного адміністрування, адаптивне управління у контексті стійкості передбачає функціонування замкнених циклів зворотного зв'язку, де дані про атаку інтегруються у процеси переконфігурації в режимі реального часу. Це забезпечує можливість швидкої ізоляції скомпрометованих компонентів та перерозподіл обчислювальних потужностей для підтримки найбільш критичних сервісів. Згідно з підходами корпорації MITRE, адаптивне управління є критичним для протидії прогресуючим кіберзагрозам (APT), оскільки воно позбавляє атакуючу сторону переваги у знанні статичної структури мережі, перетворюючи кіберпростір на «рухому ціль» [165; 324; 325].

Паралельно з адаптивністю фундаментальне значення має концепція динамічної (граціозної) деградації, про яку ми вже згадували. У науковій літературі цей принцип обґрунтовується як здатність системи до усвідомленого та керованого зниження продуктивності або відключення другорядних функцій задля збереження працездатності життєво важливого ядра. Теоретична база граціозної деградації заперечує бінарний підхід «працює/не працює» та впроваджує континуум станів працездатності. Наукове пізнання цього процесу зосереджене на визначенні ієрархії системних місій та сервісів, де в умовах дефіциту ресурсів або активного ураження пріоритет надається функціям, від яких залежить фізична безпека, життєзабезпечення або виконання критичних державних завдань. Математичне моделювання таких станів дозволяє розраховувати порогові значення, за яких система ще зберігає свою сутність, попри значні втрати у периферійних вузлах. Як зазначає Я. Хаймс [269, с. 499], граціозна деградація є вищою формою інженерної витривалості, оскільки вона дозволяє уникнути катастрофічного каскадного руйнування всієї інфраструктури через локальний збій.

Окремим перспективним напрямом наукового пізнання змісту кіберстійкості є вивчення стратегій кібердецепції. У контексті стійкості децепція розглядається не просто як метод виявлення атак, а як стратегічний інструмент підвищення виживаємості системи через введення противника в

оману. Теоретичне обґрунтування децепції базується на зміні асиметрії інформації на користь захисника. Використання фальшивих цілей, мережевих «приманок» та маніпуляція відображенням реальної топології мережі дозволяють розпорошувати ресурси атакуючого, змушуючи його витратити час на неіснуючі вразливості. Це створює необхідний часовий резерв для активації механізмів відновлення та адаптації основної системи. Більше того, науковий аналіз децепції вказує на її здатність виявляти тактики та процедури (TTPs) противника на ранніх стадіях, що є основою для подальшої «імунізації» системи. У роботах дослідників NIST децепція інтегрується у загальну архітектуру стійкості як метод активного впливу на когнітивну модель зловмисника, що робить атаку економічно недоцільною або занадто ризикованою для нього [169; 219; 387].

Синтез цих функціональних цілей – адаптивного управління, граціозної деградації та децепції – формує цілісний концептуальний зміст наукового пізнання стійкості. Вони взаємно доповнюють один одного: децепція забезпечує час для виявлення загрози, адаптивне управління дозволяє змінити конфігурацію для уникнення подальшого ураження, а граціозна деградація гарантує виживання системи навіть за умови часткового успіху атаки. Такий багаторівневий підхід до визначення функціональних цілей свідчить про зрілість наукової думки, яка перейшла від ілюзорних концепцій повної безпеки до реалістичних моделей стійкого розвитку в агресивному цифровому середовищі. Це створює методологічну базу для розробки складних соціотехнічних систем, де технічна досконалість поєднується з інтелектуальними стратегіями захисту, що забезпечує сталість цифрової економіки та національної безпеки.

Висвітлення змісту функціональних цілей також підкреслює важливість «самоорганізації» кіберсистем. У наукових роботах останнього десятиліття дедалі частіше згадується концепція «автономної стійкості», де система здатна самостійно обирати між різними сценаріями деградації або адаптації без безпосереднього втручання людини. Це потребує розробки складних

алгоритмів прийняття рішень, що базуються на ієрархії цінностей активів та прогнозованому аналізі дій противника. Таким чином, сучасна наука формує бачення кіберстійкості як активного процесу підтримки місії, де здатність системи «гнути, але не ламатися» є ключовим атрибутом її досконалості.

Останнє десятиліття у сфері кібербезпеки позначене фундаментальним зсувом наукових пріоритетів, що відображає перехід від вузькоспеціалізованих технічних засобів захисту до всеохоплюючих стратегій виживання складних систем. Цей процес зумовлений усвідомленням того, що в умовах гіперпов'язаності та зростаючої складності технологічного ландшафту традиційні методи вже не забезпечують необхідного рівня стабільності. Головними стратегічними векторами розвитку сучасної наукової думки є зміна парадигми управління – від менеджменту ризиків до менеджменту стійкості, а також концептуалізація цифрової довіри як похідної від здатності системи до відновлення.

Фундаментальною ознакою сучасної наукової трансформації є поступовий перехід від домінування парадигми управління ризиками до парадигми управління стійкістю. Традиційний ризик-менеджмент базується на предикативному аналізі, що намагається ідентифікувати конкретні загрози, оцінити імовірність їх реалізації та мінімізувати вразливості до того, як вони будуть експлуатовані. Однак наукові розвідки останніх років вказують на те, що така модель виявляється малоефективною у середовищах, які характеризуються високим рівнем «невідомої невизначеності». Як підкреслює Т. Авен [153], управління ризиками часто зосереджене на статистичній ймовірності минулих подій, тоді як стійкість спрямована на готовність системи до подій типу «чорний лебідь» – малоімовірних, але критичних за наслідками інцидентів, які неможливо передбачити за допомогою класичних імовірнісних моделей. Менеджмент стійкості, на відміну від ризик менеджменту, виходить з презумпції успішності атаки, фокусуючись на збереженні цілісності місії організації та здатності до швидкого самовідновлення. Це вимагає від наукової спільноти розробки нових моделей

прийняття рішень, де пріоритетом є не відсутність шкоди, а здатність поглинати удар та адаптуватися до нових умов функціонування [174; 325].

Наукове обґрунтування цього переходу спирається на теорію складних систем, де кіберпростір розглядається як середовище з нелінійними зв'язками. У таких системах неможливо усунути всі ризики, оскільки саме усунення одного ризику може парадоксально створити нові, більш складні вразливості через каскадні ефекти. Відтак, стратегічний вектор наукового пізнання зміщується у бік створення «антикрихких» архітектур, які здатні не просто протистояти стресу, а й ставати міцнішими в процесі боротьби з ним. Це підтверджується змістом сучасних регуляторних ініціатив, зокрема EU Cyber Resilience Act, де кіберстійкість трактується як безперервний процес управління життєвим циклом продукту, що включає постійну оцінку спроможності системи до виживання. Науковий дискурс у цій сфері підкреслює, що менеджмент стійкості є вищою формою стратегічного управління, оскільки він інтегрує технічну надійність із організаційною гнучкістю, дозволяючи суб'єктам цифрового простору зберігати працездатність у стані постійної турбулентності [238; 350; 396].

Іншим ключовим вектором розвитку наукової думки є концептуалізація цифрової довіри як стратегічної мети та результату забезпечення кіберстійкості. У науковому розумінні цифрова довіра більше не розглядається як суто психологічна або комерційна категорія; вона стає техніко-юридичним показником якості цифрового середовища. Довіра до системи сьогодні безпосередньо залежить від її прозорості та здатності демонструвати передбачувану поведінку під час інцидентів. Наукове пізнання цифрової довіри зосереджене на вивченні механізмів підтвердження стійкості, які дозволяють користувачам, партнерам та регуляторам бути впевненими у тому, що система не лише захищена, а й здатна відновити критичні послуги у разі збою. Як зазначають аналітики DigiCert [238], цифрова довіра формується через поєднання надійних ідентифікаційних даних, цілісності програмного забезпечення та прозорих процесів реагування на вразливості. Таким чином,

кіберстійкість стає технологічним фундаментом довіри: організація, яка демонструє високий рівень стійкості, автоматично отримує вищий кредит довіри у цифровій економіці, що є критичним фактором конкурентоспроможності та стабільності [417, с. 97].

Більше того, стратегічний вектор наукового пізнання включає інтеграцію кіберстійкості у ширший контекст сталого розвитку і в англomовному середовищі цим терміном є «Sustainability». Наукові праці останнього періоду акцентують увагу на тому, що без забезпечення стійкості цифрових систем неможливо досягти стійкості економічної чи екологічної, оскільки вони глибоко інтегровані через системи Інтернету речей (IoT) та хмарні обчислення. Стійкість кіберсистем починає сприйматися як суспільне благо, що потребує колективних зусиль держави, приватного сектора та наукової спільноти. Це зумовлює виникнення нових напрямів досліджень, таких як «національна кіберсила», де стійкість є одним із ключових вимірів спроможності держави захищати свої інтереси у глобальному кіберпросторі [404, с. 99]. Розвиток цієї думки веде до розуміння того, що майбутнє наукового пізнання полягатиме у створенні цілісної екосистеми стійкості, де технічні стандарти, правові норми та етичні засади використання технологій будуть гармонійно поєднані задля забезпечення безпечного та сталого прогресу людства.

Отже, стратегічні вектори розвитку наукової думки у сфері кіберстійкості відображають еволюцію людства у цифрову епоху. Відмова від ілюзії повної безпеки на користь розбудови адаптивної спроможності свідчить про зрілість наукового підходу. Перехід до менеджменту стійкості та фокус на цифровій довірі створюють нову методологічну базу, яка дозволяє не лише реагувати на поточні виклики, а й формувати безпечний ландшафт майбутнього. Це відкриває нові перспективи для наукових досліджень, спрямованих на глибше розуміння природи складних систем та пошук інноваційних шляхів забезпечення їх життєздатності у світі, де зміни є єдиною постійною величиною.

Підсумовуючи аналіз сучасних напрямів наукового пізнання стійкості кіберсистем, слід констатувати, що в межах світової наукової думки відбулася остаточна концептуальна трансформація. Кіберстійкість більше не розглядається як другорядна технічна функція, а сприймається як фундаментальна стратегічна спроможність, що забезпечує життєздатність складних соціотехнічних систем у волатильному цифровому середовищі. Синтез техноцентричного, екосистемного та соціотехнічного підходів дозволив сформулювати багатовимірне бачення проблеми, де інженерна досконалість архітектури поєднується з біологічною адаптивністю та організаційною гнучкістю.

Наукова розробленість теми на сьогодні характеризується високим ступенем деталізації інженерних та технічних аспектів. Завдяки працям фахівців NIST, MITRE та SEI, було створено ґрунтовну базу методологій оцінювання, яка дозволяє кількісно вимірювати здатність системи передбачати загрози, витримувати їхній вплив та оперативно відновлюватися. Математизація стійкості через теорію графів, імовірнісні моделі та апарат нечіткої логіки надала дослідникам інструментарій для формалізації невизначеності, що є критично важливим для управління «невідомими ризиками». Разом із тим, зміст наукового пізнання функціональних цілей стійкості, таких як адаптивне управління та граціозна деградація, свідчить про перехід від ідеалістичних моделей «абсолютного захисту» до реалістичних стратегій керованого виживання.

Попри значні успіхи в інженерному та методичному вимірах, аналіз стану наукової розробленості виявляє низку прогалин, які потребують подальшого дослідження. По-перше, більшість існуючих моделей стійкості зосереджені на внутрішніх властивостях системи, недостатньо враховуючи динаміку сучасного криміногенного ландшафту та еволюцію тактик високоорганізованої кіберзлочинності. По-друге, стратегічний перехід від ризик менеджменту до менеджменту стійкості потребує глибшого теоретичного обґрунтування організаційно-правових механізмів, які б

дозволили імплементувати технічні стандарти у площину державного управління та національної безпеки. Існує нагальна потреба у розробці інтегрованих підходів, де технічна стійкість була б органічно поєднана з правовими нормами відповідальності та кримінологічними засадами протидії зловмисному використанню технологій.

Крім того, наукова думка лише починає осмислювати роль проактивної аналітичної розвідки та предиктивних моделей у забезпеченні стійкості на рівні держави. Якщо технічні метрики дозволяють оцінювати стан «тут і зараз», то питання стратегічного форсайту та прогнозування довгострокових ризиків у контексті глобальної кібервійни залишаються відкритими. Це створює об'єктивні передумови для подальшої наукової роботи, яка б синтезувала існуючі світові досягнення з реальними потребами національних систем безпеки.

Таким чином, сучасний стан наукового пізнання кіберстійкості є міцним фундаментом, що дозволяє переходити від вивчення загальних принципів до розробки комплексних організаційно-правових та кримінологічних засад забезпечення стійкості. Саме на перетині технічних наук, права та кримінології лежить потенціал для створення наступного покоління систем захисту, здатних не лише виживати в умовах атак, а й забезпечувати сталий розвиток цифрового суспільства та довіру до державних інституцій.

1.3. Нормативно-правове та стратегічне забезпечення національної кіберстійкості

На сучасному етапі розвитку міжнародних відносин забезпечення кіберстійкості перейшло з розряду галузевих технічних завдань до рівня стратегічних пріоритетів глобальної безпеки. Провідні міжнародні організації та розвинені країни світу визнають, що в умовах гіперзв'язності цифрова вразливість однієї держави може мати каскадні наслідки для всієї світової

економіки та стабільності. Головним глобальним трендом є перехід від індивідуальних заходів захисту окремих вузлів до формування екосистем «колективної стійкості», де здатність витримувати кібершоки стає спільним обов'язком урядів, приватного сектору та міжнародних інституцій.

Центральну роль у формуванні концептуальної та нормативної бази кіберстійкості на глобальному рівні відіграє НАТО. Для Альянсу стійкість є однією з трьох основних засад колективної оборони, закріплених у статті 3 Північноатлантичного договору. Сучасна політика НАТО у цій сфері базується на «Зобов'язанні щодо посилення стійкості» (Resilience Commitment), прийнятому на Варшавському саміті 2016 року, де кіберпростір було офіційно визнано окремим операційним доменом поряд із сушею, морем та повітрям. Науковий аналіз підходів НАТО вказує на те, що стійкість розглядається не лише як технічна надійність систем зв'язку, а як здатність держави підтримувати критичні урядові функції та цивільні послуги під час масштабних криз. Важливим інструментом у цьому процесі є діяльність Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE), який розробляє методологічні рекомендації та проводить навчання (наприклад, Locked Shields), спрямовані на відпрацювання сценаріїв відновлення національних інфраструктур після масштабних кібератак [404, с. 99].

У НАТО давно сформувалися системні підходи щодо посилення стійкості на основі запобігання кіберзагрозам. Високий рівень кіберстійкості забезпечується участю усіх суб'єктів системи кібербезпеки, формуванням надійних та ефективних інституцій, структур, агенцій та місій, що сприяють кібербезпеці та реагують на кібератаки [131, с. 129].

На початковому етапі існування НАТО стійкість реалізовувалась загальним сутнісним підходом саме щодо можливості витримувати неочікувані військові удари, що закріплювалося Північноатлантичним договором та застосуванням принципу колективної оборони. Так у ст. 3 зазначалося, що для забезпечення ефективнішої реалізації цілей Договору

країни-члени, діючи окремо чи колективно, шляхом постійного та ефективного вдосконалення власних можливостей та взаємодопомоги, підтримуватимуть і розвиватимуть свою індивідуальну та колективну здатність протистояти збройному нападу [12; 90]. Але сучасні підходи прямо визначають стійкість у якості одного з ключових напрямів.

За сучасних безпекових умов актуальність забезпечення стійкості в НАТО значно зросла та все частіше розглядається у якості окремого напрямку діяльності Альянсу. Посилюючи цю складову, спочатку принцип колективної оборони було доповнено розбудовою спроможностей кризового менеджменту та розвитком співробітництва за напрямом безпеки [7, с.13]. Але анексія Криму РФ у вересні 2014 року сформувала нові виклики в глобальному безпековому середовищі, що потребувала упровадження нових підходів в стратегічному та операційному плануванні і визначенні завдань. Як результат, було затверджено «План дій НАТО щодо забезпечення готовності» [340], який хоча і не реалізував ще прямо концепцію стійкості, все ж змістовно наблизив цей процес так як передбачав: посилення оборонних спроможностей, підвищення мобільності та оперативності, поліпшення співпраці і координації між структурами Альянсу, відпрацювання заходів антикризового управління, посилення спроможностей отримання розвідувальної інформації тощо.

Безпосередньо стійкість була реалізована у нормативних документах НАТО у червні 2016 р. на зустрічі міністрів оборони країн-членів НАТО з прийняттям відповідних Керівних принципів. Їх зміст прямо визначав ключові напрями забезпечення стійкості:

- гарантована дієвість уряду і критично важливих урядових служб;
- стійке постачання енергії;
- здатність ефективно вирішувати ситуацію з неконтрольованим переміщення людей;
- стійкі джерела продуктів і води;
- здатність впоратися з проблемою значних людських втрат;
- стійкі цивільні системи зв'язку;

стійкі транспортні системи (для потреб НАТО) [12; 339].

На цьому ж етапі упроваджуються нові напрями та заходи розбудови стійкості у кіберпросторі [12]:

створені команди кіберреагування;

підписано Меморандум про порозуміння між Альянсом і окремими його країнами-членами щодо забезпечення захищених підключень для обміну інформацією і врегулювання криз;

Центр передового досвіду з кіберзахисту НАТО активізував діяльність у напрямку розвитку спеціальних можливостей щодо протидії шкідливим програмам та підготовки фахівців відповідного рівня;

налагоджується співпраця між Альянсом і малими та середніми компаніями-розробниками кібертехнологій, які часто найбільш інноваційні в цій сфері;

у ході саміту НАТО у Варшаві був підписаний документ під назвою «Зобов'язання щодо кіберзахисту», згідно з яким країни-члени Альянсу підтвердили курс на розвиток сил і засобів з метою зміцнення загальної стійкості організації;

у країнах-членах НАТО прийняті національні стратегії кібербезпеки і внесені зміни до законодавства щодо злочинів проти неї [12].

Із врахуванням специфіки гібридної війни НАТО визначає напрями щодо посилення стійкості у протистоянні кіберзагрозам:

широке втілення кіберзахисту в операції і місії НАТО, підвищення статусу внесків країн-членів Альянсу у кіберзахист з допоміжного до більш самостійного;

розвиток сил і засобів кіберзахисту серед членів НАТО, обмін досвідом між членами Альянсу з використанням формальних і неформальних каналів (включаючи процес оборонного планування в НАТО);

чітке визначення міжнародної ролі Альянсу у підтримці відповідальної поведінки держави в кіберпросторі і заходів з розбудови довіри в кіберсфері;

обмін розвідувальними даними та інформацією про стан справ у кіберсфері як між членами НАТО, так і з іншими міжнародними організаціями;

налагодження співпраці на основі взаємного доповнення з Центром ЄС з боротьби з кіберзлочинами, особливо у світлі гібридної війни та конфліктів у сірих зонах [12].

Досвід НАТО у розбудові концепту стійкості є надзвичайно важливим і для України. Перш за все, реалізація стійкості держави та суспільства стосується сфери національної безпеки, що передбачає розбудова на нових засадах, з рисами стійкої системи, сектору безпеки і оборони. Насамперед це стосується:

безперебійного функціонування у нормальному (штатному) режимі, адаптацію до умов, що змінюються;

здатності витримувати неочікувані удари;

відновлення після руйнівних наслідків явищ/дій будь-якої природи до бажаної рівноваги за умови збереження безперервності процесу управління[116, с. 23–24].

Нормативно-правове забезпечення реалізації концепту стійкості в Україні сформувалося лише за останні роки. Стратегія національної безпеки України 2015 року цей термін використовує лише у контексті підвищення стійкості національної економіки до негативних зовнішніх впливів [12; 32; 111] і понятійного визначення змісту зазначеного терміну взагалі не містить. Водночас наступна 2020 року Стратегія національної безпеки України: «БЕЗПЕКА ЛЮДИНИ – БЕЗПЕКА КРАЇНИ» ключовими засадами визначає стримування, стійкість та взаємодію [32; 109]. А у ст. 47 прямо вказується: «Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз ...». Що буде реалізовуватися шляхом:

оцінки ризиків, своєчасної ідентифікації загроз і визначення вразливостей;

ефективного стратегічного планування і кризового менеджменту;

дієвої координацію та чіткої взаємодії органів сектору безпеки і оборони, інших державних органів, територіальних громад, бізнесу, громадянського суспільства і населення у запобіганні й реагуванні на загрози та подоланні наслідків надзвичайних ситуацій;

поширення необхідних знань і навичок у цій сфері;

налагодження та підтримання надійних каналів комунікації державних органів із населенням на всій території України [32].

У заключних положеннях зазначається, що вона є основою для розроблення галузевих стратегій, зокрема кібербезпеки України, яка і була введена в дію відповідним Указом Президента України у травні 2021 року [32; 110]. В останньому розділі «Виміри успіху (метрики)» зазначається, що за результатами реалізації Стратегії Україна забезпечить:

стійкість до кіберзагроз, підвищивши здатність державних органів, бізнесу і громадян захищати себе та реагувати на кіберзагрози;

спроможність до ефективної протидії недружнім діям у кіберпросторі ...;

розвиток кадрового потенціалу та інноваційного ринку кібербезпеки

Таким чином, стійкість до кіберзагроз Стратегією національної безпеки України визначається одним із головних пріоритетів її реалізації.

Паралельно з військово-політичними зусиллями Альянсу, на глобальному рівні відбувається інтенсивна стандартизація метрик та процесів стійкості. Міжнародний союз електрозв'язку (ITU) та Міжнародна організація зі стандартизації (ISO) формують єдину «мову» кіберстійкості, що дозволяє різним країнам порівнювати свої рівні готовності. Зокрема, Глобальний індекс кібербезпеки (GCI) ITU став важливим інструментом бенчмаркінгу, що стимулює країни до розробки національних стратегій стійкості. Крім того, наукове пізнання глобальних трендів вказує на зростаючу роль галузевої саморегуляції. Прикладом такої успішної моделі є вимоги Міжнародної асоціації класифікаційних товариств (IACS), які впроваджують уніфіковані

стандарти (UR E26 та E27) для забезпечення кіберстійкості суден та морської інфраструктури. Це свідчить про те, що світовий досвід рухається шляхом «вертикальної» стійкості, де кожна критична галузь розробляє власні жорсткі регламенти виживання, що відповідають специфіці її технологічних процесів [209; 365].

Ще одним визначальним трендом є посилення публічно-приватного партнерства у сфері обміну інформацією про загрози. Сучасні міжнародні стратегії, зокрема підходи США та Великобританії, базуються на визнанні того, що понад 80% критичної інфраструктури перебуває у приватній власності [277, с. 303]. Це зумовлює перехід від директивного управління до створення «коаліцій стійкості», де державні органи (такі як CISA у США) виступають координаторами та фасилітаторами, що надають бізнесу необхідні інструменти для самооцінки (наприклад, Cyber Resilience Review). Таким чином, глобальна архітектура кіберстійкості трансформується у складну багаторівневу мережу, де технічні стандарти, політичні зобов'язання та економічні стимули поєднуються задля створення безпечного цифрового простору, здатного до швидкої адаптації в умовах непередбачуваних викликів XXI століття.

Європейський Союз за останнє десятиліття здійснив фундаментальну трансформацію своєї нормативно-правової бази, перейшовши від фрагментарних заходів захисту інформаційних мереж до створення цілісної екосистеми цифрової стійкості. Сучасний стратегічний підхід ЄС ґрунтується на розумінні того, що стійкість є не лише технічним параметром, а й ключовою умовою функціонування єдиного ринку та забезпечення цифрового суверенітету. Центральним елементом цієї архітектури є перехід до проактивного регулювання, яке охоплює весь життєвий цикл цифрових продуктів і послуг – від проектування до виведення з експлуатації. Науковий та політичний дискурс ЄС у цій сфері концентрується на трьох фундаментальних стовпах: горизонтальному регулюванню ринку продуктів,

секторальній стійкості критичної інфраструктури та забезпеченні стабільності фінансового сектору.

Ключовим інструментом цієї трансформації став Закон ЄС про кіберстійкість (EU Cyber Resilience Act – CRA) [366], який є першим у світі горизонтальним законодавчим актом такого роду. Наукове значення CRA полягає у запровадженні обов'язкових вимог до кібербезпеки для всіх продуктів із «цифровими елементами», що постачаються на ринок ЄС. Як зазначається у аналітичних оглядах Європейського парламенту [237; 396], цей регламент усуває критичну прогалину у відповідальності виробників програмного та апаратного забезпечення. До ухвалення CRA відповідальність за стійкість часто перекладалася на кінцевого споживача, що створювало умови для розповсюдження вразливих пристроїв (зокрема в сегменті IoT). Тепер виробники зобов'язані впроваджувати принципи «безпеки за дизайном» (security by design) та «стійкості за замовчуванням», а також забезпечувати підтримку продуктів та усунення вразливостей протягом усього часу їхнього використання. Це створює нову парадигму ринку, де кіберстійкість стає не додатковою перевагою, а обов'язковою умовою допуску товару до продажу, що кардинально підвищує загальний рівень захищеності європейського цифрового простору [350].

Паралельно з регулюванням продуктів, ЄС посилив вимоги до суб'єктів, що забезпечують життєдіяльність суспільства, через Директиву про заходи для високого спільного рівня кібербезпеки в межах Союзу (NIS2). Цей документ розширює коло організацій, що підлягають нагляду, та впроваджує жорсткі вимоги до управління ризиками та звітності про інциденти. Науковий зміст NIS2 полягає у переході до моделі «ланцюжка постачання стійкості» (supply chain resilience). Організації тепер відповідальні не лише за власну інфраструктуру, а й за рівень безпеки своїх постачальників та сервіс-провайдерів. Директива також гармонізує санкції за недотримання вимог стійкості, що робить її виконання критичним для топ-менеджменту компаній. Таким чином, ЄС формує мережу взаємопов'язаних та взаємозалежних

суб'єктів, де стійкість кожного елемента підтримує стійкість системи в цілому. Це особливо актуально для енергетики, транспорту та охорони здоров'я, де збій у кіберсистемі може призвести до реальних людських жертв або масштабних економічних втрат [399].

Окремим напрямом стратегії ЄС є забезпечення стійкості фінансової системи через Регламент про цифрову операційну стійкість (DORA). Цей акт визнає, що фінансовий сектор є найбільш критичною та водночас найбільш атакованою частиною цифрової економіки. DORA запроваджує уніфіковані стандарти тестування стійкості, управління ризиками сторонніх постачальників ІКТ-послуг (наприклад, хмарних провайдерів) та механізми швидкого відновлення після атак. Наукове пізнання DORA дозволяє стверджувати, що фінансова стійкість тепер неможлива без кіберстійкості. Регламент змушує фінансові установи не просто захищати дані, а доводити свою здатність продовжувати операції навіть у разі повної відмови основних ІТ-систем. Це створює прецедент для інших галузей, демонструючи, як жорстке регулювання та високі технічні стандарти можуть стати основою для системної стабільності в масштабах всього континенту [238].

Важливим інституційним підґрунтям цієї стратегії є діяльність Агентства ЄС з кібербезпеки (ENISA) та Мережі груп реагування на інциденти комп'ютерної безпеки (CSIRTs Network). ENISA відіграє ключову роль у розробці схем сертифікації кібербезпеки, що є інструментом верифікації стійкості для бізнесу та держави. Стратегічний підхід ЄС також передбачає тісну співпрацю між цивільними та військовими структурами, що відображено у Кіберстратегії ЄС (EU Cybersecurity Strategy for the Digital Decade). Зміст цієї політики полягає у створенні «Кіберщита» (Cyber Shield) – мережі центрів операційної безпеки (SOC), які використовують штучний інтелект та великі дані для виявлення загроз на ранніх стадіях. Таким чином, ЄС демонструє світові приклад інтегрованої моделі забезпечення стійкості, де правове регулювання, економічні стимули та технологічні інновації об'єднані

спільною метою – створенням надійного та безпечного цифрового дому для громадян і бізнесу.

У висновку до аналізу стратегії ЄС слід зазначити, що європейська модель базується на трьох принципах: солідарності, відповідальності та прозорості. Солідарність виявляється у спільній відповіді на масштабні інциденти; відповідальність – у жорстких вимогах до виробників та операторів; прозорість – у обов’язковому обміні інформацією про вразливості. Цей досвід є надзвичайно цінним для України, яка в процесі євроінтеграції має адаптувати своє законодавство до стандартів NIS2 та CRA. Створення національної системи кіберстійкості за європейським зразком дозволить Україні не лише посилити власну безпеку, а й стати повноправним та надійним учасником цифрового ринку ЄС, здатним витримувати виклики сучасної гібридної війни.

Сполучені Штати Америки демонструють одну з найбільш комплексних та прагматичних моделей забезпечення кіберстійкості, яка еволюціонувала від концепції захисту периметра до стратегії «нульової довіри» (Zero Trust) та безперервної життєздатності. Американська модель базується на тісному поєднанні державних директив, наукових стандартів та ринкових механізмів, де ключову роль відіграє Агентство з питань кібербезпеки та захисту інфраструктури (CISA). Науковий зміст підходу США полягає у визнанні кіберпростору середовищем постійної загрози, що вимагає не лише пасивного захисту, а й активної стійкості, здатної мінімізувати наслідки неминучих інцидентів для національної безпеки та економічного добробуту.

Фундаментом сучасної політики США є державні стратегії та виконавчі укази Президента, зокрема Виконавчий указ 14028 «Про покращення кібербезпеки нації» [240]. Цей документ ознаменував перехід до нових стандартів стійкості для всіх федеральних інформаційних систем та їхніх постачальників. Наукове обґрунтування цієї політики базується на принципі «радикальної прозорості» та обов’язковості впровадження багатофакторної автентифікації, шифрування даних та хмарних технологій як засобів

підвищення відмовостійкості. Уряд США розглядає кіберстійкість як динамічну спроможність, яка вимагає постійної модернізації застарілих систем (legacy systems), що є найбільш вразливими вузлами національної інфраструктури. Важливим аспектом є також концепція «Shared Responsibility» (спільної відповідальності), де держава надає приватним операторам критичної інфраструктури розвідувальні дані про загрози в обмін на прозору звітність про інциденти [200].

Провідну роль у методичному забезпеченні цієї моделі відіграє Національний інститут стандартів і технологій (NIST). Фреймворки NIST, зокрема NIST Cybersecurity Framework (Рамкова програма кібербезпеки) та спеціальна публікація SP 800-160 Vol. 2 «Developing Cyber-Resilient Systems», стали світовим золотим стандартом у пізнанні стійкості. Науковий внесок NIST полягає у формалізації інженерних принципів стійкості, таких як адаптивність, надлишковість та сегментація, у зрозумілі для бізнесу та держави кроки. Модель NIST не є жорстко регуляторною; вона пропонує гнучкий інструментарій для оцінювання ризиків та вибору оптимальних стратегій виживання залежно від місії організації. Це дозволяє створювати системи, що здатні до «граціозної деградації», зберігаючи критичні функції під час кібератак. Важливо, що підхід NIST інтегрує технічні аспекти з управлінськими процесами, створюючи цілісну модель «управління стійкістю», яка дозволяє організаціям бути антикрихкими у цифровому середовищі [219, с. 113–114].

Окремим вектором американської моделі є діяльність CISA як «національного ризик-менеджера». CISA розробляє та впроваджує практичні інструменти оцінки стійкості, зокрема Cyber Resilience Review (CRR), що базується на моделі зрілості CERT-RMM. Науковий зміст цих інструментів полягає у переході від перевірки наявності технічних засобів захисту до аналізу стабільності бізнес-процесів. Агентство активно сприяє розвитку «колективної стійкості» через створення центрів обміну інформацією (ISACs) за галузевим принципом (енергетика, фінанси, водопостачання тощо). Це

дозволяє галузям самоорганізовуватися для відсічі складним загрозам. Окрім того, США активно використовують механізм «полювання на загрози» (threat hunting) як засіб проактивного забезпечення стійкості, що дозволяє виявляти зловмисників у мережі до того, як вони завдадуть непоправної шкоди [200].

Наукове пізнання американського досвіду також висвітлює роль приватного сектору та технологічних гігантів у підтримці національної стійкості. Компанії, такі як Microsoft, Google та Amazon, фактично формують «першу лінію оборони» через свої хмарні інфраструктури. Стратегія США заохочує міграцію державних сервісів у захищені хмарні середовища, що забезпечує географічну розподіленість даних та швидке відновлення після масштабних збоїв. У цьому контексті стійкість розглядається як економічний актив: інвестиції у стійку інфраструктуру знижують потенційні збитки від кіберзлочинності, які за оцінками експертів можуть сягати трильйонів доларів. Таким чином, модель США демонструє синергію між науковою думкою (NIST), державною волею (CISA) та технологічною потужністю приватного сектору, що робить її однією з найефективніших у світі.

Завершуючи аналіз, варто відзначити, що американська модель постійно еволюціонує у відповідь на нові виклики, такі як квантові обчислення та штучний інтелект. Наукова спільнота США вже працює над стандартами «постквантової стійкості», що свідчить про глибокий предиктивний характер цієї моделі. Для України досвід США є надзвичайно цінним у частині розбудови галузевих центрів стійкості та впровадження стандартів NIST як методологічної основи для захисту об'єктів критичної інформаційної інфраструктури. Вивчення цієї моделі дозволяє зрозуміти, що стійкість – це не кінцевий стан, а безперервний процес вдосконалення, заснований на даних, інноваціях та партнерстві.

Великобританія представляє одну з найбільш прогресивних моделей розбудови національної стійкості, де кібербезпека розглядається не просто як засіб захисту, а як фундаментальний компонент «кіберпотужності» (Cyber Power) держави. Науковий та стратегічний підхід Сполученого Королівства

базується на цілісному баченні, де стійкість інтегрована в усі сфери суспільного життя – від національної оборони до цифрової економіки. Особливий інтерес для наукового аналізу становить дворівнева модель реалізації цієї стратегії: загальнодержавний рівень (UK National Cyber Strategy) та регіональний рівень на прикладі Шотландії (Cyber Resilience Strategy for Scotland), що дозволяє забезпечити максимальне охоплення та адаптивність заходів безпеки.

Центральним вектором Національної кіберстратегії Великобританії (UK National Cyber Strategy) є перехід від реагування на інциденти до проактивного формування стійкого цифрового середовища. Стратегія визначає стійкість як здатність нації витримувати системні кібершоки без втрати стратегічної автономії. Науковий зміст британської моделі полягає у фокусі на «цілісному підході суспільства», де відповідальність за безпеку розподілена між урядом, приватним сектором та громадянами. Важливим інструментом реалізації цієї стратегії є Національний центр кібербезпеки (NCSC), який виступає єдиним вікном взаємодії та джерелом експертизи. Британський підхід акцентує увагу на зміцненні критичних ланцюгів постачання та інвестиціях у «наступну генерацію» технологій, що забезпечує стійкість системи на десятиліття вперед. У межах цієї парадигми кіберстійкість стає основою для «цифрової переваги», дозволяючи Великобританії залишатися впливовим гравцем на світовій арені [277; 336].

Натомість Шотландська стратегія кіберстійкості (Cyber Resilience Strategy for Scotland) демонструє унікальний приклад регіональної адаптації глобальних принципів. Якщо загальнобританська стратегія більше зосереджена на геополітичних аспектах та кіберпотужності, то шотландська модель фокусується на «людському капіталі» та економічному добробуті. Шотландія першою у світі інтегрувала кіберстійкість у концепцію національного добробуту (National Outcomes), розглядаючи безпечне цифрове середовище як базове право кожного громадянина та умову успішного бізнесу. Науковий зміст шотландського підходу базується на трьох стовпах: «люди,

місця та бізнес». Це означає, що стійкість вибудовується знизу вгору – через підвищення цифрової грамотності населення, зміцнення локальних громад та підтримку малого й середнього бізнесу. Шотландська модель доводить, що навіть за обмежених політичних повноважень регіон може досягти високого рівня захищеності через розбудову мережевої співпраці та формування культури відповідальності [400].

Компаративний аналіз цих двох рівнів виявляє цікаву синергію. Великобританія на загальнодержавному рівні забезпечує високу технічну експертизу та розвіддані про загрози, тоді як Шотландія реалізує ці знання через прикладні програми навчання та підтримки конкретних секторів економіки. Важливим аспектом шотландського досвіду є концепція «економічної можливості»: стійкість не сприймається як витрата, а як шанс для місцевих ІТ-компаній розробляти інноваційні рішення, що згодом експортуються на світовий ринок. Такий підхід робить кіберстійкість драйвером інновацій, а не гальмом для розвитку. Більше того, Шотландія активно впроваджує стандарти кіберстійкості у державні закупівлі, змушуючи приватних підрядників дотримуватися високого рівня захисту як умови співпраці з урядом, що є ефективним механізмом «м'якого» регулювання ринку [417, с. 96].

Окремим елементом британського досвіду, який заслуговує на наукову увагу, є інтеграція кіберстійкості з фізичною безпекою та управлінням кризами. У межах ініціативи «Stronger together», Великобританія відпрацьовує сценарії, де кібератака є частиною ширшої гібридної агресії, що зачіпає енергетику та транспорт. Досвід NCSC у наданні автоматизованих послуг захисту (наприклад, Web Check та Mail Check) для малих організацій демонструє, як держава може масштабувати безпеку через технологічні інструменти. Це дозволяє створювати «колективний імунітет» нації, де стійкість кожного окремого суб'єкта посилює загальну стабільність держави. Таким чином, британська та шотландська моделі доповнюють одна одну,

створюючи багат шарову систему захисту, яка є водночас технологічно потужною та соціально адаптованою.

Для України досвід Великобританії та Шотландії є надзвичайно актуальним у контексті децентралізації та розбудови регіональних центрів стійкості. Поєднання жорсткого стратегічного управління на рівні центру з гнучкими, людиноцентричними програмами на рівні громад є тим ключем, який дозволить Україні підвищити життєздатність своєї критичної інфраструктури в умовах тривалих воєнних викликів. Вивчення цих моделей підтверджує, що кіберстійкість – це не лише про сервери та код, а насамперед про людей, їхню обізнаність та здатність діяти злагоджено під час кризи.

Наукове пізнання світового досвіду було б неповним без аналізу вертикальних, галузевих стратегій, де стійкість набуває специфічного прикладного змісту. На відміну від загальнодержавних фреймворків, галузеві стандарти фокусуються на забезпеченні життєздатності операційних технологій (ОТ) та кіберфізичних систем, де збій може призвести не лише до втрати даних, а й до екологічних катастроф або людських жертв. Найбільш репрезентативним у цьому контексті є досвід морської галузі та промислового сектору, де стійкість інтегрується безпосередньо в інженерні цикли та процеси сертифікації об'єктів.

У морській індустрії провідну роль у формуванні стандартів стійкості відіграє Міжнародна асоціація класифікаційних товариств (IACS). Науковий зміст підходу IACS полягає у визнанні того, що сучасне судно – це складна мережа взаємопов'язаних систем управління, які є вразливими до кіберзагроз. Впровадження Уніфікованих вимог (UR), таких як UR E26 та UR E27, ознаменувало перехід до обов'язкового проектування суден із врахуванням кіберстійкості. Вимога UR E26 («Кіберстійкість суден») визначає судно як цілісний об'єкт і вимагає від судновласників та верфей інтегрувати стійкість у всі етапи – від розробки концепції до експлуатації. Це включає обов'язкову сегментацію бортових мереж, захист навігаційних систем та систем управління енергетичними установками. Важливо, що IACS розглядає

стійкість через призму безпеки мореплавства, що робить кіберзахист невід'ємною частиною технічного нагляду за флотом. Такий підхід гарантує, що навіть у разі успішної кібератаки судно зберігає здатність до безпечного маневрування та повернення в порт [208; 209].

Паралельно з морською галуззю, значного прогресу у пізнанні стійкості досяг промисловий сектор, особливо в контексті впровадження Промислового Інтернету речей (IIoT) та критичних енергетичних систем. Наукові дослідження у цій сфері підкреслюють унікальність промислової стійкості, де пріоритет «цілісність–доступність» домінує над «конфіденційністю». Кіберстійкість промислових систем (Industrial Cyber Resilience) базується на стандартах серії IEC 62443, які визначають рівні безпеки для систем автоматизації та управління (IACS). Ключовим аспектом тут є здатність системи до самовідновлення без зупинки технологічного процесу. Тому стійкість промислових об'єктів досягається через глибоку ешелонованість захисту та використання детермінованих мереж, де час затримки сигналу є критичним параметром [350]. У енергетичному секторі стійкість пізнається як спроможність енергомережі до автономного функціонування у разі кіберураження центральних диспетчерських пунктів, що забезпечує безперервність енергопостачання критичних об'єктів [187, с. 6].

Специфіка галузевих підходів також виявляється у методах тестування та верифікації. У морській та промисловій сферах дедалі частіше використовується концепція «цифрових двійників» (Digital Twins) для моделювання поведінки систем під впливом кібератак. Це дозволяє науково обґрунтовувати межі витривалості обладнання та розробляти алгоритми «граціозної деградації» ще до моменту фізичного впровадження технологій. Більше того, галузеві стандарти (наприклад, IACS Rec. 166 [365]) детально регламентують процедури оновлення програмного забезпечення на віддалених або автономних об'єктах, що є критичним для підтримання стійкості протягом тривалого життєвого циклу обладнання (15–20 років). Таким чином, галузева стійкість стає синергією класичної інженерії та

передової кібернетики, де кожне технічне рішення оцінюється з точки зору його впливу на загальну виживаємість системи.

Аналіз спеціалізованих підходів дозволяє виділити загальну світову тенденцію: перехід від загальних рекомендацій до жорстких галузевих регламентів, що мають силу закону або обов'язкового технічного стандарту. Це особливо актуально для України, яка має потужний енергетичний, транспортний та промисловий потенціал. Адаптація вимог IACS для морського сектору та стандартів ІЕС 62443 для промисловості дозволить створити надійний каркас національної кіберстійкості, що базується на кращих світових інженерних практиках. Вивчення галузевого досвіду доводить, що універсальні стратегії кібербезпеки повинні обов'язково доповнюватися глибокою технологічною експертизою, що враховує специфіку конкретних фізичних процесів.

Завершуючи цей блок, варто зазначити, що галузева стійкість є найбільш динамічною ділянкою наукового пізнання. Вона вимагає постійного оновлення через швидкий розвиток автоматизації та впровадження штучного інтелекту в управління інфраструктурою. Світовий досвід показує, що лише ті галузі, які змогли інтегрувати кіберстійкість у свій «генетичний код» через стандарти та інженерну культуру, виявляються здатними успішно протистояти викликам сучасної епохи кіберфізичних воєн.

Аналіз глобальних стратегій та моделей забезпечення кіберстійкості у розвинених країнах дозволяє сформулювати цілісне бачення того, як Україна може інтегрувати світові здобутки у власну систему національної безпеки. Світовий досвід переконливо доводить, що кіберстійкість є не лише технічним станом, а комплексною стратегічною спроможністю, яка вимагає гармонізації законодавства, інженерних стандартів та організаційної культури. Синтез підходів ЄС, США та Великобританії створює надійний методологічний фундамент для розбудови вітчизняної екосистеми стійкості, що базується на принципах проактивності, адаптивності та колективної відповідальності.

Найбільш пріоритетним вектором для України є адаптація європейської нормативної бази, зокрема регламентів CRA та NIS2. Впровадження принципів EU Cyber Resilience Act дозволить встановити чітку відповідальність постачальників цифрових продуктів за вразливості, що є критичним в умовах активного використання ворогом програмних закладок та нуль-денних експлуатацій. Україна має перейти від моделі добровільного дотримання стандартів до обов'язкової сертифікації продуктів із цифровими елементами, що входять до критичної інфраструктури. Це дозволить створити «фільтр» для небезпечного обладнання та програмного забезпечення, підвищуючи базовий рівень стійкості державних інформаційних систем та приватних мереж, від яких залежить життя громадян.

Від американської моделі (NIST/CISA) Україні доцільно запозичити гнучкість інженерних фреймворків та фокус на «нульовій довірі» (Zero Trust). Впровадження стандартів NIST SP 800-160 у практику проектування національних кіберсистем забезпечить їхню спроможність до «граціозної деградації» – здатності виживати під час кібератак за рахунок сегментації та ізоляції уражених вузлів. Більше того, досвід CISA у розбудові галузевих центрів обміну інформацією (ISACs) є життєво необхідним для України, оскільки він дозволяє поєднати зусилля держави та приватного сектору у виявленні та нейтралізації гібридних загроз у реальному часі. Створення таких центрів у енергетиці, транспорті та фінансовій сфері дозволить сформувати «колективний імунітет» проти зовнішньої агресії.

Водночас, Британський та шотландський досвід акцентує увагу на важливості соціотехнічного виміру стійкості. Україні необхідно розвивати не лише технічні спроможності, а й «людський капітал», залучаючи широкі верстви населення до формування культури кіберстійкості. Регіональний підхід Шотландії, де стійкість розглядається як запорука соціального добробуту, може стати моделлю для українських територіальних громад, особливо в умовах децентралізації. Створення локальних програм підтримки

цифрової витривалості малого бізнесу та органів місцевого самоврядування дозволить уникнути каскадних збоїв у наданні критичних послуг на місцях.

Нарешті, галузевий підхід (IACS/IEC) демонструє важливість інтеграції кіберстійкості безпосередньо в операційні технології. Україна, як велика промислова та морська держава, має імплементувати жорсткі вимоги до кіберстійкості промислових систем управління (ICS) та морської інфраструктури на рівні технічних регламентів. Вивчення досвіду IACS UR E26/E27 доводить, що кіберзахист має бути невід'ємною частиною інженерної безпеки об'єктів, що дозволяє мінімізувати фізичні наслідки кіберінцидентів. Це вимагає тісної співпраці між регуляторами кібербезпеки та галузевими наглядовими органами задля створення єдиного безпекового простору.

Підсумовуючи, адаптація світового досвіду для України не повинна бути сліпим копіюванням, а має бути творчим синтезом найкращих практик, адаптованих до умов постійного воєнного протистояння. Формування національної системи кіберстійкості на основі європейського права, американських інженерних стандартів та британських соціотехнічних стратегій дозволить Україні не лише ефективно протидіяти поточним викликам, а й стати надійним форпостом цифрової безпеки всього європейського континенту. Стійкість держави починається з визнання того, що цифрова безпека є спільним благом, а здатність швидко відновлюватися після ударів є вищим показником національної потужності у XXI сторіччі.

Висновки до розділу 1

Проведене комплексне дослідження генезису поняття «стійкість» дозволило встановити його міждисциплінарну природу та еволюційну траєкторію від технічних і екологічних систем до складних соціо-кібернетичних структур. Науковим результатом є доведення того, що сучасна концепція кіберстійкості не є простою ітерацією кібербезпеки, а виступає

якісно новим етапом розвитку системної інженерії та теорії управління ризиками. Виявлено, що перехід від «статичної стійкості» (здатність повертатися до вихідного стану після шоку) до «динамічної адаптивності» (здатність розвиватися під тиском) є ключовим для функціонування в умовах сучасних АРТ-загроз. Дослідження підтвердило, що історичне коріння стійкості в екології (праці Голлінга) заклало фундамент для розуміння системи як такої, що має кілька станів рівноваги, що трансформувало підхід до кіберсистем: від спроб побудувати «непроникну стіну» до створення архітектур, здатних «граціозно деградувати» без повної втрати працездатності.

Крім того, теоретичний аналіз дозволив виокремити специфічні властивості кіберстійкості, такі як емерджентність та самоорганізація. Обґрунтовано, що актуалізація кіберстійкості у науковому дискурсі останнього десятиліття спричинена неможливістю класичних методів захисту гарантувати цілісність систем у середовищі з високим рівнем невизначеності. Це дало змогу сформулювати авторське бачення стійкості як здатності системи підтримувати цільову спрямованість дій навіть за умови часткового успіху атаки противника. Таким чином, сформовано фундаментальне розуміння того, що стійкість є процесом, а не кінцевою точкою, що вимагає постійного циклу навчання та корекції архітектурних рішень відповідно до динаміки загроз.

Досліджено також детермінації внутрішньої структури кіберстійкості та механізмів її реалізації. Основним науковим результатом тут є розробка та обґрунтування чотирьохкомпонентної функціональної моделі стійкості: «передбачати (anticipate), витримувати (withstand), відновлюватися (recover) та адаптуватися (adapt)». На відміну від існуючих підходів, доведено критичну важливість фази «адаптації» як завершального етапу життєвого циклу стійкої системи, що забезпечує інкорпорацію досвіду подолання інциденту в майбутні захисні механізми. Встановлено, що кіберстійкість оперує не лише технічними показниками, а й категоріями довіри та цілісності функцій, що дозволяє

розглядати її як стратегічну характеристику життєздатності організації чи держави.

Особливу увагу приділено аналізу взаємозв'язку між кібербезпекою та кіберстійкістю. Науково аргументовано, що ці поняття перебувають у стані комплементарності: якщо безпека мінімізує ймовірність реалізації загрози, то стійкість мінімізує наслідки її неминучої реалізації. Доведено, що впровадження технік кіберстійкості (таких як адаптивна диверсифікація, обманні технології та сегментація) дозволяє радикально підвищити вартість атаки для зловмисника, роблячи її економічно та технічно недоцільною. Цей результат має важливе значення для проектування систем критичної інфраструктури, де фізичні наслідки кіберзбоїв можуть бути катастрофічними. Розділ також розкриває роль «людського фактора» та організаційних процесів як невід'ємних складників кіберстійкості, що виводить дослідження за межі чисто технічного домену в площину комплексного системного управління. Сформована логіка функціональних компонентів дозволяє перейти до розробки конкретних метрик та інструментів вимірювання стійкості на наступних етапах дослідження.

Здійснено системний аналіз глобальних та національних стратегій розбудови систем кіберстійкості. Науковим результатом розділу є критичне оцінювання світових стандартів (NIST SP 800-160, ISO/IEC 27031, директиви NIS2) та їх адаптація до національного безпекового контексту. Виявлено, що найбільш прогресивні моделі (зокрема MITRE CREF) базуються на принципі «спільної відповідальності» та активного державно-приватного партнерства.

Доведено, що розбудова національної кіберстійкості потребує створення екосистеми, яка включає не лише регуляторні вимоги, а й механізми швидкого обміну інформацією про інциденти та спільні плани відновлення. Аналіз досвіду провідних країн (США, Великої Британії, Естонії) дозволив виділити ключові індикатори зрілості національної системи кіберстійкості, серед яких – рівень автоматизації захисту та швидкість адаптації до нових типів атак. Важливим висновком блоку є твердження про те, що національна

кіберстійкість є похідною від стійкості окремих суб'єктів (від малого бізнесу до великих держкорпорацій), що потребує диференційованого підходу до встановлення вимог безпеки. Обґрунтовано необхідність впровадження ризик-орієнтованого підходу на державному рівні, де пріоритетність захисту визначається соціально-економічною значущістю функцій, що підтримуються цифровими системами. Зазначено на необхідності логічного переходу від філософських та інженерних аспектів до рівня державної політики та стратегічного управління, що створює плацдарм для подальших юридичних розробок кіберстійкості.

РОЗДІЛ 2

ОРГАНІЗАЦІЙНО-ПРАВОВІ НАПРЯМИ ТА ЗМІСТ ІНСТИТУАЛІЗАЦІЇ КІБЕРСТІЙКОСТІ

2.1. Інституціоналізація кіберстійкості

Витонченість та зростаючі частота й інтенсивність кібератак, спрямованих на установи у кіберпросторі, підкреслюють їх високу ризиковість та складність повноти захисту цілісності критично важливих об'єктів та систем. У цьому контексті кіберстійкість пропонує привабливу додаткову альтернативу існуючій парадигмі кібербезпеки. Загалом кіберстійкість визначається як здатність протистояти зовнішнім потрясінням, спричиненим кіберризиками, відновлюватися після них та адаптуватися до них. Водночас, запити сучасного суспільства щодо поширення кіберстійкості потребують конкретизації заходів, методів та інструментів, що вирішують такого роду завдання [101, с. 31].

Кіберстійкість останнім часом стала однією з найбільш розкручених концепцій в дискусіях про кібербезпеку. Зокрема, виділяється три типи інституційних підходів, що забезпечують певні галузеві заходи кіберстійкості [101, с. 31; 232, с. 6]: маркетинг, стандартизація та регулювання. Кожен підхід реалізується певною групою інституцій, які переслідують різні цілі і можуть використовувати широкий набір ресурсів, які варіюються від простого переконання та стимулювання до примусу. Кожна з цих груп має своє розуміння кіберстійкості та шляхів її досягнення.

Маркетинг кіберстійкості. Інституціоналізація через механізми маркетингу базується на формуванні ринкового попиту на високий рівень захищеності як конкурентну перевагу. У цьому ракурсі кіберстійкість виходить за межі суто ІТ-функції, інтегруючись у стратегічне корпоративне управління (Cyber Governance). Важливим інструментом тут постає

кіберстрахування, яке виконує роль непрямого регулятора: встановлюючи вимоги до аудиту та відповідності стандартам (ISO/IEC 27001, NIST) як умову страхового покриття, воно стимулює суб'єктів господарювання до безперервного самовдосконалення систем захисту. Таким чином, ринкові інституції створюють економічні стимули для інвестицій у стійкість, що доповнює державний примус.

Протягом 2013-2018 років кіберстійкість стала основною темою в постійному потоці звітів, що випускаються процвітаючою індустрією кібербезпеки. Щонайменше 11 компаній, що продають консалтингові послуги (Accenture, EY, McKinsey, PwC), сертифікацію найкращих практик (Axelos), страхування (American International Group), програмне та апаратне забезпечення для забезпечення безпеки (Cisco, IBM, Symantec, UpGuard) або послуги з управління безпекою (SecureWorks) випустили маркетингові матеріали, які визначають переваги кіберстійкості та знайомлять існуючих або потенційних клієнтів з тим, що, на їхню думку, є майбутнім кібербезпеки. Одна компанія навіть заявила, що «кібербезпека померла», наводячи переконливі аргументи на користь кіберстійкості як єдиної життєздатної моделі, що залишилася [27, с. 31-32; 207].

Для кращого розуміння інструментальної природи концепції кіберстійкості та неоднорідності її значення в індустрії кібербезпеки, було узагальнено звіти цих компаній та визначено концептуальні елементи притаманні кіберстійкості [27, с. 32; 232].

Незважаючи на активну пропаганду, менше половини (4 з 11) проаналізованих звітів надали визначення того, що таке кіберстійкість. Хоча більшість цих визначень містять звичайні посилання на підготовку, виявлення, реагування на інциденти та пом'якшення наслідків, деякі з них були більш загадковими і межували з грандіозними, як, наприклад, визначення UpGuard: «Кіберстійкість – це спосіб використання технологій на підприємстві для досягнення успіху» [207]. Сім звітів, які не надають робочого визначення, припускають, що концепція кіберстійкості є самозрозумілою або інтуїтивно

зрозумілою для фахівців-практиків. Таким чином, кіберстійкість визначається не стільки тим, чим вона є, скільки тим, що вона прагне замінити – застарілу модель традиційної кібербезпеки, яка не здатна впоратися зі складним і руйнівним характером кіберризиків. У жодному з 11 розглянутих звітів не міститься жодного посилання на більш загальну концепцію стійкості в таких галузях, як інженерія, управління катастрофами, управління соціально-екологічними системами або психологія, що ілюструє вузькість їхньої сфери застосування [27, с. 32].

Хоча визначення кіберстійкості є нечітким, перераховано широкий спектр складових технологій, процесів і практик, які демонструють зростання організаційної спроможності в цій сфері. В 11 звітах було виявлено дванадцять елементів кіберстійкості, перелічених у порядку зменшення частоти: спільна відповідальність (10), виявлення загрози (9), реагування на інциденти (9), запобігання (8), мапування ризиків (7), відновлення (6), мережевий потенціал (6), розробка кризових сценаріїв (5), моделювання (5), адаптація (5), цифрова криміналістика (2) і страхування (1) [27, с. 32].

Поняття спільної відповідальності, яке згадується найчастіше, стосується необхідності залучення більш широкого кола структурних підрозділів (разом з керівниками) до запобігання та пом'якшення кіберризиків, ніж це зазвичай має місце в більш традиційних підходах до кібербезпеки (визначення відповідальним директора з інформаційної безпеки (*Chief information security officers (CISO)*)) [27, с. 32].

Наступні три функції є більш технічно орієнтованими на контроль, виявлення та реагування на кіберінциденти. Цікаво відзначити, що більш запобіжного характеру заходи, такі як мапування ризиків, розробка кризових сценаріїв і моделювання інцидентів, а також заходи, спрямовані на відновлення, співпрацю з третіми сторонами та адаптацію, рекомендуються більш епізодично. Трансформаційний потенціал кіберстійкості згадується лише двічі [207; 390], можливо, тому, що 11 досліджуваних компаній не пропонують конкретних продуктів і послуг для підтримки цієї більш

розрізної діяльності. Нарешті, такі особливі заходи, як цифрова криміналістика та кіберстрахування, пропонуються лише компаніями, які працюють у цих конкретних сегментах ринку кібербезпеки [27, с. 32-33].

Водночас, у зазначених звітах прослідковується прямий зв'язок між пропагованими шляхами до кіберстійкості та продуктами і послугами, які пропонують корпоративні спонсори цих звітів. Зокрема, документ компанії Symantec закінчується прямим запрошенням до читача *«зв'язатися з представником Symantec, щоб обговорити, як можна почати впроваджувати кіберстійкість в стратегію безпеки»* [397], звіт Cisco підкреслює, як її технічні продукти можуть бути використані для підвищення стійкості мережевої архітектури [211], а UpGuard розкидає скріншоти своєї платформи CSTAR у своєму звіті, щоб проілюструвати, як вона може допомогти клієнтам реалізувати конкретні цілі кіберстійкості (за визначенням компанії) [27, с. 33].

Зазначене свідчить, перш за все, про упередженість та обмеженість поглядів на кіберстійкість, на які значною мірою впливають інтереси їхніх спонсорів, і що їхній внесок у загальну скарбничку знань про кіберстійкість залишається досить скромним [27, с. 33].

Водночас, мають місце і більш глибокі та системні підходи. Існує кілька винятків: звіти PwC та Accenture включають результати опитувань, проведених серед 9 500 та 4 600 міжнародних керівників відповідно [250; 390], тоді як IBM замовляє щорічне дослідження кіберстійкості від Ponemon Institute [401]. Незважаючи на ці нечисленні спроби розробити більш систематизовану базу знань про поширеності практик кіберстійкості в організаціях, більшість галузевих звітів залишаються нормативними, не розкриваючи доказів що підтверджують їхні приписи. У цьому відношенні деякі звіти майже копіюють рамки кіберстійкості, які були розроблені організаціями зі стандартизації [27, с. 33].

Стандартизація кіберстійкості. Стандарт можна визначити як правило або норму, яку можна виміряти, випробувати, дослідити і переглянути, а іноді його описують як «рецепт реальності» [183]. Стандарти застосовуються до

продуктів, процесів або людей і стали повсюдними у складному світі, де потоки товарів, інформації, грошей і людей мають бути скоординовані та синхронізовані в глобальному масштабі. Стандарти, хоча часто невидимі, підтримують технічну та організаційну інфраструктуру, які уможливлюють сучасне життя [27; 261; 386]. Тому вони відіграють центральну роль в управлінні ризиками, допомагаючи зменшити невизначеність та інформаційну асиметрію, які ускладнюють взаємодію між партнерами. Навіть необов'язкові стандарти, які здаються несуттєвими і нейтральними, мають велику силу, оскільки вони контролюють «можливість встановлювати правила, яких дотримуються інші, або встановлювати перелік критеріїв, з якого вони можуть обирати» [183]. Поширення стандартів було прискорене зростанням кількості національних і міжнародних органів, що встановлюють стандарти органів, які об'єднують державні та галузеві зацікавлені сторони [178].

У сфері кібербезпеки домінують два загальні стандарти, які включають заходи, сумісні з підходом до кіберстійкості: стандарти Міжнародної організації зі стандартизації (*International Organization for Standardization (ISO)*) 27000-серії щодо стандартів інформаційної безпеки та Національного інституту стандартів і технологій (*National Institute of Standards and Technology (NIST)*) [27, с. 33].

Міжнародна організація зі стандартизації (ISO) базується у Швейцарії та об'єднує 163 національні органи стандартизації. З моменту свого створення у 1947 році вона розробила понад 22 000 стандартів. У співпраці з Міжнародною електротехнічною комісією (*International Electrotechnical Commission (IEC)*), вона підтримує набір з понад 40 стандартів інформаційної безпеки, які охоплюють широкий спектр питань, від створення спільної термінології до розробки та впровадження засобів контролю управління ризиками й найкращих практик реагування на інциденти до судових розслідувань [292]. Це сімейство стандартів бере свій початок з більш ранньої роботи Британського інституту стандартів, який прийняв кодекс практики управління інформаційною безпекою в 1995 році. Згодом цей стандарт був

гармонізований ISO і привів до створення стандарту ISO/IEC 27001 у 2005 році, за яким послідували 39 більш спеціалізованих, але все ще взаємопов'язаних стандартів [27, с. 34; 226, с. 98]. Стандарт ISO/IEC 27001 побудований навколо восьми функцій високого рівня, які варіюються від розуміння «контексту організації» до «лідерства», «планування», «підтримки», «документування інформації», «функціонування», «оцінювання результативності» та «вдосконалення». Зазначені пункти розбиті на 35 цілей і 114 засобів контролю (або заходів), які відповідають вимогам цього стандарту. Складність цієї структури ускладнюється тим, що ці заходи не представлені та не обговорюються в порядку пріоритетності впровадження, що може зробити їх імплементацію непосильним завданням навіть для організації, яка бажає їх запровадити. Станом на 2017 рік було видано понад 39 000 чинних сертифікатів організаціям, які продемонстрували свою відповідність стандарту, але половина з них була сконцентрована в п'яти країнах (Японія, Великобританія, Індія, Китай, Німеччина), що ілюструє постійний низький рівень та нерівномірність прийняття стандарту у порівнянні з набагато більш успішною серією стандартів ISO 9000 [27; 244].

Хоча сімейство стандартів серії 27000 явно не включає стійкість як одну зі своїх цілей, вона рекомендує багато заходів які сприяють кіберстійкості організації, такі як «обізнаність, освіта та навчання з питань інформаційної безпеки», «резервне копіювання інформації», «планування безперервності інформаційної безпеки» або «навчання на основі інцидентів інформаційної безпеки», і це лише деякі з них. Комітет, відповідальний за розробку цього сімейства стандартів (відомий як ISO/IEC JTC 1/SC 27), також регулярно підтримує зв'язок з Комітетом ISO з питань стійкості (ISO/TC 292, який відповідає за стандарт ISO 22316) стандарт організаційної стійкості ISO 22316, оновлений у 2017 році), а також з комітетом з управління ризиками та безпеки (ISO/TC 262). Більш сфокусований стандарт (ISO/IEC 27035) містить набір настанов щодо планування, підготовки та проведення заходів з реагування на кіберінциденти. Відповідність цьому стандарту дає організаціям можливість

протистояти неочікуваним та невідомим загрозам, а його п'ять етапів відображають динамічну природу кіберстійкості: планування та підготовка, виявлення та інформування, оцінка та прийняття рішень, реагування та засвоєння уроків [291]. Її більш детальні заходи також підкреслюють мережеві, практичні та адаптивні виміри стійкості [27, с. 35].

Другий стандарт кібербезпеки, який привернув великий міжнародний інтерес, незважаючи на своє національне походження, був розроблений в США Національним інститутом стандартів і технологій (NIST). Створений у 1901 році, NIST описує себе як нерегулятивне федеральне агентство, яке надає технології, вимірювання та стандарти для промисловості США з метою підвищення їхньої конкурентоспроможності [27, с. 35].

Кібербезпека – це добровільний інструмент, спочатку розроблений за вказівкою Білого дому і запущений у 2014 році з метою покращення цифрової безпеки критично важливої інфраструктури [278]. Рамкова концепція кібербезпеки, що з'явилася в результаті тривалих консультацій з широким колом зацікавлених сторін у промисловості, уряді та академічних колах, має на меті консолідувати існуючі стандарти та практики, а також виявити прогалини, для усунення яких необхідні оновлені або нові стандарти [27; 248]. На відміну від свого аналога ISO, який має бути придбаний компаніями і надає сертифікат відповідності, що видається акредитованою третьою стороною, Рамка кібербезпеки NIST є безкоштовною і не підтримується формальним процесом оцінки відповідності, а це означає, що її впровадження залишається пристосованим до індивідуальних потреб і можливостей кожної організації, що приймає її.

Рамкова програма NIST організована навколо «ядра» з п'яти функцій (ідентифікація, захист, виявлення, реагування та відновлення), які, в свою чергу, поділяються на 23 категорії цілей і 108 підкатегорій результатів. Кожен результат співвідноситься з аналогічними заходами або засобами контролю, що містяться в інших стандартах кібербезпеки, таких як ISO/IEC 27001 або

COBIT – Control Objectives for Information and Related Technologies (*Цілі контролю для інформаційних та суміжних технологій*) [186; 219; 226].

Визнаючи, що організації значно відрізняються за своєю здатністю впроваджувати Рамкову програму, передбачено чотири «рівні впровадження»: частковий, з урахуванням ризиків, повторюваний та адаптивний [320; 376]. Кожен рівень фіксує прогрес у ступені кіберстійкості до більш цілісного, адаптивного та мережевого потенціалу. Бібліотека публікацій, організована за функціями, каталог історій успіху та щорічна конференція доступні для підтримки користувачів Рамкової програми у їхніх зусиллях з імплементації. Значна кількість категорій та підкатегорій де-факто орієнтовані на кіберстійкість (наприклад, тестування планів реагування та відновлення, впровадження механізмів для досягнення технічної стійкості в нормальних і несприятливих ситуаціях, пом'якшення наслідків інцидентів та включення отриманих уроків до планів відновлення), але, як і в стандарті ISO/IEC, немає чіткого розмежування між кібербезпекою та кіберстійкістю, а також не визначено пріоритетів чи ранжування заходів, щоб вказати ті з них, які є найбільш важливими, на відміну від тих, що є другорядними або повинні розглядатися лише найбільш зрілими адептами [63, с. 710; 202, с. 73].

У березні 2018 року NIST опублікував проект документа, в якому викладено набір керівних принципів і просить надати коментарі щодо того, як слід розробляти кіберстійкі системи [372]. Ця публікація, яка не пов'язана з Рамковою концепцією кібербезпеки, використовує суто технічний підхід, який менше стосується загальної стійкості організацій, що стикаються з кібершоком, ніж живучості їхніх цифрових активів. Незважаючи на вужчу спрямованість, цей майбутній стандарт чітко узгоджує свої принципи побудови з чотирма цілями кіберстійкості – передбачення, протистояння, відновлення та адаптація, а також з більш конкретним набором з 8 цілей і 14 методів, мотивованих попередніми дослідженнями, проведеними на початку 2010-х років у MITRE Corporation [27, с. 32-36; 167; 372].

Виходячи за межі загальних стандартів кібербезпеки, запроваджених ISO/IEC і NIST, були запропоновані більш спеціалізовані стандарти щодо різних етапів і сфер кіберстійкості. Найбільш детальним з них є Модель управління стійкістю CERT (CERT-RMM), розроблена підрозділом Інституту інженерії програмного забезпечення Університету Карнегі-Меллона [186]. Цей 860-сторінковий документ надає всеосяжну структуру операційної стійкості що є результатом формалізації та консолідації найкращих практик на стику IT-безпеки, безперервності бізнесу та реагування на катастрофи. CERT-RMM прагне знайти шляхи для декомпозиції та інституціоналізації кіберстійкості, а також визначити правильний баланс між технічними та організаційними заходами, необхідними для її посилення, наголошуючи на необхідності підтримування високого рівня контекстуальної та ситуативної обізнаності, розвитку мережових та відпрацьованих навичок управління загрозами та посилення адаптивних можливостей. Вона організована навколо 26 сегментів процесу, які розбиті на 94 конкретні цілі і 256 конкретних практик. Як і в NIST, можливим є відображення у форматі детальної таблиці перехресних посилань певних відповідностей і прогалів з іншими стандартами, такими як ISO/IEC, COBIT та багатьма іншими практиками. Розроблений на цій основі інструмент самооцінки, який більше зосереджений на кіберризиках і сумісний із NIST, доступний за-для допомогти організаціям в оцінюванні власного рівня кіберстійкості [50; 186].

Водночас, Агентство Європейського Союзу з мережевої та інформаційної безпеки (*European Union Agency for Network and Information Security (ENISA)*) з 2009 року здійснює моніторинг та доповнює роботу органів стандартизації у сфері кібербезпеки, де кіберстійкість є особливою сферою інтересів [363]. У 2009 році видано посібник з передової практики щодо розробки, проведення та оцінки національних навчань з підвищення кіберстійкості публічних комунікаційних мереж [260]. У 2011 році опубліковано технічний звіт, в якому було розглянуто існуючі системи вимірювання та метрики для стійких мереж і послуг і, нарікаючи на

відсутність стандартизованої системи, запропоновано уніфіковану таксономію для використання організаціями [236]. Агенцією також розроблена онлайн-платформа, яка підтримує роботу експертних груп, що розробляють галузеві настанови з кіберстійкості [50].

Всесвітній економічний форум (*The World Economic Forum*), хоча технічно не є органом зі стандартизації, також визначив кіберстійкість одним зі своїх пріоритетних питань, що відображає зростання кіберризиків як однієї з двох основних проблем, що турбують його членів (поряд з екологічними ризиками) [398]. У відповідь на це розроблено систему кіберстійкості для рад директорів, яка містить набір з 10 принципів і 47 детальних питань, що представляють елементи або заходи, які, як вважається, посилюють управління діяльністю з кіберстійкості у цій сфері [141].

Усі розглянуті вище добровільні стандарти, як загальні, так і спеціалізовані, мають спільне базове припущення: вони неявно припускають, що кіберстійкість може бути досягнута майже механічно, шляхом трудомісткого впровадження довгого переліку надмірно деталізованих технічних та організаційних заходів контролю. У цій домінуючій моделі, мотивованій інженерним мисленням, здатність поглинати, протистояти і адаптуватися до кібершоків розглядається як результат кумулятивного і стабільного процесу, в якому заходи, хоч і вважаються однаковим внеском у кінцевий результат, все ж не представляються у певному порядку важливості. При такому підході втрачається непередбачуваний, несподіваний і дестабілізуючий характер кіберкриз і необхідність розвитку загальних ресурсів та спроможностей, які можуть адаптуватися і вистояти [27, с. 37].

Регулювання кіберстійкості. Зростаюча ймовірність і серйозність кіберризиків, що впливають на різні установи і здатні дестабілізувати цілі системи (фінансові, енергетичні, телекомунікаційні тощо), підштовхнуло регуляторні органи до розробки широкого спектру заходів з оцінки та комплаєнсу, з метою посилення кіберстійкості установ, за якими вони здійснюють нагляд. У питаннях регулювання кіберстійкості визнається, що не

всі організації бажають або можуть добровільно прийняти стандарти і практики, які покращать їхню здатність витримувати кібершок. Однак, враховуючи гіперзв'язане та взаємозалежне середовище, в якому працюють ці організації, такий брак занепокоєння та бездіяльності може стати джерелом спільних втрат. Тому деякі регулятори вивчають низку стратегій, що охоплюють повний спектр піраміди комплаєнсу – від підвищення обізнаності та освіти до більш жорстких форм взаємодії та правозастосування. Ідея піраміди комплаєнсу запозичена з роботи Айреса та Брейтуейта [154], з її основним принципом «безпечної великої гармати», який полягає в тому, що ескалація правозастосовної практики повинна розглядатися як спосіб індивідуалізації інтенсивності регуляторної діяльності відповідно до поведінки окремих суб'єктів. Стратегією у цьому контексті є неінтрузивне та делеговане регулювання, яке з більшою ймовірністю сприятиме співпраці між приватними суб'єктами, оскільки дозволяє їм на власний розсуд вирішувати, як найкраще досягти регуляторних цілей, зокрема підвищення кіберстійкості. Маючи справу з приватними суб'єктами, які не бажають або не можуть впроваджувати ефективні стратегії, держава зберігає можливість ескалації свого втручання, переходу до адміністративних методів регулювання, які передбачають різні форми впливу. Ця теорія глибоко вкорінена в стратегії відповідальності, описаній Гарландом, згідно з якою державні органи *«формують стратегічні відносини з іншими силами соціального контролю [...] для створення широких альянсів, залучаючи повноваження приватних суб'єктів і формуючи їх відповідно до цілей контролю ...»* [253]. Але загальна стратегія є більш широкого діапазону, і не покладаючись виключно на механізми покарання і примусу, як це пропонує Гарланд, натомість розглядає більш повний перелік методів втручання які включають переконання та медіацію [175, с. 23]. У цьому відношенні, притягнення до відповідальності відбувається як добровільно, з власних інтересів, так і в результаті регуляторної діяльності держави [27, с. 36].

Особливої ваги у контексті нормативного регулювання набуває імплементація положень Директиви ЄС 2022/2555 (NIS2), яка детермінує кіберстійкість як об'єкт суворого державного нагляду. Інституціоналізація за цим підходом передбачає не лише впровадження технічних заходів захисту, а й встановлення чітких обов'язків щодо звітування про значні інциденти протягом жорстко визначених часових лімітів. Це трансформує роль суб'єкта кібербезпеки із пасивного реципієнта послуг захисту на активного учасника загальнодержавної системи моніторингу, де прозорість інцидентів стає передумовою для швидкого колективного відновлення інфраструктури

У контексті національної моделі забезпечення кіберстійкості України зазначені теоретичні підходи знаходять своє практичне втілення через чіткий розподіл повноважень між ключовими суб'єктами.

Зокрема, підхід «регулювання» реалізується переважно через діяльність Адміністрації Держспецзв'язку, яка як уповноважений орган у сфері захисту критичної інфраструктури, встановлює обов'язкові вимоги та регламенти для суб'єктів КІІ, здійснюючи державний нагляд за їх дотриманням. Паралельно з цим, Служба безпеки України в межах регуляторних повноважень забезпечує контррозвідувальний захист інтересів держави у кіберпросторі, фокусуючись на виявленні та нейтралізації загроз національній безпеці.

Функція «стандартизації» та розробки методичного забезпечення покладена на Національний координаційний центр кібербезпеки (НКЦК) при РНБО України, який виступає платформою для гармонізації національних стандартів із міжнародними (ISO/IEC, NIST). НКЦК забезпечує єдність підходів до оцінки ризиків та впровадження протоколів стійкості на рівні всієї держави, виконуючи роль методологічного хабу.

Маркетинговий підхід, що базується на стимулюванні ринку та формуванні культури кіберстійкості, активно реалізується через ініціативи Міністерства цифрової трансформації України. Шляхом популяризації цифрової гігієни, підтримки інноваційних стартапів у сфері Cybersecurity та

створення прозорих цифрових сервісів, Мінцифра формує суспільний та бізнесовий попит на безпечні технології.

Така функціональна детермінація дозволяє уникнути дублювання повноважень та забезпечує комплексне охоплення всіх аспектів інституціоналізації — від жорсткого нормативного примусу до ринкового стимулювання.

Захист критично важливих національних кібер-активів є основою для зусиль країн у сфері кібербезпеки. Для політиків, перед якими стоїть завдання розвивати національну систему кібербезпеки, питання визначення і захисту критично важливої інформаційної інфраструктури (далі ЗКІІ) змістилося від переважно фізичного розуміння інфраструктури до захисту критично важливих послуг. ЗКІІ використовується для узагальненого позначення захисту життєво важливих ІТ-сервісів, які підтримують надання критично важливих послуг як приватними, так і державними організаціями. [404]

Якщо поглянути на історію ЗКІІ, то цей термін з'явився під час холодної війни, коли перед оборонним відомством було поставлено завдання наглядати за критично важливими цивільними об'єктами. Визнаючи зростаючу залежність сучасного суспільства від цифрової інфраструктури, Комісія з питань захисту критичної інфраструктури при Президентів США у 1997 році підготувала звіт, який став першим відомим публічним документом, що обговорював кібербезпеку цілої нації. У ньому зазначалося «Одним з найважливіших є визнання того, що власники і оператори наших критично важливих об'єктів інфраструктури зараз знаходяться на передовій наших зусиль з забезпечення безпеки. Саме вони найбільш вразливі до кібератак. І ця вразливість ставить під загрозу нашу національну безпеку, глобальну економічну конкурентоспроможність і внутрішній добробут». [234]

Це питання, безумовно, є актуальним для багатьох країн і сьогодні через різке зростання залежності від цифрової складової сучасної економіки і суспільства. Тим не менш, обізнаність та ресурси, що виділяються на

національну кібербезпеку, залишаються дуже нерівномірними навіть серед індустріальних країн.

У той же час, кількість суб'єктів, потенційно здатних до незаконної кіберактивності з різних мотивів, стрімко зростає. З появою мільйонів нових інтернет-користувачів на ринках, що формуються, і в країнах, що розвиваються, відбудеться стрибок з 2,5 мільярдів інтернет-користувачів у 2015 році до 5 мільярдів користувачів до 2025 року. [257] Тому проблема кібербезпеки стає загрозою економічному зростанню та національній безпеці не лише в розвинених індустріальних країнах, а й у країнах з економікою, що розвивається.

Для покращення кібербезпеки критично важливих послуг основна увага має бути зосереджена на організаційних аспектах, а необхідні технічні компоненти – на вдосконаленому управлінні кіберризиками. Через складність захисту кібер-елементів критично важливих послуг, питання, на яке слід відповісти, в першу чергу, полягає в тому, як організувати це завдання і забезпечити необхідне лідерство уряду у протидії кібер-викликам. Нещодавні рекомендації Організації економічного співробітництва та розвитку (ОЕСР) дійшли висновку: «Замість того, щоб розглядати цифровий ризик як технічну проблему, яка вимагає технічних рішень, до нього слід підходити як до економічного ризику; отже, він повинен бути невід'ємною частиною процесів управління ризиками та прийняття рішень в організації». [221]

Наразі, має місце думка щодо певних проблем, пов'язаних з ідентифікацією ІТ-послуг, які підтримують найбільш критичні послуги. Наявність такого переліку критично важливих секторів є необхідністю, але насправді перелік критично важливої інфраструктури є досить загальними і теоретичними. [332, с. 22–23] Тому таке завдання буде мати місце постійно з метою більш детального визначення найбільш важливих послуг у кожному секторі і регулярне оновлення цього переліку, включаючи також нові послуги, що з'являються в онлайн економіці. Результат такої роботи буде різним у кожній країні, залежно від її економічної структури та інших факторів. Але

існують базові підходи до вирішення проблеми. Наприклад, послуга може вважатися життєво важливою для нації, якщо вона займає 5% ринку або створює понад 5% ВВП.

Перелік компаній та організацій, що надають найбільш важливі послуги, має визначатися тим самим міжвідомчим механізмом, який визначає найбільш важливі послуги. Водночас, такий перелік переважно є конфіденційним. Правило конфіденційності також слугує інтересам приватного сектору. Багато експертів можуть вважати, що формування переліку життєво важливих послуг та операторів забирає багато часу та коштів і не підходить для країн з великою кількістю критично важливих операторів. Але обмеження наприклад в 5% все ж формує певним чином помірний список найбільш важливих послуг. І якщо уряд вирішив розпочати державно-приватне партнерство, яке допоможе операторам критично важливих послуг захистити свої сервіси, чіткий поріг найбільш важливих допоможе спрямувати ресурси на центральні частини національної критично важливої інформаційної інфраструктури.

Компанії також можуть оцінити конкретний перелік послуг, оскільки він надає їм рекомендації щодо того, на чому слід зосередити зусилля з безпеки на додаток до їхніх ключових бізнес-операцій. Наприклад, компанії можуть дізнатися, що не всі послуги, які вони надають, вважаються критично важливими з національної точки зору, що дозволить їм не витратити занадто багато коштів на заходи безпеки. По-друге, точний перелік також полегшить подальший аудит та управління ризиками критично важливих операторів, що допоможе підвищити їхню загальну стійкість та зменшити ризики для ІТ-систем та мереж, що підтримують критично важливі послуги.

Важливим елементом розвитку системи ЗКІІ є державно-приватне партнерство. У більшості країн постачальники критично важливих послуг належать до приватного сектору. Тому уряди повинні прорахувати, на чому сконцентрувати свої зусилля, перш ніж звертатися до приватного сектору з проханням додати рівень додаткового захисту до певних послуг. Відомим є вислів у сфері кібербезпеки – «державно-приватне партнерство» – працює

лише тоді, коли обидві сторони домовилися про чіткий набір цілей і параметрів співпраці. [404, с. 99] Для стратегічного лідерства уряд повинен визначити, що захищати і як визначити критичні послуги. Він також повинен зібрати разом ключових галузевих і міжгалузевих гравців і запропонувати перелік стимулів для співпраці. Ці стимули можуть включати спеціалізоване навчання, огляд взаємозалежності між критично важливими операторами, спільні навчання, ресурси для фінансування резервного копіювання та засобів відновлення, а також інші вимоги, які диктуються інтересами національної безпеки.

Стандартне занепокоєння приватного сектору полягає в тому, щоб мати чітке розуміння того, що очікується від нього в рамках кіберпартнерства з урядом. Постачальники критично важливих послуг вже зобов'язані дотримуватися багатьох правил, а кібервимоги без чітких стимулів з боку уряду можуть не створити сприятливого клімату для покращення безпеки. Якщо компанії не помічають відповідних зусиль з боку урядів щодо інвестування в кіберстійкість, або якщо вони вважають, що всі кіберзадачі покладені виключно на них, це, ймовірно, не сприятиме кращому кіберзахисту нації. Тому успішне державно-приватне партнерство починається з правильного ставлення з боку урядів, з чітко визначеного національного бачення того, як досягти захисту критично важливих послуг, і розуміння того, який внесок обидві сторони зроблять для досягнення цієї мети.

Одним з найбільш важливих аспектів національної системи ЗКІ є пошук відповідної організаційної моделі, яка сприятиме ефективній та стабільній роботі в цій сфері. Достатньо глибокий аналіз акцентує увагу на різних моделях ЗКІ, і хоча немає двох абсолютно однакових моделей, все ж є певні закономірності, що склалися в Європі. Початково такі системи сформувалися в невеликих європейських країнах і здебільшого базувалися на міцних довірчих відносинах в однорідних суспільствах, де основна група критично важливих компаній і національних кіберорганізацій розробили системи обміну технічною кіберінформацією та раннього попередження з критично

важливими операторами. На початковому етапі було створено окремий орган ЗКІІ, який виконував лише політичні функції і діяв як національний координатор, здійснюючи нагляд і консультування критично важливих компаній і організацій. Водночас цей орган інформує політиків вищого рівня, проводить навчання, готує національні кібернавчання і підтримує зв'язок з ключовими державними установами. В ідеалі така установа повинна бути розташована разом з національною структурою реагування на інциденти (CERT), щоб мати технічну кібер-компетентність, а також мати доступ до оперативної інформації з кібербезпеки.

У деяких європейських країнах модель базується на галузевих підходах до ЗКІІ і тому відіграють більш важливу роль. Галузеві регулятори не обов'язково є найбільш компетентними кіберорганами, але оскільки ЗКІІ часто організована на галузевій основі, регулятори також мають мандат на нагляд за виконанням вимог щодо управління кіберризиками та звітності про інциденти. Цілісний підхід до ЗКІІ, коли кібербезпека інтегрована з фізичною та кадровою безпекою, добре слугує загальним цілям управління ризиками операторів критично важливих послуг. Деякі національні агентства ЗКІІ також демонструють здатність брати на себе наглядову і консультативну роль з питань ЗКІІ.

Існує також модель централізованого змісту з сильним кіберорганом в центрі національних зусиль, який має мандат на нагляд за реалізацією цілей ЗКІІ. У цьому випадку центральний орган також повинен мати можливість надавати корисні рекомендації та певну технічну допомогу постачальникам критично важливих послуг, а також не нехтувати галузевими специфікаціями у вимогах до кібербезпеки.

У більшості країн галузеві регулятори повинні бути більш обізнаними щодо кіберризиків і з часом відігравати певну роль в управлінні та нагляді за управлінням кіберризиками постачальників критично важливих послуг. Однак, оскільки багато європейських країн є малими або середніми державами, вони можуть не мати достатньої кількості кіберспеціалістів у всіх

галузових регуляторних органах, і було б економічно доцільно зосередити завдання з управління кіберризиками в національній організації ЗКІІ, яка тісно співпрацює з галузовими органами влади. В ЄС багато галузових вимог до безпеки визначаються загальноєвропейськими регуляторними органами. Ці гармонізовані європейські вимоги сприяють функціонуванню внутрішнього ринку та операторів критично важливих послуг, але національні уряди все одно здійснюють нагляд за виконанням нормативних актів.

Важливо зазначити, що кожна країна повинна знайти власну модель захисту критично важливих послуг у цифрову епоху. Досвід європейських країн показує, що центральним осередком національних зусиль у сфері кібербезпеки, як правило, є сильна державна установа з солідним фінансуванням і політичним керівництвом, орієнтованим на безпеку. Оскільки національна організація ЗКІІ повинна мати можливість залучати широке коло зацікавлених сторін з державного і приватного секторів, вона виграє від приналежності до національної установи, яка має прямий доступ до вищого політичного керівництва і володіє певним ступенем повноважень для здійснення нагляду.

Серйозний технологічний або антропогенний збій в інформаційній інфраструктурі може мати далекосяжні і непередбачувані наслідки. Теоретично, більшість критично важливих мереж в енергетиці, транспорті та інших життєво важливих секторах не повинні бути безпосередньо підключені до інтернету, а отже, повинні бути здатні уникнути збоїв. На практиці, навіть закриті об'єкти критичної інфраструктури або військові мережі можуть бути інфіковані і постраждати від наслідків кібервтрутлення. Усвідомлюючи неминучість кібервразливостей, політики почали шукати відповіді на них, щоб убезпечити критично важливу інфраструктуру. Саме тому, в Європі та США сформувався широкий консенсус щодо включення аспекту кіберстійкості в урядові та галузеві нормативні акти [29, с. 79; 404].

В умовах широкомасштабного вторгнення РФ, швидкої цифрової трансформації, яка змінює всі економіки і суспільства, важливо підвищувати

обізнаність про кіберзагрози як серед широкої громадськості, так і у приватному та державному секторах. Кібербезпека є одним із ключових елементів обороноздатності держави. Сьогодні кібервійна у розпалі. Російські хакери здійснюють цілеспрямовані атаки на органи влади та інфраструктурні підприємства для того, щоб знизити або паралізувати економічну активність громади, підвищити соціальну напругу через відсутність або не стабільну роботу підприємств, які забезпечують роботу критичної інфраструктури [29; 38; 373].

Ефективне реагування на кіберзагрози вимагає цілісного, загальнонаціонального підходу, в якому кібербезпека буде інтегрована у багатьох сферах державної політики. Таким чином можна створити середовище, яке буде відносно захищене від серйозних порушень, але це також буде тривалим процесом, який вимагає співпраці всіх основних зацікавлених сторін, включно з приватним сектором. Крім того, воно вимагає зміни мислення щодо того, наскільки впливовим стає цифрове підґрунтя та його незахищеність [29, с. 79].

Особи, відповідальні за розробку кіберполітики, стикаються зі складним завданням прийняття рішень, в яких переплітаються питання економіки, внутрішньої та національної безпеки, а окремі варіанти розроблених політик у кожній з цих сфер можуть суперечити одна одній. Країни, які хочуть бути кіберзабезпеченими, отримують вигоду саме від комплексної моделі кіберуправління, яка оцінюючи конкуруючі політичні пріоритети, здатна збалансувати національні інтереси в кіберпросторі. Національна кіберполітика має відношення до внутрішніх справ, безпеки і зовнішньої політики, промислової та економічної політики, а також політики у сфері досліджень, освіти та технологічного розвитку [300]. Для того, щоб збалансувати всі інтереси, політики також повинні регулярно консультуватися з приватним сектором. Національна кіберполітика повинна забезпечити стратегічне бачення, сформулювати варіанти політики і, що дуже важливо, виділити додаткові кошти для досягнення цілей кібербезпеки [29, с. 79].

Оскільки кіберпростір розвивається зі швидкістю інноваційного зростання, що стимулюється приватними компаніями, уряди мають різний ступінь здатності повністю орієнтуватися в цій швидкозмінній сфері. Уряди повинні швидко адаптуватися, щоб бути в змозі зрозуміти динаміку цифрової трансформації та йти в ногу з рівнем інновацій, навчання та інвестицій. Ключова сфера, з якою сьогодні стикаються національні розробники кіберполітики є захист мереж інформаційно комунікаційних технологій (далі ІКТ), які підтримують надання критично важливих послуг. Але їм також необхідно розвивати спроможність реагування на інциденти на національному рівні, що охоплює критично важливі організації приватного і державного секторів, а також розвивати спроможність розслідування кіберзлочинів та переслідування злочинців. Ці сфери політики формують базовий трикутник мінімальної національної кіберсистеми, здатної захищати критично важливі послуги, боротися з кіберзлочинністю та забезпечувати достатній потенціал реагування на інциденти [29, с. 80; 362, с. 282].

У кожній добре скоординованій національній кіберсистемі повинна існувати керівна структура, яка бере на себе відповідальність за прийняття рішень на вищому рівні. Її мандат полягає в тому, щоб забезпечити бачення, нагляд і ресурси для національних зусиль у сфері кібербезпеки. Керівна структура, еквівалент Національної ради з кібербезпеки, в ідеалі повинна підпорядковуватися вищому органу, який приймає рішення з питань національної безпеки або врегулювання кризових ситуацій, в безпосередній близькості до уряду, щоб включити кібербезпеку в число національних пріоритетів на найвищому рівні. Провідна структура також повинна взяти на себе відповідальність за розробку та оновлення національних стратегій і політик, а також нагляд за реалізацією пріоритетів національної політики. До складу національної структури управління кіберпростором повинні входити не лише вищі державні службовці, які відповідають за реагування на кіберінциденти, захист критичної інформаційної інфраструктури та боротьбу з кіберзлочинністю, а й більш широке коло вищих державних службовців [347,

с.14]. Окрім правоохоронних органів, до неї, безумовно, мають бути залучені дипломати, представники оборонного відомства, політики у сфері науки та освіти, представники торговельної та промислової політики, а також, якщо це можливо, консультації з асоціаціями приватного сектору. Широке коло зацікавлених сторін сприятиме підвищенню обізнаності про різні елементи національної політики кібербезпеки і про їхнє значення для широкого спектру цифрових питань. Це також дозволить досягти консенсусу щодо низки пріоритетів національної кіберполітики [29, с. 80].

Реагування на кіберінциденти, боротьба з кіберзлочинністю та захист критичної інформаційної інфраструктури є ключовими компонентами національної кіберполітики. Як правило, на політичному рівні формується модель організації цих елементів у функціонуючу і добре скоординовану національну кіберсистему. Хоча всі згадані сфери політики однаково важливі для національної кіберстійкості, не завжди очевидно, де в різних країнах інституційно знаходиться центр реагування на кіберінциденти та ЗКІІ [29, с. 80].

Боротьба з кіберзлочинністю зазвичай належить до компетенції Міністерства внутрішніх справ, яке разом з іншими органами правопорядку очолюють цю сферу політики. Через наскрізний характер реагування на кіберінциденти та ЗКІІ, країни знайшли дуже різні рішення щодо того, де розмістити ці можливості в своєму інституційному ландшафті. В європейських країнах національна група реагування на кіберінциденти (далі – CERT) може належати різним установам, таким як регулятор телекомунікаційного сектору, ІТ-агентство, розвідувальна організація, міністерство внутрішніх справ, оборонна структура або офіс кабінету міністрів. Деякі країни створили спеціальне національне кібер-агентство, яке діє як координаційний центр для реагування на інциденти та ЗКІІ, а деякі країни мають таку можливість як частину свого апарату внутрішньої безпеки [29, с. 80-81].

Зокрема, в Україні CERT-UA є спеціалізованим структурним підрозділом Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України [128] та його діяльність врегульована законами України «Про Державну службу спеціального зв'язку та захисту інформації» [98] та «Про основні засади забезпечення кібербезпеки України» [106].

Насправді не так важливо, де саме знаходяться ці можливості, як те, що вони належать авторитетному органу, який здатен координувати національну кібердіяльність і може взяти на себе горизонтальну роль у скликанні всіх необхідних зацікавлених сторін, включно з приватним сектором. Сили реагування на інциденти та органи ЗКІІ також можуть бути розташовані в різних адміністративних одиницях, але через їхні специфічні оперативні функції та політичну компетенцію вони повинні працювати в тісній координації [29, с. 81].

Здатність боротися з кіберзлочинністю є іншим не менш важливим компонентом національної кіберполітики. Вона передбачає наявність певного рівня законодавства для криміналізації кіберзлочинців, а також спроможність збирати електронні докази і розслідувати злочини у сфері високих технологій. Основні виклики включають підготовку поліцейських, які першими реагують на кіберзлочини, зважаючи на те, що традиційні злочини все частіше пов'язані з електронними доказами. Країни також повинні навчати суддів, прокурорів, слідчих та інших працівників судової системи щодо інструментів кіберзлочинності, які швидко розвиваються. Крім того, судові органи або поліцейські організації повинні створити підрозділи кібер-криміналістики для розслідування кібер-злочинів, що іноді є дорогим задоволенням для менш розвинених країн. ЄС запустив мережу лабораторій кібер-криміналістики в своїх країнах-членах, що є гарним прикладом, який можна було б наслідувати в інших регіонах [29, с. 81].

Важливе коло питань пов'язане з економічними аспектами кібербезпеки і охоплює промислову та торговельну політику. Недобросовісна торговельна

практика та економічні збитки, спричинені від кіберкрадіжки інтелектуальної власності – це виклик, з яким дедалі частіше стикаються дедалі частіше стикаються державні політики. Знову ж таки, отримання загального уявлення про масштаби втрат інтелектуальної власності є делікатним балансуєчим актом. Для оцінки наслідків кіберкрадіжки необхідна тісна співпраця з великими промисловими гравцями. Крім того, інструментарій політичного реагування для протидії крадіжкам інтелектуальної власності все ще розвивається і потребує як національних, так і міжнародних елементів підтримки. Наприклад, покарання за кібер-крадіжку через відповідні механізми міжнародної торгівлі може бути одним із способів реагування на таку недобросовісну торговельну практику [29, с. 81; 194].

Очевидною політичною метою має бути підтримка промислової політики, яка вимагає вищого рівня стандартів безпеки в галузі ІКТ та інновацій з використанням ІКТ в інших галузях, оскільки цей сектор відіграватиме значну роль у підтримці майбутнього економічного зростання саме в країнах з розвинутою економікою. Досягненню більшої довіри та безпеки до продуктів ІКТ може сприяти цільове фінансування досліджень і розробок у сфері кібербезпеки, заохочення інновацій у сфері безпеки та створення кластерів стартапів. Це особливо актуально в епоху інтернету речей, коли автомобілі, побутова техніка та інше обладнання будуть підключені до інтернету [29, с. 82].

Для великих компаній все частіше постає питання про те, скільки їм потрібно інвестувати в кіберстійкість, щоб стати кіберзахищеними. Існує певний поріг інвестицій, який керівництво компанії вважає пропорційним сприйнятому рівню ризику. І, безумовно, є рівень вище цього порогу, який не може бути досягнутий без надмірних інвестицій, які можуть бути економічно не виправданими. Як логічний наслідок, страхова галузь долучилася до кібердебатів, додавши важливий елемент обґрунтованої оцінки ризиків для приватних підприємств. Страхові компанії можуть забезпечити вимірний вплив на зниження ризиків через механізм застосування фінансових наслідків

за вжиття заходів безпеки промисловими організаціями. У США розпочалися ініціативи з визначення відповідних метрик кіберризиків та збитків за участю представників страхових компаній та керівництва галузі. Уряди повинні заохочувати зусилля щодо аналізу потенційного позитивного впливу страхових практик на плани ЗКП [29, с. 82].

Дуже важливим елементом буде відпрацювання способів реагування на великі кібератаки, а також включення кібер-аспектів у національні навчання з врегулювання кризових ситуацій. Ідеальний сценарій кібернавчань охоплюватиме як технічні, так і стратегічні аспекти прийняття рішень, на додаток до кібернавчань, які проводяться в лабораторіях лише серед технічного персоналу. Хоча технічні навчання є цінними з оперативної точки зору, національні командно-штабні навчання повинні включати різні відомства, відповідальні за надання критично важливих послуг, керівників приватного сектору і ключовий персонал органів державного управління. Уряди також повинні мати можливість відпрацювати національну кризу з кількома елементами, одним з яких може бути кібер порушення життєво важливих мереж або послуг. Добре проведені навчання дозволять підготувати плани на випадок надзвичайних ситуацій і оцінити готовність національних кіберструктур. Навчання також нададуть інформацію політикам, куди слід спрямувати додаткові інвестиції, наприклад, на придбання альтернативних засобів зв'язку, посилення мережевого захисту у життєво важливих сферах тощо [29, с. 82].

Важливим, у контексті широкомасштабного вторгнення РФ на територію України, використання агресором усього спектру гібридних загроз, зокрема кібератак, також є врахування кібер-аспектів при плануванні політики оборони і безпеки. Сили оборони повинні бути здатні захистити себе і діяти в умовах кібератаки; вони повинні мати спеціалізовані структури реагування на інциденти для пом'якшення наслідків кібервторгнень, і вони повинні бути включені в національне планування дій на випадок надзвичайних ситуацій і визначення їх місця та ролі. Посилення кібербезпеки в системі національної

безпеки, оборони, врегулювання кризових ситуацій та захист критичної інфраструктури вимагатиме вдосконалених спроможностей з виявлення та аналізу кіберзагроз на національному рівні [29, с. 82-83].

Наразі, слід не забувати, що навчання та освіта в галузі кібербезпеки – це широка сфера, яка включає в себе підготовку персоналу з ІТ-безпеки та інших спеціалістів, а також інформування обізнаності широкої громадськості та керівників щодо кіберзагроз. Нестача експертів з ІТ-безпеки вже є критичною, і багато урядів розробляють складні механізми, щоб утримати найталановитіших кіберфахівців у себе вдома. Включення елементів комп'ютерної та інформаційної безпеки в усі навчальні програми з інформаційних технологій є вимогою часу, паралельно зі збільшенням інвестицій у спеціалізовану підготовку з ІТ-безпеки та мережевого захисту. Пріоритетом має стати фінансування прикладних і теоретичних досліджень в галузі інформатики, а також заохочення міждисциплінарних кібердосліджень для підготовки наступного покоління осіб, які приймають рішення, і аналітиків [29, с. 83].

Нарешті, центральна група проблемних питань пов'язана із занепокоєнням щодо глобальної кіберстабільності та необхідністю введення поняття відповідальності держави в кіберпросторі. У сфері міжнародної безпеки, пов'язаної з кіберпростором, існує кілька ініціатив, які сприяють покращенню глобальної кібербезпеки, зобов'язуючи провідні уряди дотримуватися правил і норм. ООН, ОБСЄ та інші міжнародні організації зробили кілька кроків для розробки кібернорм і заходів зі зміцнення довіри, спрямованих на запобігання кіберконфліктам і зниження напруженості між державними суб'єктами [193, с. 6]. Дипломатичне співтовариство разом з агентствами розвитку також допомагає країнам, що розвиваються, боротися з кіберзлочинністю та створювати мінімальні можливості реагування на кіберінциденти [29, с. 83].

2.2. Суб'єктний склад та міжнародний контекст формування системи кіберстійкості

Еволюція поглядів на забезпечення безпеки в інформаційному та кіберпросторах України пройшла шлях від вузькотехнічного «захисту інформації» до комплексної, багаторівневої «кіберстійкості». На початкових етапах становлення незалежності державна політика фокусувалася переважно на технічному захисті інформації з обмеженим доступом, що було відображено в Законі України «Про захист інформації в інформаційно-комунікаційних системах» [101]. Проте стрімка цифровізація державного управління та економіки, а особливо початок гібридної агресії у 2014 році, виявили обмеженість статичних методів захисту.

Прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [107] у 2017 році стало відправною точкою для переходу до термінології «кібербезпеки» як стану захищеності життєво важливих інтересів людини, суспільства та держави. Проте справжня актуалізація саме кіберстійкості відбулася з прийняттям оновленої Стратегії кібербезпеки України (2021) [110]. У цьому документі кіберстійкість уперше була виокремлена не просто як технічна характеристика, а як стратегічна здатність національної інфраструктури зберігати працездатність та швидко відновлюватися після масштабних кібератак.

Наукове пізнання кіберстійкості в Україні сьогодні базується на розумінні того, що це інтегральна динамічна категорія. На відміну від «кіберзахисту», який спрямований на створення бар'єрів для запобігання проникненню, «кіберстійкість» аксіоматично визнає можливість успішного подолання цих бар'єрів противником. Таким чином, у вітчизняному науковому дискурсі відбувається зміна парадигми: від ілюзорної спроби забезпечити «непроникність» систем до практичного завдання забезпечення їх «життєздатності».

Перш за все, важливо акцентувати увагу на кіберстійкості як складовій національної безпеки в умовах воєнного стану. Для України, яка перебуває в стані повномасштабної кібервійни, стійкість цифрових систем є критичним фактором виживання держави. В умовах, коли кібератаки використовуються як інструмент стратегічного впливу для руйнування критичної інфраструктури, дезорганізації державного управління та деморалізації населення, національна кіберстійкість набуває ознак цифрового суверенітету.

Такий зв'язок між стійкістю та національною безпекою проявляється в кількох аспектах:

стійкість державного управління – здатність реєстрів, систем документообігу та комунікаційних каналів уряду функціонувати в умовах постійного деструктивного впливу;

економічна стійкість – забезпечення стабільності економічних процесів, зокрема, банківського сектору та енергомереж, де цифрова складова є критичною для запобігання системному колапсу;

соціальна стабільність – безперервність надання електронних послуг громадянам, що підтримує довіру до державних інституцій навіть у кризові періоди.

Враховуючи зазначені зв'язки нацбезпеки і кіберстійкості, теоретична побудова архітектури кіберстійкості в Україні має базуватися на низці фундаментальних аксіом, які визначають логіку всіх наступних організаційних та технічних рішень:

Наріжним каменем філософії стійкості є аксіома неминучості компрометації. Ми виходимо з того, що будь-який периметр може бути подоланий, будь-який інструмент захисту може бути обійдений, а всередині системи вже може перебувати зловмисник. Це змушує зміщувати ресурси з «воротарських» методів на методи внутрішнього моніторингу та ізоляції.

Водночас, аксіома пріоритетності відновлення передбачає, що у ситуації критичного інциденту головною метою є не збереження недоторканності даних (якщо вони вже скомпрометовані), а мінімізація часу простою. Стійкість

вимірюється швидкістю повернення до штатного або мінімально допустимого режиму функціонування.

І на завершення, аксіома безперервності управління. Система повинна мати вбудовані альтернативні механізми управління, які залишаються доступними навіть при повному ураженні основної інфраструктури.

Таким чином, філософський зміст національної кіберстійкості полягає у переході від культури «виправлення помилок» до культури «функціонування в умовах помилок». Це вимагає від суб'єктів кібербезпеки не лише технічної грамотності, а й стратегічного мислення, орієнтованого на довгострокове виживання системи в агресивному середовищі. Водночас, важливим є процес трансформації зазначених філософських засад у конкретну архітектуру та процеси управління національною безпекою.

Сучасний стан розбудови національної системи кіберстійкості в Україні визначається логікою Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», затвердженої Указом Президента України № 447/2021. Цей документ фактично заклав фундамент для переходу від реактивного кіберзахисту до проактивної стійкості. Науковий аналіз Стратегії дозволяє констатувати, що кіберстійкість у ній розглядається як багатофакторна спроможність, що включає не лише технічну готовність, а й політичну волю, правову визначеність та суспільну довіру [110].

Ключовим нововведенням вітчизняного законодавства є детермінація кіберстійкості як «здатності системи до самовідновлення». Згідно з положеннями Закону України «Про основні засади забезпечення кібербезпеки України», система національної кібербезпеки має забезпечувати мінімізацію наслідків кіберінцидентів для об'єктів критичної інфраструктури [107]. Проте наукова думка вказує на те, що законодавча дефініція потребує розширення: стійкість – це не лише відновлення після удару, а й здатність системи до трансформації в самому процесі відсічі агресії. Це корелюється з європейськими підходами, закладеними в Директиві NIS2, де акцент

зміщується на «ланцюги постачання» та «управління ризиками на рівні вищого керівництва» [9; 223].

Із врахуванням критичного аналізу правового регулювання стійкості критичної інформаційної інфраструктури (КІІ), специфіка України полягає в тому, що нормативне регулювання кіберстійкості здійснюється в умовах правового режиму воєнного стану. Це накладає додаткові вимоги до архітектури системи. Зокрема, Постанова Кабінету Міністрів України № 1106 «Про затвердження Порядку формування переліку об'єктів критичної інфраструктури» визначає критерії категорювання об'єктів, де кіберстійкість виступає як один із показників життєздатності системи в умовах надзвичайної ситуації [41].

Наукове обґрунтування концептуальної моделі кіберстійкості вимагає розв'язання суперечності між «закріпленістю» нормативних норм та «плинністю» кіберзагроз. Водночас, стійкість архітектури національної системи має базуватися на принципі інституційної пам'яті – здатності суб'єктів кібербезпеки не лише ліквідовувати наслідки, а й інтегрувати отриманий досвід у майбутні оборонні стратегії [29; 258; 294].

Із врахуванням зазначеного, та з досвіду відсічі повномасштабної кіберагресії з боку РФ, пропонується авторське бачення архітектурного змісту національної стійкості, що базується на трьох фундаментальних площинах:

Правова стійкість – створення законодавчого поля, яке дозволяє миттєво адаптувати повноваження суб'єктів кібербезпеки до нових типів атак без бюрократичних затримок;

технологічна гнучкість – перехід до хмарних та розподілених інфраструктур, що забезпечують географічну віддаленість даних та сервісів від фізичних зон ураження;

когнітивна витривалість – здатність персоналу та суспільства зберігати критичне мислення та дотримуватися протоколів безпеки в умовах потужного дезінформаційного впливу, що супроводжує кібератаки.

Таким чином, філософська база національної кіберстійкості в Україні еволюціонувала від «захисту інформації» до «забезпечення безперервності держави». Це вимагає від архітекторів системи не лише інженерних розрахунків, а й розуміння соціально-політичних наслідків кожного технічного рішення.

Наукове проектування національної системи кіберстійкості вимагає відмови від монолітних структур на користь багаторівневої, децентралізованої архітектури. В умовах сучасної кібервійни, де цілями атакуючої сторони є одночасно і державні реєстри, і приватні постачальники послуг, і критичні об'єкти енергопостачання, архітектура має базуватися на принципах модульності та ізоляції відмов. Запропонована модель національної кіберстійкості України структурується за трьома ієрархічними рівнями: об'єктовим (мікро-рівень), галузевим (мезо-рівень) та національним (макро-рівень) [27; 118].

На рівні окремого суб'єкта – будь-то орган державної влади чи приватне підприємство – кіберстійкість пізнається через здатність його локальної ІТ-інфраструктури витримувати ураження окремих вузлів. Науково-технічною основою цього рівня є імплементація архітектури «нульової довіри». На відміну від класичних моделей «захищеного периметра», «нульова довіра» базується на аксіомі, що мережа вже скомпрометована. Це вимагає постійної верифікації кожного запиту, мікросегментації мережі для запобігання горизонтальному переміщенню зловмисника та суворого дотримання принципу найменших привілеїв [421].

Для українських об'єктів критичної інфраструктури (ОКІ) архітектурна стійкість на мікро-рівні також передбачає впровадження механізмів «незмінних бекапів» та ізольованих середовищ відновлення. Це дозволяє гарантувати, що навіть у разі успішної атаки шифрувальників або «вайперів», система має змогу миттєво відновити дані з джерела, яке було фізично або логічно недоступне для зловмисника під час атаки [20; 138].

Галузевий рівень архітектури забезпечує координацію між однорідними за своєю функцією суб'єктами. Науковий зміст цього рівня полягає у формуванні галузевих екосистем стійкості, де вихід з ладу одного об'єкта не призводить до каскадного колапсу всього сектора. Особливого значення це набуває в енергетиці та фінансах. Наприклад, енергетична кіберстійкість України під час війни продемонструвала необхідність створення галузевих центрів операційної безпеки (SOC), які здатні в режимі реального часу обмінюватися даними про аномалії між різними обленерго та генеруючими компаніями [127; 220; 230; 294].

На галузевому рівні стійкість пізнається через стандартизацію протоколів взаємодії. Це включає розробку галузевих профілів захисту та проведення регулярних стрес-тестів, що імітують відключення критичних вузлів. Архітектурне рішення тут зміщується у бік створення «галузевих кіберхмар», що дозволяють балансувати навантаження та перерозподіляти ресурси у разі ураження локальних центрів обробки даних окремих компаній [79; 102; 125; 405].

Національний рівень є вищою ланкою архітектури, яка забезпечує стратегічне управління та координацію зусиль усіх суб'єктів. Центром цієї архітектури в Україні є Національний координаційний центр кібербезпеки (НКЦК) [103] при РНБО України та Державна служба спеціального зв'язку та захисту інформації (ДССЗІ). Наукове пізнання макро-рівня стійкості зосереджене на створенні єдиного контуру ситуаційної обізнаності.

Архітектурна модель національного рівня базується на концепції «мережі мереж». Це означає, що державна система не намагається контролювати кожен комп'ютер, а створює стандарти та платформи для обміну даними про загрози між CERT-UA, військовими підрозділами кібероборони та приватними SOC. Такий підхід забезпечує колективний імунітет: інформація про атаку на один об'єкт протягом лічених хвилин стає основою для оновлення правил захисту на національному рівні, роблячи аналогічну атаку неможливою для інших суб'єктів [28; 29; 63; 18].

Таким чином, багаторівнева архітектура національної системи кіберстійкості України – це динамічна конструкція, яка дозволяє державі бути гнучкою. Вона поєднує жорстку інженерну стійкість на місцях із гнучкою координацією на рівні секторів та стратегічним форсайтом на рівні держави. Це робить систему не просто «міцною», а «антикрихкою» — такою, що вдосконалюється в процесі протидії ворожим впливам.

Функціональний зміст архітектури національної кіберстійкості визначається її спроможністю виконувати критичні завдання на кожному етапі життєвого циклу кіберзагрози. На відміну від традиційного кіберзахисту, де функції обмежені ідентифікацією та захистом, архітектура стійкості інтегрує предиктивну аналітику, механізми адаптивного опору та стратегії еволюційного навчання. Це дозволяє системі не просто реагувати на інциденти, а випереджати їх, трансформуючи кожен виклик у нову форму системної міцності [27; 29; 134; 215; 294].

Важливим архітектурним компонентом є предиктивний аналіз – інтелектуальний форсайт загрози. Функція передбачення в сучасній архітектурі стійкості базується на глибокій інтеграції інструментарію аналітичної розвідки, зокрема, із використанням ресурсу на базі штучного інтелекту. Науковий зміст цього компонента полягає у переході від аналізу сигнатур (минулого) до аналізу патернів та намірів (майбутнього). Предиктивна архітектура передбачає створення національної платформи обміну даними про загрози, яка акумулює індикатори компрометації та тактики, техніки і процедури зловмисників [137, с. 240; 265; 266].

Водночас, використання алгоритмів машинного навчання дозволяє виявляти аномалії на рівні національних магістральних каналів зв'язку ще до того, як атака набуде масштабного характеру. Функція передбачення також включає «полювання на загрози» всередині мереж критичної інфраструктури, що дозволяє виявляти латентні фази перебування ворога в системі, забезпечуючи архітектурну перевагу захисника за рахунок скорочення часу знаходження зловмисника в інфраструктурі [167; 380].

Ядром архітектури стійкості є спроможність системи функціонувати в «деградованому» стані. Характеризуючи дослідженість проблематики та теоретичні засади, ми вже згадували про механізм «граціозної деградації», що передбачає у ситуації масованої атаки автоматичну активацію протоколів ізоляції критичних сервісів. Наприклад, для державних реєстрів це означає перехід у режим «тільки читання» або відключення другорядних інтеграцій для збереження цілісності бази даних [153; 210].

Функціонально це реалізується через динамічну переконфігурацію мережі, де потік даних автоматично перенаправляється через резервні вузли або хмарні середовища. Архітектура витривалості також включає механізми «автономного функціонування вузлів», коли локальна система (наприклад, управління ТЕЦ або банківським відділенням) здатна виконувати базову місію навіть за умови повної втрати зв'язку з центральним ситуаційним центром [54; 109; 294].

Важливо процес відновлення в архітектурі кіберстійкості розглядати також через рекуперативний компонент та еволюційну адаптацію, що інтерпретується як «відновлення краще, ніж було» (Build Back Better). Функціональний зміст цього етапу полягає у автоматизованому розгортанні інфраструктури з перевірених кодів, тобто «інфраструктура як код» (Infrastructure as Code – IaC), на чистих потужностях, що виключає повторне зараження [52; 84; 279; 121]. Архітектура рекуперації базується на принципах «незмінності» інфраструктури, де пошкоджені вузли не відновлюються, а знищуються і миттєво замінюються новими, чистими копіями [126; 155].

Нарешті найвищою функцією архітектури є адаптивне самонавчання. Кожен інцидент в Україні сьогодні автоматично перетворюється на «код безпеки». Результати аналізу атаки інтегруються в оновлені алгоритми моніторингу та конфігурації фаєрволів по всій країні. Це створює ефект еволюційного імунітету: система, що пережила атаку, стає не просто відновленою, а якісно новою, з вищою межею витривалості до аналогічних впливів у майбутньому [60; 167; 411].

Розглядаючи національну архітектуру кіберстійкості України важливо вказати на нормативно-методологічне її забезпечення, що в сучасних умовах є не лише сукупністю регламентів, а фундаментальним регуляторним каркасом, що визначає життєздатність держави в цифровому вимірі. Актуальність цього блоку зумовлена необхідністю подолання правової та методологічної асиметрії між динамічною природою кіберзагроз та статичним характером класичного законодавства. Водночас, формування цього блоку в Україні має базуватися на гармонізації міжнародних стандартів із унікальним вітчизняним досвідом функціонування в умовах постійного кіберпротистояння. Без чіткої методологічної бази архітектура залишається сукупністю технічних рішень, позбавлених системної стійкості на рівні держави [39; 71; 93; 131; 133]. В умовах повномасштабної агресії методологія стійкості має трансформуватися у гнучку систему стандартів, що здатна до самоадаптації в режимі реального часу [6; 107; 122].

Архітектура, яку неможливо виміряти, не може бути ефективно керованою. Тому важливо використовувати відповідну систему метрик, що дозволяють оцінювати стан кіберстійкості держави. Пропонується впровадження інтегрального Національного індексу кіберстійкості, який базується на таких показниках:

коефіцієнт функціональної деградації – математичне відношення обсягу послуг, що надаються під час атаки, до штатного режиму функціонування;

час повернення до стану довіри – інтегральний показник швидкості повної рекуперації системи після ураження;

рівень адаптивної спроможності – показник, що відображає частку автоматизованих рішень у процесі відсічі атаки та швидкість оновлення політик безпеки на основі досвіду інциденту [52; 77; 327].

Ці метрики мають стати основою для нормативно закріпленої звітності ОКІ перед НКЦК при РНБО та Держспецзв'язку, що дозволить формувати динамічну мапу стійкості країни.

Для українських реалій методологічне забезпечення має включати розробку національних «профілів стійкості» для різних секторів критичної інфраструктури. Це дозволяє, зокрема, врахувати специфіку енергетики, де пріоритетом є доступність систем реального часу (SCADA/ICS), на відміну від фінансового сектору, де ключовою є цілісність транзакцій. Нормативне закріплення цих профілів створює умови для прогнозованої поведінки системи в цілому, незалежно від форми власності конкретного об'єкта [18; 102; 107; 164; 227].

Методологічне забезпечення архітектури на галузевому рівні передбачає:

визначення критичних функцій місії – ідентифікація процесів, зупинка яких призведе до системного колапсу галузі;

сценарне моделювання – методика проведення стрес-тестів на основі моделювання атак «найгіршого сценарію», що дозволяє верифікувати архітектурні рішення до моменту виникнення реальної кризи;

стандартизація інтерфейсів взаємодії – нормативне регулювання безпеки міжсистемних зв'язків, що забезпечує стійкість ланцюгів постачання цифрових послуг [20; 135].

Важливим елементом методологічного забезпечення є визнання людини як активного елемента архітектури. Наукове пізнання соціотехнічних систем вказує на те, що навіть найдосконаліша технічна архітектура може бути нівельована людською помилкою або когнітивним упередженням під час кризи. Тому нормативне забезпечення має включати стандарти «цифрової мобілізації» та кібергігієни для персоналу ОКІ [8; 43].

Культура стійкості пізнається як здатність фахівців діяти згідно з протоколами в умовах повної невизначеності та стресу. Це вимагає впровадження в архітектуру системи методів «психологічної стійкості» команд реагування та регулярного проведення кібернавчань, які є не просто тренуванням, а методом верифікації дієздатності всієї національної архітектури [327, с. 4545].

Наукові дослідження доводять, що людина є найбільш волатильним елементом архітектури кіберстійкості і передбачають наявність відповідної методології розбудови «культури стійкості» через:

стандарти когнітивної безпеки – методи протидії соціальній інженерії та психологічним операціям, що супроводжують кібератаки;

нормативне закріплення обов'язкових кібернавчань – перехід від формального інструктажу до регулярного практичного відпрацювання навичок виживання в умовах «туману кібервійни»;

систему стимулювання та відповідальності – імплементація логіки Директиви NIS2 щодо персональної відповідальності керівництва (C-level) за невідповідність об'єкта стандартам стійкості [9; 223].

Процес розбудови кіберстійкості в Україні вимагає імплементації кращих світових практик у національне законодавство. Ключовим вектором тут є адаптація стандартів серії ISO/IEC 27031 (Забезпечення готовності інформаційно-комунікаційних технологій до безперервності бізнесу) та спеціальних публікацій NIST SP 800-160 Vol. 2., що пропонують науковий підхід до проектування систем, що здатні передбачати, протистояти, відновлюватися та адаптуватися до деструктивних впливів. Зміст такої гармонізації полягає у переході від пасивного контролю за відповідністю (compliance) до активного управління спроможністю виживати [219; 290].

Загалом, розбудова певної моделі кіберстійкості, передбачає і відповідні регуляторні ініціативи, що сприяють підвищенню кібербезпеки критично важливих послуг. З цього приводу, тривалий час в розвинених країнах серед суб'єктів кібербезпеки відбувалася дискусія щодо того чи варто здійснювати регуляторні функції у сфері кібербезпеки. Представники національної безпеки та правоохоронних органів виступали за регулювання, тоді як ІТ-розробники та приватний сектор іноді запекло протистояли цьому. Оскільки більшість індустріальних країн зробили вибір на користь кіберрегулювання, спільною позицією стало посилення управління ризиками ІТ-безпеки в компаніях та організаціях державного сектору, які забезпечують критично важливу

інфраструктуру та послуги. Стало очевидним, що для боротьби зі стрімким зростанням кіберзагроз необхідне втручання держави.

Після кібератаки на Естонію в 2007 році багато технологічно розвинених урядів почали зміцнювати свою національну кіберстійкість, а рівень обізнаності в державній політиці стрімко зростав. Після атак Stuxnet і Saudi Aramco, а також зростаючої тенденції використання програм-вимагачів проти комунальних підприємств, на національному рівні з'явився новий чіткий політичний напрямок захисту критично важливих послуг. [59; 377; 391] Однак в деяких країнах законопроектні ініціативи щодо підвищення кіберстійкості зазнали серйозних невдач, зокрема у 2012 році Сенатом США був відхилений Закон Лібермана про кібербезпеку. Але у 2013 році Указом Президента США було визначено новий курс для галузевої практики управління кіберризиками. [239; 375]

Згодом Національний інститут стандартів і технологій (*National Institute of Standards and Technology – NIST*) підготував збірник найкращих галузевих практик під назвою «Концепція кібербезпеки» [342]. Концепція NIST сприяла збору цінних передових практик у сфері кібербезпеки, оскільки вона була розроблена із залученням найкращих галузевих експертів. Однак, оскільки вона залишається «добровільною», важко виміряти її ефективність. Наприкінці 2015 року США прийняли Закон про обмін інформацією з питань кібербезпеки як частину більш широкого законопроекту. Закон не лише сприяв обміну інформацією між приватним сектором та урядом, але й зосереджував увагу на превентивних та оборонних заходах для захисту критично важливої інфраструктури, федерального уряду та уряду штатів, а також установ охорони здоров'я [50; 267]. Закон також включає інші важливі елементи національної кібербезпеки і зобов'язує Міністерство внутрішньої безпеки (*Department of Homeland Security*) та інші урядові установи США вжити необхідних заходів для запобігання та реагування на кіберзагрози.

Водночас, Європейський Союз наприкінці 2015 року погодив Директиву про мережеву та інформаційну безпеку (*Directive on Network and Information*

Security – NIS) [224]. Втім, окремі європейські країни вже мали відповідне національне законодавство що врегульовувало питання кібербезпеки. Наприклад, у 2009 році Естонія ухвалила закон, який містив детальний перелік критично важливих послуг, з обов'язковим управлінням кіберризиками та звітуванням про інциденти операторами критично важливих послуг. [213] На той час Естонія була першою європейською країною, яка включила в закон перелік детальних критично важливих послуг у різних секторах, що викликало багато запитань у більш ліберальних кібер-колах. До 2015 року інші європейські країни підготували подібні закони, хоча і з різним рівнем деталізації. Франція визначила кібербезпеку своїм головним пріоритетом у кількох Білих книгах, починаючи з 2009 року; Німеччина ухвалила закон про ІТ-безпеку у 2015 році. Багато інших європейських країн прийняли комплексні національні стратегії кібербезпеки.

Директива ЄС про мережеву та інформаційну безпеку (NIS) базувалася на комплексному регулюванні кібербезпеки з багатьма елементами. Вона спрямована на створення рівних умов для країн-членів ЄС, встановлюючи вимогу щодо наявності компетентного кібероргану, а також технічної спроможності реагування на інциденти на національному рівні. Вона також заохочує до співпраці між державами-членами для полегшення обміну інформацією та оперативного співробітництва щодо інцидентів. Крім того, вона забезпечує впровадження заходів безпеки в ключових секторах у всіх країнах-членах ЄС, включаючи енергетику, транспорт, водопостачання, банківські, медичні та фінансові послуги. Директива також поширює заходи ІТ-безпеки на постачальників цифрових послуг, таких як онлайн-маркети.

Водночас, важливим питанням залишалося те, як ці регуляторні кроки насправді вплинуть на стан кіберстійкості критично важливих об'єктів інфраструктури та послуг. Багато експертів приватного сектору попереджали уряди, що надмірно суворе регулювання може призвести до неналежних зусиль з дотримання вимог, які можуть бути малоефективними щодо посилення реальної кібербезпеки. На початковому етапі державного

регулювання кіберпростору в цих країнах, навіть з розвиненою індустріальною економікою, ще було занадто рано оцінювати ефективність такого регулювання. Однак досвід європейських країн, які вже запровадили відповідне регулювання, вказував на досить позитивні результати. Наприклад, уряд Естонії розгорнув допомогу для багатьох компаній щодо поглиблення уваги управлінню кіберризиками, проведенню навчань та підвищення обізнаності про кіберризики. Ці кроки супроводжувалися «м'яким» регулюванням, а також було створено державне агентство з мандатом нагляду за реалізацією національних пріоритетів у сфері ЗКІІ. У Німеччині прийняття закону про ІТ-безпеку сприяло розвитку державно-приватного партнерства у сфері кібербезпеки.

Резюмуючи щодо Директиви NIS, варто зазначити, що вона зосереджується переважно на організаційних аспектах національних кіберзаходів, закликаючи країни-члени ЄС розробити національне бачення та розбудовувати кіберстійкість разом з приватним сектором. Вона не містить надто детальних технічних вимог, а зосереджується на створенні організаційних рамок для національної кібербезпеки в ключових секторах і що важливо, вона розвивається як сама система кіберстійкості, тому що сьогодні набрала чинності вже наступна Директива – NIS2.

Отже, архітектура національної системи кіберстійкості – це динамічна система, що пов'язує воєдино технічну досконалість, управлінську дисципліну та наукову об'єктивність вимірювання. Це інструмент, який дозволяє українській державі перетворювати досвід війни на непереборну правову та технологічну фортецю.

Функціонування національної системи кіберстійкості в Україні базується на чіткій ієрархічній вертикалі, де кожен державний орган виконує специфічну роль у загальному циклі забезпечення життєздатності держави. Наукове пізнання суб'єктного складу цієї вертикалі вимагає аналізу не лише їхніх формальних повноважень, а й реальної операційної спроможності в умовах гібридної агресії. Державна вертикаль в Україні побудована за

принципом розподіленої відповідальності при централізованій стратегічній координації, що є оптимальною моделлю для протидії масштабним кіберзагрозам [9; 29; 49; 71; 112].

Перш за все, виділимо Раду національної безпеки і оборони України (РНБО) та НКЦК як стратегічний центр, що перебувають на вершині ієрархії в Україні, і здійснюють загальне керівництво та координацію діяльності органів виконавчої влади у сфері кібербезпеки. Національний координаційний центр кібербезпеки (НКЦК) [103] є робочим органом РНБО. Центр має забезпечити координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки. Тобто виконує певні функції «стратегічного хабу» стійкості [103].

Серед основних завдань Центру [103]: аналіз стану кібербезпеки; кіберзахисту критично важливих об'єктів інфраструктури результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Центр прогнозує та виявляє потенційні та реальні загрози у сфері кібербезпеки України, узагальнює міжнародний досвід у сфері забезпечення кібербезпеки; оперативне, інформаційно-аналітичне забезпечення РНБО з питань кібербезпеки [103].

Центр бере участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів, розробляє відповідні методичні документи і рекомендації.

Згідно з Положенням, Центр має право запитувати та одержувати від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення питань, що належать до його компетенції; користуватися інформаційними базами даних державних органів, державними, в тому числі урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами тощо [103].

Рішення Центру є обов'язковими для розгляду органами державної влади, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, підприємствами, установами та організаціями [103].

В умовах воєнного стану НКЦК трансформувався у майданчик для миттєвого прийняття рішень, де представники силових структур та цивільних відомств спільно виробляють протоколи протидії новим типам атак.

Державним регулятором щодо кіберстійкості в Україні є Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку) [98; 102; 107]. Держспецзв'язку є головним органом у системі центральних органів виконавчої влади, який відповідає за формування та реалізацію державної політики у цій сфері. Це центральний орган виконавчої влади, підпорядкований Президентові, що забезпечує функціонування державної системи зв'язку, захист державних інформаційних ресурсів, криптографічний захист інформації та кіберзахист критичної інфраструктури. У структурі Держспецзв'язку ключовим суб'єктом є Державний центр кіберзахисту (ДЦКЗ) [34] та підпорядкована йому команда CERT-UA [196].

Основними завданнями Державного центру кіберзахисту Держспецзв'язку є [36; 37; 83]:

впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки;

забезпечення створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет;

забезпечення створення та функціонування системи антивірусного захисту національних інформаційних ресурсів;

аудит інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури;

забезпечення створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту;

забезпечення створення та функціонування системи взаємодії команд реагування на комп'ютерні надзвичайні події;

у взаємодії з іншими суб'єктами забезпечення кібербезпеки, розробка сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, програм та методик проведення кібернавчань тощо.

Загалом, незважаючи на те, що прямого згадування про кіберстійкість у визначених завданнях ДЦКЗ немає, все ж зазначення про забезпечення створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, а також розробка сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, програм та методик проведення кібернавчань, вказує на конкретні елементи, властиві розбудові саме кіберстійкості.

В свою чергу завданнями CERT-UA передбачено [95; 128]:

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

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

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

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

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

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;

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 тощо.

І знову, важко зазначити про пряме посилення на формування кіберстійкості, водночас, необхідно враховувати, що CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України і в умовах кібервійни адекватність реагування на кібератаки є вже компонентом стійкості [128]. І CERT-UA це доводить ефективністю своєї діяльності.

Водночас, відповідно до Постанови Кабінету Міністрів України від 23.12.2020 № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» [40], CERT-UA входить до складу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, що також характеризує певні аспекти кіберстійкості.

Служба безпеки України (СБУ) відіграє критичну роль у забезпеченні превентивної стійкості держави. Її повноваження у сфері контррозвідувального забезпечення інформаційної та кібербезпеки визначені Законом України «Про Службу безпеки України» та Законом України «Про основні засади забезпечення кібербезпеки України», які закріплюють за СБУ функції протидії розвідувально-підривній діяльності в кіберпросторі та боротьби з кібертероризмом [107; 112].

Зокрема, СБУ відповідно до закону «Про основні засади забезпечення кібербезпеки України» [107] реалізує комплекс контррозвідальних та оперативно-розшукових заходів для виявлення та припинення злочинів проти національної безпеки, що вчиняються у цифровому просторі. Важливою складовою формування превентивної кіберстійкості є повноваження СБУ щодо негласної перевірки готовності об'єктів критичної інфраструктури до можливих атак, що дозволяє виявляти системні вразливості до моменту їх експлуатації ворогом. Координація зусиль у цьому напрямі забезпечується через функціонування Ситуаційного центру забезпечення кібербезпеки СБУ та мережі регіональних центрів, які формують єдиний контур оперативного виявлення кіберзагроз у сфері державної безпеки. Держспецзв'язку та СБУ з метою вжиття заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози в межах своїх повноважень можуть надавати обов'язкові до виконання вимоги про реагування власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури, операторам критичної інфраструктури.

Окремим інструментом динамічної стійкості держави є спільний механізм СБУ та Держспецзв'язку щодо надання обов'язкових до виконання вимог про реагування на кіберінциденти. Такі вимоги мають статус актів організаційно-розпорядчого характеру і спрямовані на негайну мінімізацію негативних наслідків атак на системи, де обробляються державні інформаційні ресурси або таємна інформація. Цей механізм не є формою державного контролю, а виступає засобом кризового управління, що зобов'язує операторів критичної інфраструктури вживати визначених заходів та звітувати про результати у встановлені строки. Завдяки такій юридичній конструкції досягається висока швидкість адаптації всієї державної системи до нових векторів загроз, що є фундаментальною ознакою національної кіберстійкості.

Таким чином, залучення СБУ до архітектури кіберзахисту забезпечує глибинну атрибуцію загроз та захист від складних цільових атак (АРТ-груп). Поєднання контррозвідальних можливостей СБУ з регуляторними функціями Держспецзв'язку дозволяє створити стійке середовище, де технологічний захист підкріплюється правовим примусом до швидкого реагування, гарантуючи безперервність функціонування життєво важливих інтересів держави у кіберпросторі.

Діяльність СБУ зосереджена на контррозвідальному забезпеченні кіберпростору, що реалізується, зокрема, через профільні підрозділи, зокрема Департамент контррозвідального захисту інтересів держави у сфері інформаційної безпеки (ДКІБ) СБУ [107; 112], що протидіє кіберзагрозам, кібертероризму та розвідувальним операціям іноземних спецслужб у кіберпросторі. Він захищає критичну інфраструктуру, державні ресурси та протидіє дезінформації і фокусується на:

атрибуції атак – виявлення конкретних хакерських угруповань, підконтрольних спецслужбам РФ, та документування їхньої діяльності;

запобіганні диверсіям – виявлення агентів впливу та агентурних мереж, спроб створення «сплячих» вразливостей у мережах ОКІІ;

кіберрозвідці – отримання випереджальної інформації про плани противника щодо проведення масованих атак на українську інфраструктуру.

Специфічним суб'єктом є підрозділи кібероборони Збройних Сил України (ЗСУ), які забезпечують стійкість військової інфраструктури та систем управління військами. Їхня роль є вирішальною у забезпеченні «військової стійкості», що включає захист засобів зв'язку та радіоелектронної боротьби (РЕБ), зв'язку та автоматизованих систем управління боєм. Особливістю української моделі є високий рівень координації між ЗСУ та цивільними суб'єктами (CERT-UA), що дозволяє спільно протидіяти атакам на подвійну інфраструктуру (наприклад, супутниковий зв'язок) [105; 107; 110].

У законотворчому процесі надзвичайно важливим у час війни є законопроект про кіберсили ЗСУ. Аналіз проєкту Закону про Кіберсили Збройних Сил України (реєстр. № 12143 від 21.10.2024) [113] дозволяє визначити концептуальні засади трансформації сектору безпеки і оборони України в умовах цифрової трансформації конфліктів.

Ухвалення цього законопроекту знаменує перехід від реактивної моделі кіберзахисту до проактивної стратегії кіберстримування. Впровадження Кіберсил як окремого роду сил ЗСУ свідчить про визнання кіберпростору повноцінним доменом ведення бойових дій, рівнозначним суходолу, морю та повітрю.

Важливо виділити три ключові складові, що притаманні законопроекту у контексті новачій та ефективності: інституціоналізація кібероборони, інтероперабельність з НАТО та технологічна перевага. Законопроект завершує формування архітектури державної системи кібербезпеки, чітко розмежовуючи функції цивільного захисту (ДССЗЗІ, СБУ) та ведення активних дій у кіберпросторі (ЗСУ). Це дозволяє реалізувати доктрину «активної оборони». Також, підтверджується орієнтація на стандарти Альянсу (зокрема, STANAG) у питаннях управління та застосування кіберсил сприяє глибшій інтеграції України до колективної системи безпеки Заходу. Це включає обмін даними про загрози в реальному часі та спільне реагування на транскордонні інциденти. А визначення завдань у сфері операцій в електромагнітному спектрі підкреслює конвергенцію кібернетичних та радіоелектронних методів боротьби (Cyber-Electromagnetic Activities, CEMA), що є критичним фактором у сучасній радіоелектронній війні.

Проєкт Закону безпосередньо закладає фундамент для формування кіберстійкості через наступні аспекти:

- розширення адаптивних спроможностей оборони: законопроект передбачає не лише захист власних мереж, а й створення умов для «кіберстримування». Формування кіберстійкості на державному рівні неможливе без здатності завдати превентивного удару або послабити

потенціал агресора, що зменшує інтенсивність навантаження на системи захисту об'єктів критичної інфраструктури.

- наступність та безперервність управління: створення спеціалізованого органу військового управління забезпечує стійкість системи управління військами. Це гарантує, що навіть за умов масованого кібервпливу на державні комунікації, військовий сектор зберігатиме автономність та здатність до скоординованих дій.

- розвиток кадрового та інноваційного потенціалу: проєкт Закону створює правове поле для залучення висококваліфікованих фахівців («кіберрезервістів»), що є ключовим елементом соціальної та організаційної стійкості. Здатність держави швидко мобілізувати інтелектуальний ресурс у критичні моменти є фундаментальною ознакою кіберстійкої нації.

- системність та ієрархічність: кіберстійкість досягається через чіткий розподіл ролей. Законопроект заповнює прогалину в ієрархії національної стійкості, де Кіберсили відповідають за зовнішній периметр загрози (джерело атаки), дозволяючи іншим суб'єктам кібербезпеки фокусуватися на внутрішній стабільності систем.

Таким чином, проєкт Закону про Кіберсили є не просто організаційним документом, а стратегічним інструментом формування національної кіберстійкості. Він забезпечує перехід від концепції «захищеної фортеці» до концепції «динамічної системи», яка здатна не лише виживати під тиском, а й активно трансформувати середовище безпеки на свою користь. Аспекти кіберстійкості у законопроекті мають системний характер і проявляються через зміцнення інституційної готовності, технологічну адаптивність та інтеграцію військових спроможностей у загальнодержавну систему протидії гібридним загрозам.

Аналіз діяльності Департаменту кіберполіції (ДКП) Національної поліції України у системі національної безпеки дозволяє визначити його роль як ключового суб'єкта, що забезпечує правоохоронний складник кібербезпеки та цивільну кіберстійкість.

На відміну від Кіберсил ЗСУ, що орієнтовані на військову відсіч та зовнішній контур, Департамент кіберполіції діє в межах цивільно-правового домену. Його функціонування визначається Законами України «Про Національну поліцію» [104] та «Про основні засади забезпечення кібербезпеки України» [107].

ДКП є основним інструментом держави у боротьбі з кіберзлочинністю. Його діяльність спрямована на документування злочинів у сфері використання ЕОМ, телекомунікаційних мереж та платіжних систем. В умовах воєнного стану ДКП трансформував свою діяльність, включивши завдання з ідентифікації колаборантів, протидії дезінформації та OSINT-розвідки (збір даних про військових злочинців рф з відкритих джерел). Через мережу контактних пунктів «24/7» та співпрацю з Європолем та Інтерполом, ДКП інтегрує Україну у світовий правоохоронний кіберпростір, що є критичним для транскордонних розслідувань.

Діяльність Департаменту кіберполіції містить виразні ознаки формування кіберстійкості, що підтверджується наступними аргументами. Кіберстійкість починається з людського фактора. ДКП реалізує функцію «завчасного інформування населення про новітні кіберзлочини». Створення та підтримка ресурсів для підвищення цифрової грамотності громадян (наприклад, регулярні звіти про фішингові схеми) підвищує поріг вразливості суспільства до атак. Через протидію скімінгу, фішингу та онлайн-шахрайству, ДКП забезпечує стабільність функціонування критичних для економіки сервісів. Здатність поліції оперативно блокувати інфраструктуру зловмисників (C&C-сервери, ботнети) безпосередньо впливає на здатність національної мережі відновлюватися після інцидентів.

Впровадження Big Data аналітики для систематизації кіберінцидентів дозволяє ДКП виявляти патерни атак на ранніх стадіях. Це забезпечує проактивну стійкість: система не просто реагує на злочин, а адаптується до нових методів соціальної інженерії та технічного проникнення.

Крім того, ДКП виступає медіатором у трикутнику безпеки «Держава / Бізнес / Громадянин». Встановлення механізмів зворотного зв'язку (форми звернень, чат-боти) дозволяє швидко акумулювати дані про загрози від приватного сектору, що є основою колективної кіберстійкості.

Таким чином, якщо Кіберсили ЗСУ забезпечують стратегічне стримування ворога, то Департамент кіберполіції формує структурну міцність внутрішнього середовища. Аспекти кіберстійкості у діяльності ДКП реалізуються через мінімізацію ризиків «людського фактора», захист економічного фундаменту держави та створення умов для швидкої ідентифікації та нейтралізації внутрішніх кіберзагроз.

Це робить Кіберполіцію невід'ємним елементом системи «Resilience», яка відповідає за життєздатність соціально-економічних процесів у цифровому вимірі.

Водночас, упровадження підходів ІОСТА (Internet Organised Crime Threat Assessment) – методологія Європолу, що визначає тенденції організованої кіберзлочинності, її рушії, інфраструктури та вплив на суспільство й економіку, у діяльність Департаменту кіберполіції є критичним чинником формування прогностичної кіберстійкості. Ця методологія дозволяє перейти від фіксації окремих інцидентів до комплексного аналізу екосистеми кіберзагроз. Основними аспектами цього процесу є розбудова сучасної моделі правоохоронної діяльності – Intelligence-Led Policing (Поліцейська діяльність, керована аналітичною розвідкою), класифікація та пріоритезація загроз та горизонтальна координація. Зокрема, використання щорічних звітів та аналітичних моделей ІОСТА дозволяє Кіберполіції ідентифікувати вектори загроз, що лише зароджуються (наприклад, конвергенція кіберзлочинності та тероризму або використання ІІІ зловмисниками). Це забезпечує «запас стійкості» через превентивну адаптацію правоохоронних алгоритмів. Завдяки методології Європолу, ДКП структурує зусилля навколо найбільш деструктивних явищ: *он-лайн шахрайство, «злочин як послуга», дезінформація, кібератаки та насильство над дітьми в Інтернет*. Така

фокусованість оптимізує використання обмежених ресурсів, що є базовою вимогою до стійких систем.

Водночас, методологія ІОСТА передбачає синергію між приватним сектором, академічними колами та правоохоронцями. Для України це означає створення стійкої мережі обміну даними, де кіберполіція виступає не лише як силовий орган, а як аналітичний хаб, що посилює загальнонаціональну обізнаність про загрози.

Таким чином, застосування стандартів ІОСТА перетворює Кіберполіцію на адаптивний елемент загальнодержавної системи. Стійкість тут виражається у здатності системи «передбачати – витримувати – відновлюватися – адаптуватися». Знання актуальних трендів організованої кіберзлочинності, отримане через інструментарій Європолу, мінімізує ефект несподіванки під час масованих гібридних атак, що безпосередньо корелює з концепцією національної стійкості.

Варто зазначити, що сучасна архітектура національної кібербезпеки України базується на функціональному розмежуванні сфер відповідальності між Держспецзв'язку та Департаментом кіберполіції, що забезпечує комплексний підхід до формування кіберстійкості. Держспецзв'язку виконує роль головного регулятора та технологічного координатора, зосереджуючи зусилля на створенні превентивного технічного базису захисту об'єктів критичної інфраструктури. Через функціонування Державного центру кіберзахисту та команди CERT-UA, служба забезпечує моніторинг інцидентів, встановлює обов'язкові технічні стандарти безпеки та надає безпосередню допомогу у відновленні працездатності систем після атак. Таким чином, відповідальність Держспецзв'язку концентрується на технологічній стійкості – здатності цифрових мереж витримувати деструктивний вплив та оперативно повертатися до штатного режиму роботи.

Натомість Департамент кіберполіції Національної поліції України оперує в межах правоохоронної парадигми, фокусуючи увагу не на технічних параметрах мереж, а на суб'єктах злочинної діяльності. У контексті захисту

критичної інфраструктури Кіберполіція забезпечує юридичну та операційну стійкість держави шляхом ідентифікації та атрибуції кібератак. Використовуючи інструментарій оперативно-розшукової діяльності та міжнародну методологію ІОСТА, ДКП здійснює документування злочинів, викриває цифрові сліди зловмисників та нейтралізує їхню інфраструктуру (C&C-сервери, ботнети). Це створює ефект невідворотності покарання та фізичного усунення джерела загрози, що є критично важливим для довгострокової стабільності національних інформсистем.

Синергія цих органів формує замкнений цикл кіберстійкості: Держспецзв'язку робить інфраструктуру максимально «складною для зламу» через впровадження стандартів NIST та ISO, тоді як Кіберполіція робить саму спробу зламу максимально «ризикованою та караною» для агресора. Такий розподіл дозволяє уникнути дублювання функцій: поки технічні фахівці CERT-UA локалізують шкідливе програмне забезпечення в енергомережах чи банківському секторі, детективи Кіберполіції паралельно працюють над блокуванням фінансових потоків та серверної бази хакерських угруповань. У підсумку, взаємодія цих суб'єктів перетворює систему кібербезпеки з пасивної оборони на динамічну екосистему, здатну адаптуватися до нових векторів загроз та ефективно протидіяти гібридним викликам сучасності.

Узагальнений аналіз діяльності трьох ключових суб'єктів – Кіберсил ЗСУ, Держспецзв'язку та Департаменту кіберполіції – дозволяє констатувати формування в Україні трирівневої архітектури кібероборони, де кожен компонент виконує специфічну роль у забезпеченні національної кіберстійкості.

Розподіл повноважень між цими інституціями створює цілісну систему захисту держави, що охоплює зовнішній, технологічний та внутрішній периметри безпеки.

Кіберсили ЗСУ – суб'єкт «першого удару» та активної оборони. Його функція полягає у веденні бойових дій у кіберпросторі та електромагнітному спектрі. Основна мета – здобуття військової переваги над ворогом,

послаблення його наступального потенціалу та проведення операцій за межами національного сегмента мережі. Кіберсили забезпечують стратегічну стійкість, нейтралізуючи загрозу безпосередньо в її джерелі.

У свою чергу, *Держспецзв'язку* виконує роль архітектора та головного інженера національної системи захисту. Діяльність служби спрямована на створення «пасивного імунітету» держави через стандартизацію, сертифікацію та методичне керівництво захистом критичної інфраструктури. Через CERT-UA орган забезпечує оперативне реагування на технічні інциденти, локалізацію кіберзагроз та швидке відновлення працездатності систем.

І на завершення, кіберполіція забезпечує внутрішню стабільність та невідворотність покарання. Використовуючи аналітику за стандартами ІОСТА, Департамент бореться з кіберзлочинністю, проводить атрибуцію атак та ліквідує цифрову інфраструктуру зловмисників. Кіберполіція формує соціальну стійкість, підвищуючи цифрову грамотність населення та захищаючи фінансово-економічні інтереси громадян і бізнесу.

У підсумку, формування Кіберсил ЗСУ як нового елемента завершує логічну побудову державної системи. Сьогодні Україна демонструє модель динамічної стійкості, розвиваючи повноваження та спектр активності суб'єктів державної системи кіберстійкості. Зокрема, доки *Держспецзв'язку* «зміцнює стіни» (захист), а кіберполіція «знаходить злочинців» всередині (правопорядок), Кіберсили ЗСУ здійснюють «винесення загрози» за межі держави (військова відсіч). Така диференціація повноважень мінімізує ризики системних збоїв та забезпечує живучість держави в умовах постійної гібридної агресії.

Таким чином, державна вертикаль управління кіберстійкістю України – це складна система стримувань, противаг та спеціалізацій. Наш аналіз підтверджує, що саме така багатосуб'єктна модель забезпечує «живучість» системи управління: навіть у разі тимчасового ураження одного вузла

(органу), інші перебирають на себе критичні функції, забезпечуючи безперервність національної оборони.

Кібервійна, в стані якої сьогодні перебуває Україна, сформувала чіткі переконання надзвичайної ваги у формуванні національної кіберстійкості операторів критичної інфраструктури та приватного сектору. Переосмислення ролі приватного сектору в системі національної кіберстійкості зумовлене тим фактом, що переважна більшість об'єктів критичної інфраструктури (ОКІ) в Україні перебуває у приватній або корпоративній власності [102]. Це створює унікальну правову та організаційну ситуацію, де держава, не будучи безпосереднім власником мереж, несе відповідальність за їхню безпеку перед суспільством. Суб'єктність приватного сектору у сфері стійкості пізнається через триєдину роль: як власника інфраструктури, як надавача критичних послуг та як джерела технологічних інновацій. Водночас, у наукових дослідженнях українських авторів наголошується, що без інтеграції приватного сектору в механізми координації, обміну інформацією та реагування, держава не здатна забезпечити належний рівень кіберстійкості [29; 49].

Згідно із Законом України «Про критичну інфраструктуру» [102], оператори ОКІ є повноправними суб'єктами національної системи захисту. Їхня суб'єктність у контексті стійкості виражається у виконанні низки імперативних обов'язків:

створення та забезпечення функціонування об'єктових підрозділів кіберзахисту: оператор зобов'язаний не просто мати системного адміністратора, а розбудувати повноцінну спроможність щодо моніторингу та реагування;

розробка планів забезпечення безперервності та відновлення: це методична основа «виживання» об'єкта, яка доводить державі здатність ОКІ відновити послугу у встановлені регламентом терміни;

обов'язкове інформування про інциденти: суб'єктність оператора передбачає його інтеграцію в національну мережу обміну даними через CERT-UA або галузеві команди реагування [99].

Корпоративні приватні центри операційної безпеки (SOC – Security Operations Centers) великих телекомунікаційних компаній, банків та енергохолдингів є «першою лінією оборони» країни. Значення цих суб'єктів полягає у їхній здатності обробляти колосальні обсяги трафіку та виявляти аномалії на ранніх стадіях. В Україні приватні SOC часто мають вищий рівень технологічного оснащення, ніж деякі державні органи, що робить їх критично важливими партнерами для НКЦК та Держспецзв'язку. Суб'єктність таких центрів виходить за межі корпоративних інтересів, оскільки їхні дані про нові тактики ворога стають надбанням усієї національної системи стійкості [220; 289].

Новим, але критично важливим суб'єктом стійкості є постачальники ІТ-рішень, хмарних послуг та програмного забезпечення. Атака на «Київстар» або інцидент із ПЗ «М.Е.Дос» у минулому довели, що розробник софту є прихованим вузлом національної стійкості. Обґрунтованим є підхід, що вимагає визнання таких компаній «суб'єктами з опосередкованим впливом». Їхня роль полягає у забезпеченні цілісності розробки та стійкості сервісів, на яких базуються державні цифрові екосистеми (наприклад, хмарні потужності для реєстрів). Водночас, сучасні дослідження показують, що в динамічних цифрових ланцюгах постачання кібербезпека стає невід'ємною частиною управління ризиками, а складні взаємозалежності між розробниками, провайдерами та кінцевими користувачами створюють нові уразливі вузли національної кіберстійкості та потребують інтегрованих стратегій побудови довіри та захисту [15; 57].

Суб'єктність приватного сектору також реалізується через колективні органи – галузеві центри обміну та аналізу інформації (ISACs – Information Sharing and Analysis Centers) [288]. В Україні цей інститут перебуває на стадії активного формування. Структурно-системна цінність ISACs полягає у

створенні «середовища довіри», де конкуренти по ринку (наприклад, різні банки) обмінюються даними про загрози без остраху розголошення комерційної таємниці. Це дозволяє галузі самоорганізовуватися для відсічі складним атакам, не чекаючи директив від державних органів, що значно підвищує швидкість адаптації національної архітектури стійкості [35; 54].

Таким чином, приватний сектор в Україні трансформувався з пасивного споживача безпекових послуг держави на її стратегічного партнера. Суб'єктність бізнесу у сфері кіберстійкості сьогодні підкріплена не лише юридичними обов'язками, а й усвідомленням того, що цифрова витривалість є запорукою ринкової конкурентоспроможності та фізичного збереження активів в умовах війни.

Загалом, концепція національної кіберстійкості України базується на принципі «всеохоплюючої оборони», де суб'єктність не обмежується лише державним та приватним секторами. Особливістю українського досвіду є потужне залучення інтелектуального та волонтерського потенціалу суспільства, що створює так званий «соціальний контур стійкості», який проявляється навіть у діяльності правоохоронних і державних органів у кіберпросторі під час воєнного стану. Такий підхід впливає на захист персональних даних громадян в умовах воєнних загроз; міжнародна співпраця у сфері кібербезпеки забезпечує нормативно-правову адаптацію сектора; адміністративно-правові механізми інформаційної безпеки адаптовані до нових воєнних викликів [75; 120, с. 228]. Цей контур забезпечує приплив інновацій, незалежний аудит та швидке залучення специфічних компетенцій, які неможливо миттєво розвинути всередині державних структур.

Важливо також визначити важливу роль суб'єктів стратегічного форсайту – наукову спільноту та академічні установи. Роль наукових установ (університетів, НДІ Національної академії наук України) у системі кіберстійкості є фундаментальною, хоча часто залишаються поза межами оперативного реагування. Наукова суб'єктність реалізується через:

розробку вітчизняних криптографічних стандартів: стійкість національних систем зв'язку залежить від наявності власних алгоритмів шифрування, що здатні протистояти квантовим загрозам;

методологічне забезпечення: створення науково обґрунтованих моделей ризик-менеджменту та оцінки збитків від кібератак;

підготовку кадрового резерву: університети є суб'єктами відтворення «людського капіталу» – єдиного ресурсу, який здатний адаптуватися до змін тактики ворога швидше за програмні алгоритми [10; 19; 21; 84].

Одним із найбільш динамічних суб'єктів стійкості в Україні стали «білі» (етичні) хакери. Юридичне визнання їхньої діяльності відбулося через зміни до Кримінального кодексу України (ст. 361) у березні 2022 року [96], що дозволило проводити тестування на проникнення без ризику кримінального переслідування, якщо це відбувається в межах програм пошуку вразливостей (Bug Bounty).

Тестування на проникнення тепер не вважається кримінальним правопорушенням, якщо воно проводиться у межах офіційних програм пошуку вразливостей, без зловмисного втручання та з повідомленням власника системи.

Основні зміни та умови безпечного тестування:

легалізація досліджень: заходи з пошуку вразливостей (пентести) у межах програм Bug Bounty виведені з-під дії ст. 361 «Несанкціоноване втручання...»;

узгоджене розкриття: дослідник має право шукати вразливості, але зобов'язаний повідомити власника системи та CERT-UA (або CSIRT) про «дірку» не пізніше ніж через 24 години;

межі дозволеного: дозволяється пошук вразливостей без завдання значної шкоди, без втручання в роботу системи та без експлуатації вразливості, що порушує функціонування;

CERT-UA як координатор: національна команда реагування CERT-UA координує процес та взаємодію між «білим хакером» та державою [100].

Ці зміни, прийняті на основі закону № 2149-IX, перевели взаємодію з дослідниками кібербезпеки із «сірої зони» у правове поле.

Суб'єктність етичних хакерів у системі стійкості полягає у безперервному аудиті (виявленні вразливостей у державних реєстрах та застосунку «Дія» до того, як їх використовують ворожі спецслужби) [45] та формуванні культури відповідального розголошення (встановленні протоколів, за якими дослідник безпеки повідомляє про проблему власнику системи, забезпечуючи її усунення без публічного розголосу, що міг би спричинити паніку) [368].

Але феномен суспільної стійкості в Україні є ІТ-армія та кіберволонтерство. Повномасштабне вторгнення породило унікального суб'єкта – ІТ-армію України. Це волонтерські кібергрупи, створені наприкінці лютого 2022 року на тлі російської агресії для протидії кібератакам та захисту цифрового простору України, а також для проведення контрзаходів у кіберпросторі. Будь-які атаки здійснюються добровільно й координуються через офіційні канали ІТ-армії [293]. Хоча їх правовий статус залишається предметом наукових дискусій (частина експертів вказує на ризики та невизначеність у застосуванні міжнародного гуманітарного права щодо добровольців у кібер-війні), сам феномен має реальний вплив на національну стійкість [416]. Українська ІТ-армія налічувала сотні тисяч волонтерів на ранніх етапах війни: за офіційними повідомленнями, до неї долучилися понад 300 тис. ІТ-спеціалістів зі світу, які підтримували її ініціативи в кіберпросторі [130]. Суб'єктність волонтерських спільнот виражається у здатності до масового перехоплення ініціативи у кіберпросторі, відволіканні ресурсів ворога та створенні «шумового фону», який ускладнює проведення складних операцій проти України (наприклад, у проведенні DDoS-атак та інших операцій, що залучають численні ресурси добровольців для відволікання ресурсів ворога та створення «шумового фону», що ускладнює роботу захисту протилежної сторони [81]). Ці спільноти здебільшого діють без формальної централізованої ієрархії, а їхня діяльність підтримується великим числом

окремих учасників, які координують свої дії через мережі та канали зв'язку (що вже нагадує модель децентралізованої цифрової стійкості) [293].

Досліджуючи це явище, можемо без перебільшення зазначити, що це приклад децентралізованої стійкості, де тисячі розрізнених суб'єктів автономно діють як єдиний організм у кіберпросторі, створюючи колективний ефект у протидії цифровим загрозам [32; 243; 408].

Водночас, згідно з концепцією стійкості, кожен громадянин є суб'єктом безпеки. Неосвіченість одного користувача може призвести до компрометації цілого відомства (через фішинг). Суб'єктність громадян виявляється у дотриманні правил кібергігієни, використанні двофакторної автентифікації та здатності розпізнавати дезінформацію. Сьогодні беззаперечним є висновок, що рівень «когнітивної стійкості» населення є прямо пропорційним загальній стійкості держави до гібридних впливів [21, с. 17].

Отже, інтелектуальний та волонтерський сегмент суб'єктів створює надзвичайну масштабність для України, яку неможливо купити або створити директивно. Саме поєднання державної потужності, приватних технологій та суспільного інтелекту робить національну систему кіберстійкості України унікальною у світовій практиці.

Завершальним етапом формування суб'єктного складу національної системи кіберстійкості є встановлення чіткої вертикалі відповідальності та визначення місця України у глобальному безпековому просторі. Без дієвого механізму примусу та персоналізації відповідальності керівної ланки, будь-яка архітектура стійкості залишатиметься декларативною. Європейське співтовариство саме у період російської агресії і нав'язаної кібервійни, остаточно сформувало своє бачення та нормативно закріпило вимогу щодо відповідальності керівної ланки. Для України імплементації норм Директиви NIS2 у вітчизняне законодавство та врахування досвіду стратегічного планування, закладеного в національних цілях протидії кіберзлочинності, є також надзвичайно важливим елементом кіберстійкості [9; 110; 179; 223].

Одним із найбільш революційних аспектів сучасної суб'єктності є перенесення відповідальності за стан кіберстійкості з технічних фахівців на вище керівництво організації (державного органу чи приватного ОКИ). Згідно з логікою Директиви (EU) 2022/2555 (NIS2) [179; 223], керівники несуть персональну відповідальність (аж до тимчасового відсторонення від посад та значних фінансових санкцій) за незабезпечення належного управління ризиками.

Директива (EU) 2022/2555 (NIS2) встановлює єдиний високий рівень кібербезпеки в Європейському Союзі та значно розширює вимоги до керівництва організацій. Це включає операторів критичної інфраструктури, які забезпечують функціонування ключових секторів економіки та безпеки.

Загалом можливим є виділення декількох ключових положень щодо відповідальності керівництва:

пряма відповідальність керівників: топ-менеджмент несе персональну відповідальність за дотримання вимог NIS2, що означає, що керівники повинні забезпечити впровадження належних заходів кіберзахисту та управління ризиками;

обов'язок контролю та нагляду: керівництво має гарантувати, що організація дотримується правил управління кіберризиками, включаючи політики безпеки, процедури реагування на інциденти та безперервність бізнесу;

навчання та компетентність: директива прямо вимагає, щоб керівники проходили регулярне навчання з питань кібербезпеки, аби мати необхідні знання для прийняття рішень;

санкції за недотримання: у випадку порушення вимог NIS2 передбачені значні адміністративні штрафи та інші заходи впливу, що створює реальний стимул для керівництва приділяти увагу кібербезпеці на стратегічному рівні.

інтеграція в корпоративне управління: кіберризики мають бути включені до загальної системи управління ризиками компанії, а

відповідальність за їх мінімізацію лежить на раді директорів та виконавчому менеджменті.

Таким чином, NIS2 переводить кібербезпеку з технічної площини у площину корпоративної відповідальності, де керівництво ОКІ стає ключовим гарантом дотримання стандартів та захисту суспільно важливих процесів. Це означає, що питання кіберстійкості тепер є не лише завданням ІТ-підрозділів, а й стратегічною функцією управління.

Для України це означає необхідність трансформації суб'єктності через:
юридичне закріплення обов'язків вищої ланки: керівник має особисто затверджувати заходи з кіберстійкості та контролювати їх виконання;

навчання керівного складу: стійкість починається з розуміння стратегічних ризиків на рівні прийняття рішень, а не лише на рівні серверної кімнати;

матеріальну та кримінальну відповідальність за недбалість: у разі успішної атаки на КІІ, що спричинила тяжкі наслідки, суб'єктом відповідальності стає посадова особа, яка проігнорувала приписи регулятора.

Україна активно працює над імплементацією Директиви (EU) 2022/2555 (NIS2), яка встановлює високі стандарти кібербезпеки для критичних секторів. Віцепрем'єр-міністр з інновацій та цифрової трансформації Михайло Федоров наголошував [129], що Україна прагне приєднатися до кіберрезерву ЄС у рамках програми «Цифрова Європа» та забезпечити відповідність національної системи кіберстійкості європейським вимогам.

У цьому контексті Кабінет Міністрів України ухвалює постанови, що визначають механізми реалізації європейських норм. Зокрема, у 2024 році уряд прийняв постанову №1318 [42], яка закріплює інституційні механізми виконання зобов'язань України перед ЄС у сфері цифрової трансформації та безпеки. Це рішення стало важливим кроком для формування національної системи координації у сфері кібербезпеки та адаптації положень NIS2 до українських реалій.

Імплементація зазначених вимог в національні правові норми забезпечує важливі аспекти кіберстійкості для України:

відповідальність керівництва ОКІ: як і в ЄС, топ-менеджмент українських операторів критичної інфраструктури має бути персонально відповідальним за впровадження політик кіберзахисту;

національна координація: постанови КМУ створюють правову основу для взаємодії державних органів та бізнесу у сфері кіберстійкості;

європейська інтеграція: імплементація NIS2 є частиною ширшого процесу наближення України до стандартів ЄС у сфері цифрової безпеки;

практичні наслідки: керівництво ОКІ повинно інтегрувати кіберризики у систему корпоративного управління та забезпечити навчання персоналу.

Саме із врахуванням аспектів більш широкого процесу євроінтеграції України та інтеграції кіберризиків у систему корпоративного управління на нормативному рівні закріплено ризик менеджмент в якості важливого компонента кібербезпеки та кіберстійкості загалом.

Імплементація Директиви (EU) 2022/2555 (NIS2) в Україні здійснюється шляхом поступового формування комплексної системи управління кіберризиками [97], яка має забезпечити відповідність національної моделі кіберзахисту європейським стандартам. Центральним інституційним суб'єктом цього процесу виступає Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). Саме цей орган розробив та затвердив каталог заходів з кіберзахисту, базові вимоги [36] та методичні рекомендації [37], що є обов'язковими для органів державної влади та операторів критичної інфраструктури.

Ключовим принципом, який лежить в основі як NIS2, так і українських нормативних актів, є ризик-орієнтований підхід. Він передбачає, що заходи з кіберзахисту не можуть бути універсальними чи шаблонними, а повинні враховувати реальні ризики, специфіку діяльності та рівень критичності конкретного об'єкта. Такий підхід забезпечує диференціацію механізмів

захисту та дозволяє оптимізувати витрати на безпеку, спрямовуючи ресурси на найбільш уразливі сегменти .

Нормативна база та координаційні механізми також демонструють узгодженість із європейськими вимогами. Директива NIS2 встановлює єдиний високий рівень кібербезпеки для держав-членів ЄС. В Україні аналогічну функцію виконує Постанова Кабінету Міністрів України №1470 від 2025 року, яка визначає порядок впровадження ризик-орієнтованого підходу та закріплює повноваження Держспецзв'язку щодо координації заходів кіберзахисту .

Як вже зазначалося, важливим елементом імплементації є визначення відповідальності керівництва. В Україні аналогічні норми відображені у методичних рекомендаціях Держспецзв'язку щодо ролі та функцій керівників з кіберзахисту (CISO) та спеціалізованих підрозділів. Вони зобов'язані здійснювати управління ризиками, реагувати на інциденти та планувати витрати на безпеку на основі оцінки загроз.

Окремо слід відзначити положення щодо галузевих стандартів. NIS2 дозволяє секторальним органам розробляти специфічні вимоги до кіберзахисту, що враховують особливості конкретних сфер. В Україні аналогічний механізм передбачає можливість формування секторальних стандартів, які погоджуються з Адміністрацією Держспецзв'язку. Це забезпечує узгодженість національної системи з європейськими нормами та водночас враховує специфіку окремих галузей.

Не менш важливим є аспект навчання та підвищення компетентності. Директива NIS2 прямо вимагає регулярного навчання керівників та персоналу з питань кібербезпеки. В Україні ця вимога закріплена у методичних рекомендаціях Держспецзв'язку, які передбачають систематичне навчання працівників з кібергігієни та кіберзахисту .

Таким чином, аналіз положень NIS2 та українських нормативних актів свідчить про високий рівень їхньої узгодженості. Спільними рисами є ризик-орієнтований підхід, персональна відповідальність керівництва, обов'язковість навчання та можливість секторальної деталізації вимог.

Постанова КМУ №1470 та каталоги заходів Держспецзв'язку формують основу для створення єдиної системи управління кіберризиками, яка відповідає європейським стандартам і водночас враховує національні особливості.

Ризик-орієнтований підхід у сфері кіберзахисту є фундаментальною складовою формування загального концепту кіберстійкості. Його сутність полягає у систематичній ідентифікації, оцінці та моніторингу загроз, а також у впровадженні заходів, спрямованих на зниження ризиків до прийнятного рівня. Такий підхід забезпечує адаптивність системи безпеки, дозволяючи організаціям не лише реагувати на вже реалізовані інциденти, але й прогнозувати потенційні загрози та мінімізувати їхній вплив.

У контексті кіберстійкості ризик-орієнтований підхід виконує роль інтеграційного механізму, що поєднує технічні, організаційні та управлінські інструменти. Він сприяє формуванню культури безпеки, де відповідальність за захист інформаційних систем розподіляється між керівництвом, спеціалізованими підрозділами та персоналом. Це відповідає сучасним європейським стандартам, закріпленим у Директиві (EU) 2022/2555 (NIS2), та узгоджується з українською нормативною базою, зокрема постановами Кабінету Міністрів України та методичними рекомендаціями Держспецзв'язку.

Таким чином, ризик-орієнтований підхід не лише забезпечує ефективне управління кіберзагрозами, але й формує основу для стійкості інформаційних систем у довгостроковій перспективі. Він перетворює кіберзахист із суто технічної функції на стратегічний елемент корпоративного управління, що є ключовим для побудови цілісної системи кіберстійкості держави та критичної інфраструктури.

Сьогодні ми можемо констатувати, що Україна вже не є просто спостерігачем, а стала активним суб'єктом міжнародної системи кіберстійкості. Це підтверджується її інституційною інтеграцією у провідні

міжнародні структури та визнанням практичного досвіду протидії кіберагресії у міжнародних аналітичних звітах [163; 205; 206; 392].

Важливою є участь в Об'єднаному центрі передових технологій з кібероборони НАТО (CCDCOE). Україна ділиться унікальним досвідом відсічі повномасштабної агресії, що робить її ключовим контрибутором до глобальних стандартів стійкості. Активною є взаємодія в межах CSIRTs Network. CERT-UA є повноправним учасником міжнародної мережі груп реагування, забезпечуючи транскордонну стійкість. Загалом, набутий досвід у кібервійні викликає надзвичайний інтерес серед партнерів, і Україна щиро ділиться з ними своїми надбаннями, розуміючи важливість глобальної безпеки у кіберпросторі та неординарні сучасні виклики.

Формування суб'єктного складу системи кіберстійкості України на сучасному етапі характеризується переходом від ієрархічної моделі до динамічної екосистеми, де НКЦК при РНБО України виконує роль стратегічного координатора, а CERT-UA – операційного вузла взаємодії. Міжнародна суб'єктність України у цій архітектурі підтверджується статусом контрибутора безпеки: залученість до Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) дозволяє не лише реценувати передовий досвід, а й брати участь у формуванні глобальних протоколів стійкості на основі унікального практичного досвіду відсічі повномасштабної кіберагресії. Це закріплює за національними суб'єктами роль ключових ланок у транскордонній мережі кіберзахисту, що відповідає вимогам колективної стійкості в межах євроатлантичного простору

Отже, інституціоналізація відповідальності та міжнародне визнання завершують формування суб'єктного складу системи. Суб'єкт у сфері кіберстійкості – це не просто юридична особа, а активна одиниця, яка несе відповідальність за свій сегмент безпеки, володіє сучасними інструментами аналізу та діє у синергії з міжнародною спільнотою.

2.3. Організаційно-правові механізми цивільно-військового співробітництва у формуванні національної системи кіберстійкості

В умовах сучасних гібридних загроз і зростання складності кіберінфраструктури національна безпека України потребує інтегрованих підходів до координації державних, приватних та громадських суб'єктів. Цивільно-військове співробітництво (ЦВС) виступає не лише механізмом взаємодії між військовими та цивільними структурами, а й системоутворюючим елементом національної архітектури кіберстійкості. Його значення полягає у здатності забезпечувати ефективну координацію, стандартизоване об'єднання ресурсів і компетенцій різних секторів, а також формувати стійку кіберархітектуру, здатну до швидкого реагування на кібератаки та гібридні загрози.

Цивільно-військове співробітництво у сучасних умовах слід розглядати не лише як механізм оперативної координації між військовими та цивільними структурами, а як системоутворюючий компонент національної архітектури кіберстійкості. У класичному розумінні ЦВС, представленому у моделі CIMIC (Civil-military cooperation) НАТО, акцент робиться на забезпеченні взаємодії з цивільним населенням та критичною інфраструктурою у рамках військових операцій. Однак сучасні дослідження показують, що в умовах гібридних конфліктів та високої динаміки кіберзагроз ця модель трансформується в ширший механізм інтеграції державного, приватного та громадського секторів у систему національної безпеки [172].

Зарубіжні наукові праці підкреслюють, що ефективність ЦВС у кіберсфері визначається здатністю об'єднувати суб'єктів різного рівня та профілю – від державних органів і військових підрозділів до приватних компаній та громадських організацій – у мережеву, інтегровану систему реагування на загрози. Так, у дослідженнях НАТО та Центру передового досвіду з кібероборони зазначається, що цивільний компонент стає не просто «партнером», а рівноправним суб'єктом стратегічного забезпечення

кіберстійкості, що включає стандартизацію процедур, обмін розвідувальними даними про загрози та спільне навчання [172].

Українські наукові публікації показують, що концептуальні основи ЦВС ще перебувають на стадії адаптації міжнародного досвіду до національних умов. Автори зазначають, що ЦВС в Україні розглядається переважно як інструмент координації між державними органами та військовими підрозділами, водночас залишаючи поза увагою інтеграцію приватного сектору та громадянського суспільства [11; 73]. Водночас, з огляду на сучасні кіберзагрози, ЦВС в Україні має потенціал для трансформації в системоутворюючий елемент національної кіберстійкості, який поєднує міжсекторальну взаємодію, координацію суб'єктів сектору безпеки і оборони та державно-приватне партнерство.

Ключовим у цьому контексті є розуміння, що ЦВС функціонує на перетині стратегічного, тактичного та операційного рівнів. Стратегічний рівень передбачає формування політик і стандартів взаємодії, тактичний – планування навчань і симуляційних сценаріїв, а операційний – безпосереднє реагування на кіберінциденти та кризові ситуації. Така багаторівнева модель дозволяє забезпечити ефективність координації та інтеграції всіх суб'єктів національної системи кіберстійкості [92, с. 113].

Отже, теоретико-концептуальний аналіз демонструє, що ЦВС в сучасних умовах виходить за межі класичного військово-операційного інструменту і стає ключовим чинником забезпечення національної стійкості в кіберпросторі, здатним інтегрувати державний, приватний та громадський сектори, стандартизувати процедури взаємодії та підвищувати оперативну та стратегічну адаптивність системи [11; 172].

Важливим компонентом ефективного функціонування ЦВС у національній системі кіберстійкості є правове регулювання, яке визначає повноваження державних органів, військових структур, приватних компаній та громадських інституцій, а також порядок їхньої взаємодії у сфері кібербезпеки.

Водночас, хоча термін «цивільно-військове співробітництво» (ЦВС) в українському нормативному полі існує, однак його використання у сфері кібербезпеки є опосередкованим, а не базовим або системно закріпленим як окрема категорія.

Якщо розглядати нормативно-правову базу, то поняття цивільно-військового співробітництва прямо закріплене передусім у секторі оборони та безпеки, а не спеціально у кібербезпеці.

Передусім, термін нормативно визначений у документах Міністерства оборони та Збройних Сил України. Зокрема, у доктринальних актах ЗСУ цивільно-військове співробітництво розглядається як система взаємодії між військовими формуваннями, органами державної влади, місцевого самоврядування, громадянським суспільством та населенням з метою створення сприятливих умов виконання військових завдань. Ця категорія імплементована відповідно до стандартів НАТО (CIMIC – Civil-Military Cooperation) [46].

Крім того, Верховна Рада 20 листопада 2024 року ухвалила Закон № 4068-IX (законопроект 11423), який офіційно врегульовує цивільно-військове співробітництво (ЦВС) в Україні як ефективний елемент національного спротиву. Закон забезпечує взаємодію Збройних Сил із цивільним середовищем для виконання бойових завдань та допомоги населенню, особливо в зонах бойових дій. Основною метою саме і стало створення сприятливих умов для виконання завдань ЗСУ, захист цивільного населення, підтримка місцевої влади та інфраструктури, що передбачає налагодження відносин між військовими та цивільними, моніторинг ситуації, гуманітарна допомога, евакуація, відновлення критичної інфраструктури. Для реалізації ключових положень Закону Кабінет Міністрів України розробляє відповідні нормативно-правові акти.

Законодавчі документи визначають правовий статус суб'єктів ЦВС, зокрема їхню участь у кризових заходах, відповідальність за забезпечення безпеки критичної інфраструктури та порядок взаємодії з приватним сектором

і громадянським суспільством. Однак наукові дослідження вказують на наявність прогалин у нормативній базі, що стосуються формалізації державно-приватного партнерства, регламентації процедур обміну розвідувальними даними про кіберзагрози та участі громадських організацій у забезпеченні кіберстійкості [73].

Водночас, стратегічні документи підкреслюють необхідність узгодження національних стандартів ЦВС із міжнародними практиками, зокрема стандартами НАТО, для забезпечення сумісності та ефективності процедур реагування на кіберінциденти. Це включає формалізацію протоколів обміну інформацією, визначення критеріїв оцінки ризиків і розробку алгоритмів спільного реагування на загрози, що дозволяє інтегрувати державні та приватні ресурси в єдину кібер-архітектуру [172].

Науковці також зазначають, що нормативна визначеність ЦВС має бути поєднана з гнучкістю правових механізмів, що дозволяє швидко адаптуватися до змін у загрозовому середовищі, включаючи гібридні кібератаки. Такі адаптивні підходи сприяють створенню єдиної системи кіберстійкості, де державні органи, приватні компанії та громадські інституції взаємодіють на основі чітких правових норм, стандартизованих процедур та регулярного обміну аналітичними даними [11, с. 155].

Таким чином, законодавчі засади ЦВС формують каркас інтеграції всіх учасників національної системи кіберстійкості, забезпечують правову передбачуваність і відповідальність, стандартизують взаємодію державного і приватного секторів та створюють умови для адаптивного реагування на сучасні кіберзагрози. Водночас, виявлені прогалини стимулюють подальші дослідження щодо уніфікації стандартів, формалізації державно-приватного партнерства та залучення громадянського суспільства до системи кіберстійкості України.

Водночас, що стосується безпосередньо сфери кібербезпеки, важливим є також зазначити, що у Законі України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України та відповідних

підзаконних актах, що регламентують механізми координації, обміну інформацією та реагування на кіберзагрози [92; 107; 110], термін *«цивільно-військове співробітництво»* не використовується. Натомість закладено модель міжвідомчої взаємодії, що фактично виконує аналогічну функцію.

Водночас, системний погляд на означену проблему дозволяє виокремити три рівні присутності ЦВС у чинному нормативному полі України щодо кібербезпеки: прямий, опосередкований та концептуальний.

Щодо першого рівня – прямого, ми вже зазначили про відсутність даної термінології. Водночас, у законодавстві про оборону та діяльність Збройних Сил категорія цивільно-військового співробітництва (CIMIC) нормативно існує в межах функціонування Збройних Сил України, де вона стосується взаємодії військових формувань із органами державної влади, місцевого самоврядування, населенням та організаціями. Однак цей термін не транспонований у кібербезпекову сферу як самостійна категорія.

Другий рівень – опосередкований, стосується функціональних аспектів. У кібербезпекових актах закладено механізми, які за своєю суттю реалізують модель цивільно-військової взаємодії, але під іншими назвами. Йдеться про: координацію суб'єктів сектору безпеки і оборони; державно-приватне партнерство; взаємодію з операторами критичної інфраструктури; обмін інформацією про кіберінциденти; спільне реагування на кібератаки.

У Законі України «Про основні засади забезпечення кібербезпеки України» визначено систему суб'єктів кібербезпеки, до якої входять як військові формування, так і цивільні органи та приватний сектор. У Стратегії кібербезпеки України прямо підкреслюється необхідність консолідації зусиль держави, бізнесу та громадянського суспільства. Це фактично відповідає логіці CIMIC, але в кіберпросторі.

Третій рівень – концептуальний і він є еволюційним. Після 2022 року модель кібероборони України на практиці набула ознак розширеного цивільно-військового співробітництва. Взаємодія між військовими структурами (зокрема підрозділами кібероборони ЗСУ), Службою безпеки

України, Державною службою спеціального зв'язку та захисту інформації України, приватними ІТ-компаніями та волонтерськими кіберініціативами формує нову модель, яку можна визначити як кібернетичний формат цивільно-військового партнерства.

Таким чином, з точки зору доктринального розвитку, це створює простір для формування авторського визначення дефініції: *цивільно-військове співробітництво у сфері кібербезпеки (Cyber-CIMIC) – це нормативно та організаційно забезпечена система взаємодії військових формувань, суб'єктів сектору безпеки і оборони, органів державної влади, операторів критичної інфраструктури, приватного сектору та інститутів громадянського суспільства, спрямована на запобігання, виявлення, стримування та нейтралізацію кіберзагроз в умовах мирного часу, кризових ситуацій і воєнного стану. Із врахуванням більш лаконічного та формального формулювання та з огляду на відсутність зазначеного терміну в чинному законодавстві пропонується додати статтю 1 Закону України «Про основні засади забезпечення кібербезпеки України» пунктом такого змісту:*

«цивільно-військове співробітництво у сфері кібербезпеки (Cyber-CIMIC) – система заходів з організації взаємодії між суб'єктами сектору безпеки і оборони, державними органами, приватним сектором та громадянським суспільством задля підвищення національної кіберстійкості, захисту критичної інформаційної інфраструктури та спільної відсічі кіберагресії».

У стратегічному вимірі таке визначення дозволяє концептуалізувати фактичну модель взаємодії, обґрунтовувати потребу у її нормативному закріпленні та інтегрувати її в систему забезпечення кіберстійкості держави.

Більш глибоке розуміння змісту зазначених термінів: *державно-приватне партнерство; міжсекторальна взаємодія; координація суб'єктів сектору безпеки і оборони; взаємодія з приватним сектором та громадянським суспільством*, – розкривається через порівняння з ЦВС, яке доцільно здійснювати через співвідношення їх функціональної природи з

класичною моделлю цивільно-військового співробітництва (СІМІС), сформованою в системі НАТО. Якщо СІМІС у натівській доктрині є спеціалізованою військовою функцією координації з цивільним середовищем задля досягнення операційних цілей, то українські механізми у сфері кібербезпеки розвиваються як багатовекторна модель взаємодії, що лише частково співвідноситься з класичним ЦВС.

Перший блок – державно-приватне партнерство. У межах Закон України «Про основні засади забезпечення кібербезпеки України» та положень Стратегія кібербезпеки України державно-приватне партнерство визначається як один із базових інструментів забезпечення кіберстійкості. Його зміст полягає у спільному управлінні ризиками, обміні інформацією про інциденти, залученні експертного потенціалу бізнесу та спільному реагуванні на кіберзагрози. За своєю природою це горизонтальний механізм взаємодії, де сторони зберігають автономність. На відміну від класичного ЦВС, де військове командування виступає координуючим центром, у державно-приватному партнерстві відсутній пріоритет військової місії як домінуючої мети. Отже, цей блок лише частково відповідає логіці ЦВС: він реалізує принцип взаємодії військового та цивільного компонентів, але без операційної ієрархії, притаманної СІМІС.

Водночас, міжсекторальна взаємодія у кібербезпековій архітектурі України має системний характер і передбачає координацію між різними секторами – оборонним, безпековим, економічним, інформаційним, науково-технічним. Інституційним ядром такої координації виступає Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Якщо співвідносити це з ЦВС, то міжсекторальна взаємодія є ширшою категорією. СІМІС у НАТО обмежений переважно відносинами між військовими структурами та цивільним середовищем у контексті конкретної операції. Українська ж модель міжсекторальної взаємодії охоплює постійний режим функціонування держави, незалежно від наявності військової операції. Таким чином, міжсекторальна взаємодія концептуально перевищує класичне

ЦВС і трансформує його у постійну модель інтегрованого управління ризиками.

Щодо координації суб'єктів сектору безпеки і оборони, то тут простежується найближча відповідність до ЦВС. Взаємодія між Збройними Силами України, Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації України та іншими суб'єктами має ознаки координаційної вертикалі, особливо в умовах воєнного стану. Однак навіть у цьому випадку українська модель не передбачає створення окремої структури цивільно-військового співробітництва в кіберпросторі. Координація здійснюється через наявні механізми стратегічного управління, а не через спеціалізований «кібер-СІМІС» підрозділ. Отже, функціонально цей блок близький до ЦВС, але організаційно є іншим за своєю природою.

А ось компонент взаємодії з приватним сектором та громадянським суспільством, на практиці кібероборони після 2022 року, саме набув особливої ваги. Волонтерські ініціативи, експертні спільноти, ІТ-компанії стали активними учасниками протидії кіберзагрозам. У класичному розумінні СІМІС така взаємодія здійснюється в межах підтримки військової операції і має чітко регламентований характер. В Україні ж вона часто має мережевий, динамічний, частково неформалізований характер. Тобто за змістом це відповідає логіці цивільно-військового співробітництва, але за формою виходить за межі класичної моделі, демонструючи більш гнучку й адаптивну систему.

Узагальнюючи, можна констатувати, що всі чотири блоки функціонально співвідносяться з концепцією цивільно-військового співробітництва, однак кожен з них відображає лише окремий її аспект. Державно-приватне партнерство репрезентує економічно-інституційний вимір ЦВС, міжсекторальна взаємодія – стратегічно-координаційний вимір, координація суб'єктів сектору безпеки і оборони – управлінсько-операційний вимір, а взаємодія з громадянським суспільством – соціально-комунікаційний вимір.

Таким чином, українська кібербезпекова модель фактично формує розширений варіант ЦВС, який має мережевий характер і функціонує на постійній основі, а не лише в умовах військової операції. Саме ця відмінність є ключовою: якщо CIMIC у системі НАТО є інструментом забезпечення військової місії, то українська модель – це елемент загальнонаціональної кіберстійкості.

З нормативної точки зору це означає доцільність інтеграції зазначених блоків у єдину концепцію цивільно-військового співробітництва у кіберпросторі, що дозволить систематизувати вже існуючі механізми та надати їм доктринальної завершеності.

Здійснивши аналіз вітчизняної системи ЦВС у сфері кібербезпеки важливо провести порівняльний аналіз моделі CIMIC НАТО та української кібербезпекової архітектури. Порівняльний аналіз моделі цивільно-військового співробітництва НАТО (CIMIC) та української кібербезпекової архітектури доцільно здійснювати не лише у площині формальних дефініцій, а передусім через призму функціонального призначення, інституційної побудови та нормативної визначеності.

У системі НАТО CIMIC є чітко доктриналізованою спроможністю, інтегрованою в оперативне планування та реалізацію військових місій. Його нормативна база сформована у стандартизованих доктринальних документах Альянсу, де цивільно-військове співробітництво розглядається як координаційна функція командування, спрямована на забезпечення взаємодії з цивільними учасниками в зоні операції. Ключовою характеристикою є інституційна визначеність: існують підготовлені підрозділи, процедури, алгоритми взаємодії, канали комунікації та механізми інтеграції цивільних ресурсів у військове планування. Метою CIMIC не є підпорядкування цивільних структур військовим, а створення умов для досягнення стратегічного ефекту через координацію інтересів, ресурсів і компетенцій.

Українська кібербезпекова архітектура має іншу генезу. Вона формувалася як відповідь на гібридні загрози, кібератаки проти державних

інституцій та об'єктів критичної інфраструктури, а з 2022 року – в умовах повномасштабної збройної агресії. Її нормативна основа закладена у Закон України «Про основні засади забезпечення кібербезпеки України», який визначає систему суб'єктів кібербезпеки, принципи координації та загальні механізми реагування на кіберінциденти. Стратегічний розвиток системи відображено у Стратегія кібербезпеки України, де наголошено на консолідації державних органів, бізнесу та громадянського суспільства.

Інституційно центральну координаційну роль відіграє Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Операційні функції розподілені між Збройними Силами України, Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації України та іншими суб'єктами сектору безпеки і оборони.

Однак, на відміну від натівської моделі, в Україні відсутня окрема доктринальна категорія, яка б прямо визначала цивільно-військове співробітництво у кіберпросторі. Взаємодія між військовими структурами, державними органами, операторами критичної інфраструктури та приватними ІТ-компаніями реалізується через механізми координації, обміну інформацією, державно-приватного партнерства, але без уніфікованої концептуальної рамки. Українська модель має мережевий характер: вона ґрунтується на горизонтальних зв'язках, гнучкості та швидкому обміні даними, що відповідає природі кіберпростору, але ускладнює формалізацію відповідальності та процедур.

Функціонально українська система вже фактично виконує роль «Cyber-SIMIS». Після 2022 року відбулася глибока інтеграція військових підрозділів кібероборони з цивільними ІТ-структурами, волонтерськими ініціативами та приватним сектором. Ця модель продемонструвала високу адаптивність та ефективність. Водночас її нормативне забезпечення залишається фрагментарним, що створює ризики правової невизначеності, особливо щодо статусу учасників взаємодії, режиму обміну інформацією, відповідальності та гарантій захисту даних.

Порівняння дозволяє зробити кілька принципових висновків. По-перше, українська кібербезпекова архітектура за змістом уже відповідає логіці цивільно-військового співробітництва, але потребує доктринальної артикуляції цієї моделі. Формалізація поняття могла б усунути термінологічну прогалину та забезпечити єдність підходів. По-друге, на відміну від НАТО, де CIMIC орієнтований переважно на підтримку військових операцій у визначеному театрі дій, українська модель повинна враховувати безперервність кіберпростору та його тотальний характер. Отже, національна «Cyber-CIMIC» концепція має бути інтегрована не лише у воєнну доктрину, а й у систему кіберстійкості держави загалом.

По-третє, законодавчі перспективи розроюляються у трьох напрямках: внесення змін до профільного закону з метою закріплення принципу цивільно-військової взаємодії у сфері кібербезпеки як одного з базових принципів державної політики; розроблення окремого підзаконного акту або доктринального документа, який би визначив механізми взаємодії військових структур з операторами критичної інфраструктури та приватним сектором у разі кіберконфлікту; унормування статусу суб'єктів, які беруть участь у кіберобороні поза межами класичних військових формувань, із визначенням гарантій правового захисту та відповідальності.

З урахуванням стратегічного курсу на інтеграцію до євроатлантичного безпекового простору, гармонізація підходів до цивільно-військового співробітництва у кіберсфері може стати одним із напрямів адаптації законодавства України до стандартів Альянсу. Водночас така адаптація має враховувати український досвід мережевої кібероборони, який фактично розширює класичну модель CIMIC і може розглядатися як її еволюційний розвиток у цифрову епоху.

Розгортаючи порівняльний аналіз, доцільно виходити з того, що модель CIMIC у НАТО формувалася як інструмент забезпечення військових операцій у складному середовищі цивільної присутності, тоді як українська кібербезпекова архітектура еволюціонувала під впливом гібридної агресії та

масштабної кібервійни. Попри різні історичні витоки, їх об'єднує інтеграційна логіка взаємодії військових і цивільних суб'єктів.

У системі НАТО цивільно-військове співробітництво (СІМІС) інституціоналізоване як функціональна спроможність Альянсу. Воно визначене у доктринальних документах НАТО і розглядається як координаційна діяльність між військовим командуванням та цивільними акторами в зоні операцій. Ключовим є те, що СІМІС має чітку доктринальну основу, організаційну структуру, підготовлені підрозділи та стандартизовані процедури взаємодії. Його мета – підтримка військової місії шляхом залучення цивільних ресурсів, координації з міжнародними організаціями, місцевою владою, населенням і бізнесом. В основі лежить принцип функціональної комплементарності: цивільний компонент не підпорядковується військовому, але інтегрується через механізми координації.

На відміну від цього, українська кібербезпекова архітектура формувалася не як допоміжний елемент військових операцій, а як багаторівнева система національної стійкості. Її нормативний фундамент закладено у Закон України «Про основні засади забезпечення кібербезпеки України», який визначає коло суб'єктів кібербезпеки, принципи координації та роль державних органів. Стратегічне бачення розвитку системи викладене у Стратегія кібербезпеки України, де наголошено на консолідації держави, приватного сектору та громадянського суспільства. Координаційний центр моделі – Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України.

Порівняння за інституційним критерієм показує, що в НАТО СІМІС є окремою доктринально оформленою спроможністю з визначеною вертикаллю управління. В Україні ж кібербезпекова взаємодія розподілена між низкою суб'єктів – Збройні Сили України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України та іншими, – без виокремлення спеціалізованої «кібер-СІМІС» структури. Координація існує, але вона має мережевий, а не ієрархічно-доктринальний характер.

За функціональним критерієм СІМІС у НАТО спрямований на забезпечення військової операції в конкретному театрі дій. Українська модель кібербезпеки має постійний, системний характер і охоплює мирний час, кризу та воєнний стан одночасно. Якщо СІМІС орієнтований на локальний простір операції, то українська кіберархітектура функціонує в умовах безперервного національного кіберпростору, що не має географічних меж.

За нормативним критерієм різниця ще виразніша. У НАТО СІМІС чітко визначений у доктринальних документах та стандартах. В Україні взаємодія військових і цивільних суб'єктів у кіберсфері не має єдиного концептуального визначення. Вона закріплена через норми про координацію, державно-приватне партнерство, обмін інформацією про інциденти та захист критичної інфраструктури. Тобто українська модель реалізує функцію СІМІС, але без формалізованої термінології.

Водночас існує й суттєва спільність. Обидві моделі ґрунтуються на принципі інтегрованої безпеки. І в НАТО, і в Україні військовий компонент не може ефективно діяти без цивільних ресурсів – технологічних, інформаційних, інфраструктурних. Особливо це проявилось після 2022 року, коли українська кібероборона фактично інтегрувала державні структури, ІТ-бізнес і волонтерські спільноти у спільну екосистему протидії кіберзагрозам. У цьому сенсі українська практика навіть випереджає класичну модель СІМІС, оскільки демонструє гнучку мережеву взаємодію у цифровому середовищі.

Таким чином, ключова відмінність полягає у ступені доктринальної формалізації: у НАТО СІМІС – це інституціоналізована військова спроможність; в Україні – це фактична, але термінологічно неоформлена модель кібернетичного цивільно-військового партнерства. Тобто. ключовою подібністю є інтеграційна природа взаємодії та залежність військової ефективності від цивільних ресурсів.

З об'єктивної точки зору це дозволяє обґрунтовувати, що українська кібербезпекова архітектура потребує концептуалізації власної моделі «Cyber-

CIMIC» – не як кальки натівської доктрини, а як елементу системи національної кіберстійкості.

Аналіз зарубіжних і українських публікацій дозволяє констатувати, що проблема співвідношення цивільно-військового співробітництва, державно-приватного партнерства та міжсекторальної взаємодії у сфері кібербезпеки є міждисциплінарною, але поки що фрагментарно дослідженою. Науковий дискурс можна згрупувати у кілька відносно однорідних напрямів.

Одна група зарубіжних досліджень, присвячена доктринальному осмисленню цивільно-військової взаємодії у кіберпросторі в межах підходів НАТО. У праці авторів [172], а також у дослідженнях, що спираються на положення Таллінського посібника застосування міжнародного права до кібервійни (Tallinn Manual) [392], увага зосереджується на інституційній ролі військових структур у кібербезпеці, правових межах застосування сили в кіберпросторі та координації з цивільними суб'єктами. Предметом аналізу виступає трансформація класичної моделі CIMIC у цифровому середовищі. Ключовий висновок цих авторів полягає в тому, що без системної інтеграції цивільного сектору – операторів інфраструктури, телекомунікаційних компаній, провайдерів кіберзахисту – військовий компонент кібероборони втрачає ефективність. Водночас наголошується на необхідності чіткої правової регламентації меж такої взаємодії, щоб уникнути надмірної мілітаризації цивільного кіберпростору.

Інші зарубіжні публікації охоплюють проблематику державно-приватного партнерства та обміну інформацією щодо кіберзагроз. Роботи дослідників [314; 352; 360] та інші дослідження у журналі *Journal of Cybersecurity* (Oxford Academic) [299], зосереджені на механізмах інтеграції приватних компаній у національні системи кібербезпеки. Предметом їх аналізу є технічні й організаційні моделі обміну розвідувальною інформацією щодо кіберзагроз, питання довіри, етичні аспекти співпраці та баланс між комерційною та державною безпекою. Основний висновок полягає в тому, що ефективна кібероборона у сучасних державах фактично неможлива без

інституціоналізованого партнерства з бізнесом, однак таке партнерство має ґрунтуватися на прозорих правилах доступу до інформації та розмежуванні повноважень. Таким чином, зарубіжний дискурс демонструє поступовий перехід від військово-центрованої моделі СІМІС до мережевої екосистеми кіберстійкості.

Українські дослідження присвячені правовим та організаційним засадам цивільно-військового співробітництва в оборонному секторі. Зокрема, у працях [73; 74] аналізується нормативне забезпечення ЦВС у діяльності Збройних Сил України, питання імплементації стандартів Альянсу, інституціоналізація СІМІС у національній оборонній політиці. Предмет дослідження тут здебільшого зосереджений на класичному вимірі ЦВС – взаємодії військових з органами влади та населенням у зоні операцій. Ключовий висновок українських авторів полягає в тому, що ЦВС стало необхідним елементом демократичного цивільного контролю та стратегічних комунікацій, проте його правове регулювання ще потребує систематизації.

Інша група українських праць стосується безпосередньо кібербезпеки та гібридних загроз. У роботах [58; 74; 122] досліджується адміністративно-правова модель кіберзахисту, гібридний характер кібератак та необхідність міжсекторальної взаємодії. Предметом аналізу є координація суб'єктів сектору безпеки і оборони, роль державних органів у забезпеченні кіберстійкості, а також взаємодія з приватним сектором. Ключовий висновок цієї групи досліджень полягає в тому, що українська система кібербезпеки має мережевий характер і вже фактично функціонує як інтегрована модель співпраці держави, військових структур та бізнесу. Однак термінологічне поєднання цієї моделі з концепцією цивільно-військового співробітництва залишається недостатньо визначеним.

Сукупний аналіз дозволяє констатувати, що зарубіжні автори переважно рухаються від класичної військової моделі СІМІС до розширеної концепції кіберекосистеми, де ключову роль відіграють приватні суб'єкти та механізми обміну інформацією. Українські дослідники, водночас, розвивають дві

паралельні лінії: нормативно-правову концепцію цивільно-військового співробітництва в оборонній сфері та адміністративно-правову модель кібербезпеки як системи міжвідомчої взаємодії. Перетин цих двох ліній лише починає формуватися.

Отже, проблема інтеграції державно-приватного партнерства, міжсекторальної взаємодії та координації суб'єктів сектору безпеки і оборони в єдину концепцію цивільно-військового співробітництва у кіберпросторі є актуальною, але недостатньо систематизованою. Дослідження демонструють наявність окремих теоретичних і прикладних напрацювань, проте відсутня комплексна правова модель, яка б поєднувала класичне ЦВС із сучасною архітектурою кіберстійкості держави. Саме ця прогалина створює підґрунтя для подальших теоретико-правових узагальнень і концептуалізації «Cyber-SIMIS» як самостійного напрямку дослідження.

Враховуючи зазначене, виникає потреба переходу від фрагментарного аналізу окремих блоків – державно-приватного партнерства, міжсекторальної взаємодії та координації суб'єктів сектору безпеки і оборони – до осмислення їх у межах єдиної концепції військово-цивільного співробітництва як структуроутворюючого чинника кіберстійкості. Якщо у класичній моделі SIMIS взаємодія спрямована на досягнення військової операційної переваги, то в умовах гібридної війни та тоталізації кіберпростору вона набуває стратегічного значення для стійкості всієї державної системи.

Таким чином, подальший аналіз зосереджується на з'ясуванні того, яким чином цивільно-військове співробітництво трансформується з інструмента підтримки військових завдань у механізм формування національної системи кіберстійкості; які елементи цієї взаємодії вже інституціоналізовані; які потребують нормативного закріплення; та як інтеграція військового й цивільного компонентів впливає на здатність держави протидіяти комплексним кіберзагрозам.

У дослідженнях з цивільно-військового співробітництва підкреслюється, що класична концепція SIMIS безпосередньо пов'язана з

операційними задачами збройних сил, але одночасно є важливою для забезпечення національної безпеки в ширшому розумінні (у тому числі в умовах гібридних загроз і кібератак) як складова загальної стійкості суспільства та держави [151; 172; 314; 352; 360]. В українському контексті, як зазначає низка авторів [73; 74; 116], ЦВС виступає ключовим інструментом інтеграції зусиль військових структур, державних органів та громадянського суспільства для реагування на кризові ситуації й гібридні загрози. Зокрема, механізм державного регулювання цивільно-військового співробітництва розглядається як важливий компонент забезпечення національної безпеки в умовах змін воєнно-політичної обстановки, що передбачає адаптацію міжнародного досвіду, насамперед стандартів країн-членів НАТО, до українських реалій з метою підвищення ефективності взаємодії (що підтверджується як практичним досвідом, так і відповідними науковими висновками).

Водночас, аргументація щодо важливості інтеграції військового та цивільного компонентів у забезпеченні кіберстійкості знаходить підтвердження у літературі [13; 122], що досліджує національні системи кібербезпеки. Зокрема, сучасні наукові праці з кібербезпеки підкреслюють [13; 58], що система національної кібербезпеки повинна бути гібридною, мережевою та включати багатьох учасників – державних, військових, приватних і громадських, що дозволяє ефективно реагувати на динамічні загрози кіберпростору. У цьому контексті цивільно-військове співробітництво набуває функціонального значення не як ізольована координаційна операція, а як організаційно-методологічний каркас, що забезпечує оперативний і стратегічний взаємозв'язок між різними складовими національної системи кіберстійкості.

З точки зору національної кіберстійкості важливим є розуміння того, що стратегічна стійкість держави визначається не лише боєздатністю збройних сил, але й здатністю цивільної складової суспільства адаптуватися й ефективно функціонувати під тиском гібридних викликів, включно з

кіберзагрозами. Ці тези підсилюють думку, що ЦВС має бути розглянутий як елемент національної архітектури кіберстійкості, який об'єднує різні рівні управління – від забезпечення безпеки критичної інфраструктури до взаємодії з приватним сектором і громадянським суспільством в умовах кризових викликів.

Міжнародні підходи до кіберстійкості, що вивчають роль багатосуб'єктності та інтеграції технічних знань із громадянським внеском до формування політик кібербезпеки, також підкреслюють потребу в системних механізмах інтегрованого планування і співпраці [393]. Це означає, що сам факт взаємодії між державою та приватними суб'єктами у кіберсфері не може бути ситуативним, він повинен бути частиною стратегічної архітектури, де ЦВС виконує роль «містка» між сектором безпеки і цивільними партнерами, посилюючи стійкість національної кіберінфраструктури.

Таким чином, перехід до аналізу ЦВС як системоутворюючого елементу національної архітектури кіберстійкості ґрунтується на трьох принципах: по-перше, ЦВС має виконувати стратегічну функцію інтеграції суб'єктів сектору безпеки і цивільних партнерів у контексті кіберзагроз; по-друге, він повинен бути частиною нормативно закріпленої системи кібербезпеки, що включає як державні органи, так і приватні суб'єкти та громадські інституції; по-третє, його роль не обмежується оперативною координацією, а включає побудову механізмів забезпечення національної стійкості через спільне планування, обмін інформацією й адаптацію до мінливих загроз кіберпростору.

Організаційний вимір ЦВС у національній системі кіберстійкості визначає, як суб'єкти сектору безпеки й оборони, приватні компанії та громадські організації взаємодіють у рамках координаційних механізмів та спільних операцій. В Україні центральною структурою для забезпечення координації ЦВС є Національний координаційний центр кібербезпеки (НКЦК) при Раді національної безпеки і оборони України, який виконує роль стратегічного і оперативного вузла інтеграції державних і приватних ресурсів [73].

Обґрунтування ролі Національного координаційного центру кібербезпеки як стратегічного хабу базується на необхідності подолання відомчої розрізненості та створення єдиного операційного простору. Як зазначається у наукових публікаціях щодо стратегічних цілей протидії кіберзлочинності, саме відсутність ефективної горизонтальної взаємодії часто стає «вузьким місцем», яким користується агресор для проведення багатовекторних атак [23; 24; 30].

Функціональна архітектура координації у сфері кібербезпеки, закріплена саме Указом Президента України №242/2016 «Про Національний координаційний центр кібербезпеки» [103], має системний характер і передбачає взаємодію ключових інституцій сектору безпеки та оборони. Центральним елементом цієї архітектури виступає НКЦК, який функціонує як робочий орган Ради національної безпеки і оборони України. Його завдання полягають у здійсненні стратегічного аналізу стану кіберзахисту, прогнозуванні та виявленні потенційних загроз, узагальненні міжнародного досвіду та розробці концептуальних засад державної політики у сфері кібербезпеки. Таким чином, НКЦК виконує роль інтеграційного вузла, що забезпечує узгодженість дій усіх суб'єктів системи.

У структурі координації важливе місце займає СБУ, яка відповідає за контррозвідувальне та оперативне забезпечення кібербезпеки. Її функції охоплюють протидію кіберзагрозам воєнного характеру, кібершпигунству, кібертероризму та злочинності. СБУ здійснює оперативне реагування на інциденти та взаємодіє з НКЦК у питаннях стратегічного планування і реалізації заходів кіберзахисту, що забезпечує баланс між аналітичною та практичною складовою системи.

Держспецзв'язку виконує функції технічного та нормативного забезпечення кіберзахисту. Вона координує діяльність державних органів у сфері захисту інформаційних ресурсів, розробляє нормативно-правові акти, каталоги заходів та методичні рекомендації, а також забезпечує функціонування державних систем спеціального зв'язку. Її роль полягає у

створенні технічних стандартів та практичній реалізації політики кіберзахисту, що формує основу для узгодженого функціонування всієї системи.

Збройні Сили України відповідають за кібероборону у військовій сфері. Їхні завдання включають протидію кіберзагрозам воєнного характеру, захист військових інформаційних систем та організацію кібероперацій у кризових ситуаціях. Взаємодія із НКЦК та іншими органами забезпечує інтеграцію військових спроможностей у загальну систему кібербезпеки держави, що є критично важливим у сучасних умовах гібридних загроз.

Таким чином, функціональна архітектура координації у сфері кібербезпеки України побудована за принципом багаторівневої взаємодії, де кожен орган виконує власні функції, але їхня діяльність узгоджується через НКЦК. Така модель забезпечує комплексний підхід до кіберзахисту, поєднуючи стратегічний, оперативний, технічний та військовий рівні, що формує цілісну систему кіберстійкості держави.

Таким чином, НКЦК при РНБО України виконує роль «центральної нервової системи» стійкості. Координаційні механізми центру структуруються за трьома основними напрямками: оперативний обмін даними, розподіл повноважень під час кризи та спільний аналіз загрози.

Новизна підходу НКЦК полягає у переході від запитної системи обміну до автоматизованого поширення індикаторів компрометації (IoCs) у реальному часі. НКЦК розробляє та впроваджує протоколи взаємодії, де чітко розмежовано: хто проводить технічне відновлення (CERT-UA), хто здійснює контррозвідувальні заходи (СБУ), а хто проводить атрибуцію та кримінальне розслідування (Кіберполіція). Водночас, регулярні засідання та робочі групи під егідою НКЦК дозволяють формувати цілісне бачення намірів ворога, що значно підвищує рівень предиктивної стійкості [32; 107].

Обґрунтована координація вимагає відмови від узагальненого підходу і побудови цілісних моделей захисту, у яких дані кіберрозвідки інтегруються з технічним моніторингом та реакцією на інциденти. У сучасних наукових

роботах підкреслюється, що інтегрований підхід до забезпечення кібербезпеки дозволяє скоротити час виявлення загроз і підвищити ефективність реагування на них, зменшуючи фрагментарність захисних механізмів та підвищуючи рівень координації між компонентами системи кіберзахисту [16; 418; 419]. У фахових публікаціях щодо кіберстійкості наголошується, що стійкість системи прямо пропорційна швидкості передачі інформації від суб'єкта, який виявив атаку, до суб'єкта, який може її нейтралізувати. Саме в межах НКЦК створюються довірливі канали зв'язку, які дозволяють залучати приватний сектор (наприклад, банківські або телеком-SOC) до єдиного контуру оборони без порушення комерційної таємниці [103; 114, с. 109].

Таким чином, НКЦК є не просто органом влади, а інтелектуально-технологічною платформою. Тут координація пізнається як мистецтво поєднання воєнної потужності, правоохоронної витривалості та наукової глибини. Використання нашого наукового доробку та практичного досвіду дозволяє стверджувати, що Україна створила унікальну модель координації, яка стала світовим взірцем для країн НАТО.

Водночас, цивільно-військове співробітництво у вітчизняному кіберпросторі базується на фундаментальній концепції всеохопної оборони, де межа між суто військовими заходами та цивільними зусиллями стає максимально прозорою для забезпечення життєздатності держави. В умовах повномасштабного вторгнення координація між Силами кібероборони Збройних Сил України та цивільними суб'єктами, насамперед Державною службою спеціального зв'язку та захисту інформації, набула ознак безперервного операційного циклу, що вимагає постійної методологічної підтримки. Як зазначається у наукових публікаціях щодо стратегічного планування, ефективність такого співробітництва прямо залежить від наявності чітких протоколів взаємодії, які дозволяють спільно використовувати обмежені ресурси для захисту об'єктів, що мають критичне значення як для потреб оборони, так і для життєдіяльності цивільного населення [22; 310]. Цей підхід дозволяє повністю усунути дублювання

функцій між відомствами та забезпечити концентрацію інтелектуальних зусиль на найбільш загрозливих напрямках, перетворюючи розрізнені заходи захисту на монолітну систему стримування агресора, що здатна адаптуватися до змін безпосередньо в ході бойових дій.

Враховуючи важливість цієї компоненти у системі ЦВС та формування відповідної системи кіберстійкості, пропонується частину другу статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» доповнити словами:

«...здійснює координацію цивільно-військового співробітництва у сфері кібербезпеки на стратегічному рівні, забезпечуючи інтеграцію спроможностей волонтерських кіберспільнот та приватних технологічних компаній до загальної системи спротиву; ...».

Юридична складова залучення цивільних фахівців до оборонних заходів у кіберпросторі дійсно вимагає детального аналізу правового статусу учасників боротьби, що є предметом численних наукових дискусій. Зокрема, у професійних публікаціях розглядається, як міжнародне гуманітарне право трактує участь «цивільних хакерів» у діях під час конфліктів, та які правові обмеження і ризики це передбачає [185, с. 101]. У наукових працях, присвячених протидії кіберзлочинності та юридичним аспектам інформаційної безпеки, підкреслюється стратегічна важливість легалізації й регламентації діяльності волонтерських ІТ-спільнот у правовому полі. Аналіз сучасних викликів у правовому забезпеченні кібербезпеки України висвітлює ключові правові рамки та нормативні бази, які формують державну політику протидії кіберзагрозам і визначають, кого і як може бути залучено до таких заходів [26; 122].

Також існують роботи з порівняльно-правового аналізу протидії кіберзлочинності, де обговорюються правові механізми, що застосовуються для боротьби з кіберзагрозами, а також виклики, пов'язані з тим, що традиційні правові категорії недостатньо охоплюють специфіку дій у кіберпросторі. Зокрема, вітчизняні фахівці аналітично порівнюють правові

механізми боротьби з кіберзлочинністю в національному й зарубіжному праві, висвітлюють ключові правові виклики та проблеми адаптації традиційних правових категорій до реалій кіберпростору – що прямо підсилює тезу про недостатню адекватність традиційних правових підходів у цифровому середовищі [2]. Ці та інші наукові джерела формують умову для подальшого розвитку правового регулювання участі цивільних фахівців у кібероборони, включно з визначенням меж їх відповідальності, правового статусу та процедурного забезпечення їхньої діяльності в умовах воєнного стану.

Створення чітких правових рамок для такого співробітництва дозволяє державі ефективно використовувати потужний інтелектуальний потенціал приватного сектору, не порушуючи при цьому норм міжнародного гуманітарного права та забезпечуючи належний рівень секретності операцій. Співробітництво в межах таких протоколів здійснюється через захищені вітчизняні платформи, де завдання розподіляються залежно від спеціалізації суб'єктів: від глибокого технічного аналізу шкідливого програмного забезпечення до оперативного моніторингу активності противника у мережевих сегментах. Така синергія забезпечує виняткову гнучкість національної архітектури, оскільки залучені цивільні фахівці часто володіють унікальними інструментами аналізу та знаннями про архітектуру сучасних хмарних систем, які критично доповнюють можливості штатних підрозділів військової розвідки та контррозвідувального захисту.

Окремим стратегічним вектором співпраці є спільне використання методології аналізу відкритих джерел, яка детально розроблена та практично реалізується, зокрема і через діяльність Інституту досліджень кібервійни (ICWR) [348; 349]. Координація розвідувальних та аналітичних зусиль на основі відкритих даних дозволяє військовим та цивільним структурам формувати єдине інформаційне середовище про наміри, фінансові потоки та технічний арсенал ворожих угруповань [31]. Це забезпечує превентивний характер стійкості, коли інформація про підготовку масштабної атаки, здобута цивільними дослідниками шляхом аналізу неструктурованих даних, стає

підставою для негайного приведення військових систем управління та засобів радіоелектронної боротьби у стан підвищеної готовності. Використання спільних стандартів візуалізації та звітності, що базуються на практичному досвіді, зводить до мінімуму час на інтерпретацію критичних даних та суттєво прискорює прийняття управлінських рішень на рівні стратегічного командування, що є життєво важливим у динамічних умовах сучасної війни [349].

Логічним завершенням механізмів цивільно-військової співробітництва виступає інституціоналізація спільних тренувальних центрів та проведення регулярних міжвідомчих навчань, що базуються на реальних кейсах. У навчальних кейсах наголошується, що життєздатність архітектури перевіряється лише в умовах контрольованої кризи, яка імітує реальні деструктивні впливи [348]. Спільні навчання дозволяють не лише відпрацювати технічні протоколи передачі управління критичними мережами у разі ураження основних вузлів, а й вибудувати особистісну довіру між фахівцями різних відомств, що є фундаментом будь-якої успішної координації. Важливо, що в ході такої взаємодії відбувається постійне «перехресне запилення» знаннями: військові фахівці отримують доступ до новітніх комерційних технологій захисту, а цивільний сектор адаптує військові методики забезпечення автономності систем у екстремальних умовах. Таке взаємозбагачення, підкріплене науковими пошуками, перетворює цивільно-військове співробітництво на стійкий еволюційний процес, що робить українську модель кіберстійкості антикрихкою та здатною до самовдосконалення безпосередньо в горнилі конфлікту [105; 106].

Наукове осмислення механізмів координації на галузевому та регіональному рівнях базується на необхідності децентралізації управління стійкістю для забезпечення її живучості в умовах територіально розподілених загроз. В ієрархічній структурі національної системи кібербезпеки галузеві та регіональні вузли виступають проміжними ланками, що забезпечують

адаптацію загальнодержавних стратегій до специфічних потреб конкретних секторів економіки або адміністративних одиниць.

Проблематика захисту критичної інфраструктури та моделювання стійкості складних енергетичних і інформаційних систем ґрунтовно досліджується українськими науковцями, зокрема у працях фахівців Інституту проблем моделювання в енергетиці НАН України [56]. Аналітичні матеріали щодо ризиків централізованої моделі управління кібербезпекою представлені також у дослідженнях Національного інституту стратегічних досліджень [80]. Концентрація координаційних повноважень виключно у центрі створює ризик затримок у реагуванні на локальні інциденти, що відображено у вітчизняних наукових публікаціях з питань управління кібербезпекою та стійкістю критичної інфраструктури. Тому створення галузевих центрів операційної безпеки та вузлів обміну інформацією є обов'язковою умовою для формування «колективного імунітету» галузей, де суб'єкти господарювання можуть ефективно взаємодіяти, мінімізуючи каскадні наслідки від кібератак на суміжні підприємства. Концептуальні засади такої моделі корелюють із положеннями Стратегії кібербезпеки України та аналітичними матеріалами Національного координаційного центру кібербезпеки і Державної служби спеціального зв'язку та захисту інформації України.

Функціонування галузевих вузлів координації, зокрема у таких критичних сферах як енергетика, транспорт та фінанси, вимагає впровадження спеціалізованих протоколів довірливого обміну інформацією. Водночас, у контексті стратегічного планування протидії кіберзлочинності підкреслюється, що успіх координації залежить від балансу між вимогами конфіденційності бізнесу та потребами державної безпеки [310, с. 31].

На практиці це реалізується через створення галузевих команд реагування, які акумулюють дані про аномалії в технологічних мережах та поширюють їх серед усіх учасників сектору без розголошення комерційних таємниць. Як показано у сучасних українських дослідженнях з аналізу гібридних кібератак та методів виявлення загроз, побудова таких підрозділів

із використанням інтелектуальних підходів до фільтрації трафіку та подій значно скорочує час виявлення аномалій і підвищує якість реагування на інциденти в сегментованих мережах [88, с. 84]. Такі галузеві та освітні команди реагування вже формуються в українському освітньому середовищі – зокрема, перша освітня команда з реагування на кіберінциденти (CSIRT-ED) була створена в Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» для підготовки фахівців у реальних умовах кіберзагроз [313]. Це свідчить про практичну реалізацію ідеї інтеграції науково-освітніх структур у процес реагування на інциденти. Така модель дозволяє ідентифікувати вектори атак на ранніх стадіях, коли ураження одного об'єкта стає сигналом для автоматичного посилення захисту на всіх інших вузлах галузі. Це співпадає з концепціями розвитку центрів операцій безпеки (Security Operations Centers, SOC) як ключових елементів національної системи кібербезпеки, які вивчаються українськими дослідниками з акцентом на інтеграцію SOC у загальну систему національної безпеки [114, с. 110]. Це значно підвищує загальний поріг витривалості національної економіки до зовнішніх деструктивних впливів, що відповідає стратегічним положенням Стратегії кібербезпеки України.

Окреме місце у системі регіональної координації посідають наукові установи та аналітичні центри, серед яких ключову роль відіграє Інститут досліджень кібервійни (ICWR) [55], який позиціонує себе інтелектуальним хабом, що забезпечує науковий супровід координаційних процесів. Використання бази ICWR для проведення міжвідомчих тренувань та спільних аналітичних сесій дозволяє фахівцям різних відомств (Кіберполіції, СБУ, регіональних підрозділів Держспецзв'язку) вибудовувати єдину методологічну мову. Це особливо важливо при розслідуванні транскордонних злочинів та координації дій під час ліквідації наслідків атак на регіональному рівні, де залучення наукової спільноти дозволяє використовувати новітні методики атрибуції та аналізу шкідливого коду, що ще не встигли стати

загальноприйнятими стандартами, але вже довели свою ефективність у ході наукових досліджень.

Логіка децентралізованої координації також передбачає активне залучення університетської науки до формування регіональних екосистем стійкості. На нашу думку, заклади вищої освіти мають бути не лише центрами підготовки фахівців, а й активними суб'єктами моніторингу локального кіберпростору.

Створення при університетах студентських команд реагування та їхня інтеграція у регіональні координаційні плани дозволяє створювати додаткові рівні захисту та забезпечувати постійний приплив інноваційних ідей у державний сектор. Наприклад, питання кореляції подій кібербезпеки й управління інцидентами на об'єктах критичної інфраструктури розглядаються українськими дослідниками у статті «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури», де обговорюється значення таких систем як основи для побудови ефективної взаємодії між навчальними, науковими й оперативними підрозділами [17, с. 182]. Також в національному контексті аналізується поняття кіберстійкості критичної інфраструктури, що прямо корелює з потребою академічної участі у моніторингу локальних кіберсередовищ [52].

Таке поєднання академічної глибини, практичного досвіду аналітичних центрів та оперативної потужності державних органів створює гнучку та живучу структуру, здатну витримувати довготривалий тиск агресора за рахунок власної інтелектуальної переваги та децентралізованої природи.

Механізми «колективного імунітету» формують важливий компонент ЦВС у сфері кібербезпеки, що в національній системі кіберстійкості базується на здатності суб'єктів до миттєвої синхронізації захисних заходів після виявлення первинного вектора атаки на будь-який елемент інфраструктури. Координація у цьому контексті розглядається як процес перетворення локального досвіду інциденту на масштабований алгоритм захисту. Теоретичні засади обміну технічною інформацією про загрози проаналізовано

у роботах щодо стандартизації IoC-обміну, зокрема в моделі STIX/TAXII [343]. Як підкреслюється в наукових дослідженнях стратегічного планування кіберзахисту, стійкість держави значною мірою вимірюється швидкістю поширення індикаторів компрометації між національними CSIRT (Computer Security Incident Response Team – Команда реагування на інциденти комп’ютерної безпеки) та приватними центрами моніторингу безпеки. Правові та організаційні механізми такого обміну закріплено у Директиві European Parliament та Council of the European Union 2022/2555 (NIS2 Directive), яка прямо наголошує на обов’язку оперативного обміну інформацією про кіберінциденти між державними та приватними структурами як ключовому елементі загальноєвропейської кіберстійкості [223]. Водночас, NIST визначає кіберстійкість як здатність системи швидко адаптуватися до нових загроз через безперервний обмін знаннями, оновлення політик фільтрації та автоматизовану корекцію захисних механізмів [219]. Така взаємодія дозволяє за лічені хвилини вибудувати ешелоновану оборону по всій країні, роблячи повторне використання тієї ж тактики ворогом неефективним. Цей механізм перетворює національну систему на самонавчальний організм, де кожен успішний або відбитий напад лише посилює загальну архітектуру безпеки за рахунок автоматизованого обміну знаннями та швидкої адаптації правил фільтрації трафіку на магістральних рівнях.

Критично важливим аспектом координації є забезпечення невідворотності покарання за кіберзлочини через єдині підходи до роботи з електронними доказами. Наукова суб’єктність у цьому процесі реалізується через розроблені тренінги та методичні посібники для суддів і прокурорів. Спільна діяльність правоохоронних органів, аналітичних центрів, таких як Інститут досліджень кібервійни (ICWR), та органів правосуддя дозволяє сформувати єдиний стандарт допустимості цифрових доказів, отриманих у ході складних транскордонних операцій. У багатьох працях наголошується, що без належної координації на етапі вилучення та аналізу даних (особливо у хмарних середовищах) доказова база може бути легко нівельована стороною

захисту, що підриває довіру до всієї системи кіберюстиції. Тому розбудова міжвідомчих протоколів фіксації кібератак є не лише технічним завданням, а формою інституційної стійкості, що забезпечує правову стабільність держави [14; 22; 76; 86; 136].

Окремим високотехнологічним напрямом координації є взаємодія органів влади при дослідженні віртуальних активів та блокчейн-мереж, що використовуються агресором для фінансування кібердиверсій. Спираючись на напрацювання щодо аналізу інструментів криміналістичної експертизи блокчейну, можна стверджувати, що координація між Кіберполіцією, СБУ та Держфінмоніторингом дозволяє створювати цілісну картину фінансової підтримки хакерських угруповань. Використання спеціалізованого програмного забезпечення для відстеження транзакцій у поєднанні з методами аналізу відкритих джерел (OSINT) дає змогу суб'єктам не лише ідентифікувати виконавців, а й блокувати цифрові гаманці, що використовуються для виплати винагород або закупівлі серверних потужностей для атак. Такий рівень координації забезпечує «економічну стійкість» кіберпростору, оскільки робить проведення атак проти України фінансово обтяжливим та ризикованим для замовників, одночасно створюючи прецеденти для міжнародних санкцій на основі верифікованих блокчейн-даних [162; 349].

Завершальним етапом механізму координації є трансформація результатів розслідувань та аналізу інцидентів у стратегічні зміни нормативно-правової бази та навчальні програми. Координація зусиль науковців, практиків та законодавців під егідою НКЦК дозволяє Україні бути не лише майданчиком для випробування нових технологій захисту, а й лідером у формуванні глобальних стандартів кібердипломатії та міжнародного права. Таким чином, поєднання технічної синхронізації «колективного імунітету» з юридичною точністю роботи з доказами створює завершений контур національної кіберстійкості, де кожен суб'єкт діє у синергії задля спільної мети – стратегічної безпеки та правового суверенітету України [107].

Важливою складовою організаційної моделі є інтеграція приватного сектору через механізми державно-приватного партнерства. Це забезпечує участь кіберкомпаній у спільних навчаннях, обмін інформацією щодо кіберзагроз, стандартизоване реагування на кіберінциденти та аналітичну підтримку державних органів. Такий підхід дозволяє поєднати ресурси та експертизу державних і приватних структур і підвищити адаптивність системи до швидкозмінного середовища [172].

Наукове переосмислення природи державно-приватного партнерства (ДПП) в умовах перманентних гібридних загроз вимагає відходу від застарілого розуміння ДПП як суто інвестиційного або концесійного механізму. В архітектурі національної кіберстійкості України партнерство між державним сектором та приватним бізнесом пізнається як стратегічний альянс, де приватний сектор надає технологічну гнучкість, інноваційний капітал та оперативну швидкість, а держава забезпечує правову легітимізацію, розвідувальні дані та загальнонаціональну координацію. Як обґрунтовано зазначається, у контексті стратегічного управління, ефективність такого партнерства прямо корелює з рівнем інституційної довіри, яка в умовах війни трансформувалася з моральної категорії у критичний безпековий ресурс [223; 310]. Юридичне закріплення форм такої взаємодії у Законі України «Про критичну інфраструктуру» [102] дозволяє створити прогнозоване середовище, де інвестиції бізнесу у власну стійкість розглядаються не як додаткове фінансове обтяження, а як необхідний внесок у загальнодержавний контур безпеки. Це особливо актуально для операторів енергетичного, фінансового та телекомунікаційного секторів, де компрометація одного приватного вузла може за принципом доміно спричинити системний колапс державних сервісів, що робить ДПП імперативним елементом виживання національної екосистеми [107].

Трансформація парадигми ДПП у кіберсфері передбачає перехід від моделі «держава-регулятор», що базується на примусовому контролі та санкціях, до моделі «держава-партнер», де основний акцент зміщується на

спільне управління ризиками. У нашому доробку підкреслюється, що класичні бюрократичні механізми не встигають за динамікою загроз, тому держава має делегувати частину моніторингових та аналітичних функцій приватному сектору, залишаючи за собою роль стратегічного арбітра [25, с. 29]. Правовий аналіз поточної нормативної бази свідчить про необхідність впровадження так званих «регуляторних пісочниць», де приватні компанії могли б тестувати новітні засоби захисту КІІ у тісній взаємодії з державними CERT, що дозволило б оперативно виявляти вразливості архітектури до їхньої експлуатації противником. Такий підхід забезпечує правову гнучкість, коли норми закону не гальмують технологічний розвиток, а створюють для нього безпечний коридор, що є життєво важливим для розбудови національної системи кіберстійкості в умовах воєнного стану.

Економічний інструментарій стимулювання стійкості є фундаментом, без якого ДПП залишатиметься лише декларативним наміром. Науково обґрунтована модель партнерства має включати механізми страхування кіберризиків, де держава виступає перестраховальником для об'єктів критичної інфраструктури першої та другої категорій. Водночас, доцільним є робити акценти і на необхідності надання податкових преференцій та митних пільг для компаній, які переходять на вітчизняні програмно-апаратні комплекси захисту інформації. Це не лише знижує імпортозалежність у чутливих сферах, а й стимулює розвиток національного ринку кібербезпеки. Більше того, розробка державних грантових програм для підтримки стартапів, що спеціалізуються на блокчейн-форензиці та аналізі відкритих джерел (OSINT), дозволяє Україні зберігати інтелектуальне лідерство. Спільне фінансування наукових розробок на базі Інституту досліджень кібервійни (ICWR) із залученням приватного капіталу створює синергію, яка перетворює наукові гіпотези на працюючі інструменти національної оборони [349].

Обґрунтування стратегічних напрямів удосконалення цивільно-військового співробітництва у кіберсфері потребує впровадження інноваційних інституційних інструментів, серед яких ключове місце

посідають створення *цивільного кіберрезерву* та детермінація спеціального правового режиму *«регуляторних пісочниць»*. Зазначені механізми покликані вирішити фундаментальну суперечність між динамічною природою гібридних загроз та статичністю класичних правових інститутів.

Концептуальна модель цивільного кіберрезерву розглядається як форма «гнучкої мобілізації» інтелектуального капіталу, що не потребує обов'язкової комбатантизації фахівця за класичними ознаками (набуття статусу військовослужбовця). Це дозволяє зберегти залученість висококваліфікованих кадрів у цивільному секторі економіки, забезпечуючи при цьому їхню легітимну участь у заходах з кібероборони як «цивільних асистентів». Правова детермінація цього статусу дозволяє розв'язати дилему Женевських конвенцій у цифровому домені, оскільки діяльність таких осіб проти військових об'єктів агресора визнається законною на рівні національного законодавства («виконання службового обов'язку»), що усуває ризики їхнього кримінального переслідування за ст. 361 КК України.

Паралельно з цим, ефективність Cyber-CIMIC залежить від впровадження режиму «регуляторних пісочниць» – експериментальних правових просторів, де для приватних суб'єктів, інтегрованих у систему ЦВС, діють особливі умови регулювання. Функціонування таких зон передбачає надання приватним операторам доступу до державних баз індикаторів компрометації (IoC) та звільнення їх від юридичної відповідальності за можливі технічні збої у цивільній інфраструктурі, що виникли внаслідок відбиття складних кібератак або тестування новітніх засобів захисту.

Таким чином, синергія цивільного кіберрезерву та регуляторних пісочниць формує цілісну архітектуру, в якій ресурсний потенціал громадянського суспільства трансформується у легітимну, керовану та технологічно спроможну силу. Це забезпечує перехід від ситуативної волонтерської допомоги до системної державної політики, що гарантує суверенітет України в кіберпросторі та повну сумісність із євроатлантичними стандартами колективної безпеки.

З огляду на зазначене, пропонується у Законі України «Про основні засади забезпечення кібербезпеки України» доповнити статтю 8:

частиною восьмою: «Суб'єкти приватного сектору, що залучаються до заходів цивільно-військового співробітництва, отримують право на використання спеціальних правових режимів («регуляторних пісочниць») за умови забезпечення автоматизованого обміну даними про кіберінциденти з державними центрами реагування (CERT-UA) та дотримання стандартів сумісності НАТО»;

а також частиною девятою: «Запровадити інститут добровільного кіберрезерву як форми реалізації цивільно-військового співробітництва, що передбачає залучення цивільних фахівців на договірній основі до виконання завдань з кібероборони без обов'язкового набуття статусу військовослужбовця, із визначенням меж їхньої юридичної відповідальності та соціального захисту».

Важливим вектором розвитку правових засад ДПП є імплементація логіки Директиви ЄС 2022/2555 (NIS2) в українське правове поле. Адаптація європейських стандартів передбачає запровадження персональної відповідальності вищого керівництва приватних компаній за стан кіберстійкості, що радикально змінює ставлення бізнесу до безпекових бюджетів [9; 223]. У межах ДПП держава бере на себе зобов'язання забезпечувати бізнес предиктивними даними про загрози, а приватний сектор, у свою чергу, гарантує дотримання суворих регламентів безпеки ланцюгів постачання. Це створює цілісну екосистему, де безпека кожного окремого суб'єкта є запорукою стабільності всієї держави. Координація зусиль через спільні платформи дозволяє вибудувати рівноправний діалог, де держава бачить у бізнесі не об'єкт перевірок, а повноцінного комбатанта на цифровому фронті, чия витривалість є фундаментом загальнонаціональної життєздатності [310, с. 30].

Таким чином, ДПП розкривається як складна соціотехнічна та юридична конструкція. Сьогодні Україна формує унікальну модель партнерства, де

правові норми, економічні стимули та наукова думка поєднані заради єдиної мети – перетворення критичної інфраструктури на нездоланий бастион. Це закладає основу для подальшого аналізу технологічного ядра цієї взаємодії.

Технологічна конвергенція державних та приватних спроможностей у сфері кібербезпеки знаходить своє найвище втілення у створенні спільних операційних центрів та єдиних платформ обміну даними про загрози. Науковий зміст цього процесу полягає у переході від розрізнених систем моніторингу до інтегрованого інформаційного середовища, де дані про аномальну активність у мережах приватних операторів миттєво стають основою для оновлення правил захисту на національному рівні.

Ключовим елементом екосистеми довіри у межах державно-приватного партнерства є імплементація протоколів світлофорного маркування інформації (Traffic Light Protocol), що дозволяє чітко регламентувати рівень доступу до даних та умови їхнього подальшого поширення. У різних працях, що стосуються стратегічного планування, наголошується, що саме відсутність гарантій конфіденційності часто стримує приватний сектор від повноцінної співпраці з державними органами [406]. Створення захищених каналів зв'язку між приватними центрами операційної безпеки (SOC) та державними командами реагування (CERT) дозволяє вибудувати дворівневу систему захисту. На першому рівні відбувається автоматизований обмін технічними метаданими, а на другому – глибокий експертний аналіз тактик та технік зломисників. Це дозволяє державним регуляторам бачити цілісну картину загроз у реальному часі, а приватному бізнесу отримувати випереджальну розвідувальну інформацію від спецслужб, що суттєво знижує витрати на локальну безпеку та підвищує загальну витривалість критичної інфраструктури [114, с. 110; 196].

Практична реалізація технологічного партнерства вимагає також створення спільних ситуаційних кімнат для відпрацювання сценаріїв масштабних кіберкриз. У ситуаціях, коли атака спрямована на декілька секторів одночасно (наприклад, енергетику та телеком), координація через

єдині технологічні платформи дозволяє централізовано перерозподіляти обчислювальні ресурси та резервувати критичні канали зв'язку. Спільна робота технічних фахівців держави та бізнесу в єдиному операційному середовищі перетворює державно-приватне партнерство на життєздатний організм, який не просто захищається, а активно еволюціонує, інтегруючи кожен інцидент у нову, більш досконалу архітектуру національної безпеки.

Науково-аналітичний супровід виступає інтелектуальним фундаментом державно-приватного партнерства, забезпечуючи перетворення сирих даних про кіберзагрози на стратегічну інформацію, необхідну для прийняття управлінських рішень. У системі національної кіберстійкості особливе місце посідають наукові установи та аналітичні центри, серед яких важливу роль відіграє Інститут досліджень кібервійни (ICWR). Інститут функціонує як місток між державними регуляторами та операторами критичної інфраструктури, забезпечуючи спільну розробку методологій захисту. Як обґрунтовано у працях, присвячених стратегічному плануванню, ефективність партнерства залежить від наявності єдиної наукової мови та стандартів аналізу, що дозволяють суб'єктам з різними організаційними культурами діяти як єдиний механізм. Така наукова синергія дозволяє не просто реагувати на інциденти, а прогнозувати вектори майбутніх атак на основі глибокого вивчення тактик і процедур противника, що робить національну систему кіберстійкості проактивною та інтелектуально переважною [71; 72; 132].

В умовах гібридної агресії приватний сектор часто першим стикається з новими методами інформаційно-психологічного та технічного впливу, зафіксованими у відкритих мережах. Використання спільних стандартів OSINT-аналізу дозволяє державі та бізнесу спільно моніторити даркнет, форуми зловмисників та соціальні мережі для виявлення ознак підготовки атак на критичну інфраструктуру. Це створює умови для формування «спільного операційного середовища», де інформація, отримана приватними дослідниками, негайно верифікується державними розвідувальними органами та трансформується у конкретні рекомендації щодо посилення захисту. Такий

підхід значно розширює можливості держави за рахунок залучення аналітичного потенціалу комерційних компаній, одночасно підвищуючи рівень обізнаності бізнесу про актуальні загрози національного масштабу [349].

Окремим стратегічним напрямом аналітичного партнерства є спільний моніторинг блокчейн-мереж та віртуальних активів, що використовуються для фінансування кіберзлочинності та підривної діяльності. Взаємодія між державними правоохоронними органами та приватними фінансовими установами дозволяє створити ефективний заслон на шляху легалізації доходів, отриманих злочинним шляхом. Координація тут здійснюється через спільне використання інструментів форензики віртуальних активів, що дозволяє відстежувати ланцюжки транзакцій агресора та ідентифікувати кінцевих бенефіціарів атак. У циклі статей наголошується, що саме в межах державно-приватного партнерства стає можливим поєднання глибокого технічного аналізу блокчейн-протоколів, який проводять приватні лабораторії, з процесуальними можливостями держави щодо накладення арешту на активи та притягнення винних до відповідальності. Така координація робить кібератаки проти України економічно недоцільними та створює правову базу для міжнародного переслідування замовників деструктивних дій [78; 82, с. 159].

Логічним завершенням аналітичної складової партнерства є створення науково-навчальних хабів для підготовки кадрів вищої ланки (C-level) та фахівців з кібербезпеки обох секторів. Подібна модель взаємодії науки, держави й бізнесу відповідає концепції багатостороннього управління кібербезпекою, що детально обґрунтована у документах та аналітичних матеріалах European Union Agency for Cybersecurity (ENISA), зокрема у звітах щодо розвитку кібернавичок та стратегічного лідерства у сфері кібербезпеки [214]. Використання результатів наукової діяльності для розробки навчальних програм відповідає також підходам, викладеним у рамках NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), де

наголошується на необхідності інтеграції академічних досліджень у підготовку керівників стратегічного рівня [392]. Крім того, у доповідях World Economic Forum підкреслюється, що формування довіри між державними структурами та великим бізнесом через спільні освітні ініціативи є ключовим елементом глобальної кіберстійкості [257]. Таким чином, науково-аналітичний супровід у межах державно-приватного партнерства трансформує національну систему кіберстійкості у високотехнологічну інтелектуальну мережу, що відповідає сучасним міжнародним підходам до розвитку стратегічного лідерства та координації у сфері кібербезпеки.

Використання результатів наукової діяльності для розробки навчальних програм дозволяє сформувати нову генерацію управлінців, які однаково добре розуміють як бізнес-процеси, так і вимоги національної безпеки. Спільні тренінги, що проводяться на базі партнерських університетів, сприяють вибудовуванню особистісних зв'язків та професійної довіри між офіцерами спецслужб та технічними директорами великих корпорацій. Це забезпечує життєздатність системи у критичні моменти, коли швидкість координації залежить від злагодженості дій конкретних людей. Таким чином, науково-аналітичний супровід у межах державно-приватного партнерства перетворює національну систему кіберстійкості на високотехнологічну інтелектуальну мережу, здатну не лише витримувати удари, а й диктувати власні правила безпеки у глобальному цифровому просторі.

Міжнародний вимір державно-приватного партнерства в архітектурі кіберстійкості України пізнається як система глобальних технологічних альянсів, що забезпечують доступ до передових інструментів захисту та обробки великих даних у масштабах, недоступних для окремої держави. В умовах повномасштабної кібервійни стратегічне партнерство з такими гігантами, як Microsoft, Google та Amazon Web Services (AWS), стало вирішальним фактором збереження цілісності державних інформаційних ресурсів. Як обґрунтовано у наукових статтях щодо стратегічного планування, винесення критичних державних реєстрів у «хмарні» середовища

міжнародних провайдерів дозволило забезпечити їхню географічну та технічну стійкість до фізичних і цифрових атак агресора [220]. Такий рівень ДПП виходить за межі класичних контрактів на закупівлю послуг, трансформуючись у спільне оперативне чергування, де інженери світових корпорацій та фахівці українських CERT працюють як єдина команда реагування. Це дозволяє Україні використовувати ресурси глобального моніторингу, що виявляють аномалії по всьому світу, для захисту національного сегменту мережі інтернет, створюючи неперевершений рівень ситуаційної обізнаності [70; 91, с. 237; 123].

Важливим аспектом міжнародного партнерства є роль України як глобального донора унікального безпекового досвіду. Сьогодні вітчизняні методики відсічі кіберагресії інтегруються у стандарти стійкості країн НАТО та Європейського Союзу. Спільні проекти з міжнародними організаціями (ENISA, FIRST) дозволяють Україні експортувати власні напрацювання, які визнаються кращими світовими практиками [317; 406; 407]. Це створює умови для зворотного партнерства: міжнародні технологічні компанії інвестують у розвиток українських аналітичних центрів, отримуючи натомість верифіковані дані про новітні тактики зловмисників. Таким чином, ДПП набуває ознак інтелектуального обміну, де українська наукова думка стає фундаментом для розробки глобальних стандартів безпеки нового покоління, що зміцнює міжнародний авторитет України як провідної кібердержави.

Стратегічні альянси у межах ДПП також включають участь України у транскордонних ініціативах з кіберстійкості, що реалізуються через програми цифрової конвергенції з ЄС. Адаптація європейських вимог до захисту ланцюгів постачання дозволяє українському ІТ-бізнесу ставати повноправним учасником європейського ринку безпеки. У межах таких проектів створюються спільні центри обміну інформацією (ISACs), що об'єднують енергетичні та фінансові компанії України та країн-сусідів. Це забезпечує регіональну стійкість, коли атака на інфраструктуру в одній країні

автоматично призводить до посилення захисту в іншій за рахунок спільних технологічних платформ [409].

Дослідження ефективності існуючих координаційних механізмів свідчать про позитивний вплив багаторівневої моделі ЦВС на загальну кіберстійкість. Зокрема, операційні центри забезпечують своєчасне виявлення і нейтралізацію кібератак, сприяють стандартизації процедур взаємодії та підвищують рівень готовності всіх суб'єктів до кризових ситуацій [11, с. 155]. Водночас аналіз практики показує, що існують прогалини у формалізації процедур залучення громадянського суспільства та стандартизації обміну інформацією з приватними провайдерами кіберзахисту, що обмежує потенціал системи у кризових умовах.

Оцінка ефективності ЦВС передбачає аналіз його здатності забезпечувати інтеграцію державного, приватного та громадського секторів у єдину систему кіберстійкості, оперативне реагування на інциденти та підтримку стратегічного прогнозування загроз. Критерії оцінювання включають інституційну узгодженість, чіткість розподілу повноважень, стандартизацію процедур обміну інформацією, швидкість реагування на кіберзагрози та адаптивність до гібридних викликів [11; 172].

Аналіз існуючих механізмів ЦВС в Україні показує, що координаційні центри та міжвідомчі групи дозволяють своєчасно виявляти та нейтралізувати кібератаки, підвищують рівень взаємодії між суб'єктами та сприяють стандартизації процедур реагування. Водночас виявлено прогалини у формалізації участі приватного сектору та громадянського суспільства, недостатню стандартизацію протоколів обміну розвідувальною інформацією щодо кіберзагроз та обмежену аналітичну підтримку на стратегічному рівні [92, с. 114].

Ці спостереження свідчать, що ефективність ЦВС визначається не лише наявністю інституційних елементів, а й рівнем їх інтеграції, узгодженістю процедур та здатністю адаптуватися до нових загроз, що робить оцінку

ефективності критичною для розробки оптимальних моделей інтеграції ЦВС у національну систему кіберстійкості.

Таким чином, організаційно-структурна модель ЦВС в Україні поєднує державний і приватний сектори та закладає основу для формування стійкої кіберархітектури. Водночас для підвищення ефективності необхідне подальше вдосконалення координаційних процедур, стандартизація протоколів обміну інформацією та розширення участі громадянського суспільства в системі кіберстійкості.

Розробка оптимальної моделі ЦВС передбачає комплексну інтеграцію нормативного, організаційного та технологічного вимірів. На нормативному рівні це включає розробку чітких правових механізмів взаємодії державних органів, військових підрозділів, приватного сектору та громадських організацій, стандартизацію процедур обміну інформацією та забезпечення правової передбачуваності дій під час кібератак [9].

Організаційний вимір передбачає багаторівневу мережеву структуру, яка поєднує стратегічне планування, тактичне моделювання сценаріїв та оперативне реагування на інциденти. Важливою складовою є інтеграція приватного сектору через механізми державно-приватного партнерства та участь громадянського суспільства у моніторингу і реагуванні на загрози [172].

Технологічний аспект моделі включає впровадження сучасних платформ для централізованого моніторингу кіберзагроз, обміну розвідувальною інформацією щодо кіберзагроз та симуляційних вправ, що дозволяє уніфікувати процедури обміну інформацією, підвищити швидкість реагування та забезпечити аналітичну підтримку прийняття рішень на стратегічному і операційному рівнях [92, с. 113].

Оптимальна модель ЦВС передбачає динамічну взаємодію між суб'єктами, стандартизовані протоколи обміну даними, узгоджені механізми оцінки ризиків та ефективності реагування, а також регулярне проведення навчань і симуляційних вправ. Така інтегрована структура забезпечує стійку

кіберархітектуру держави, здатну до швидкого реагування на складні гібридні загрози, що поєднують кібернапади, фізичні та інформаційні компоненти [11, с.156].

Розгортаючи законодавчу перспективу в Україні не у формі декларативного закріплення термінів, а як системну модернізацію кібербезпекової архітектури із впровадженням елементів «Cyber-CIMIC» у чинну нормативну модель, передусім логічним є внесення змін до Закон України «Про основні засади забезпечення кібербезпеки України». Перш за все, це стосується вже визначених у розділі новацій щодо терміну «Cyber-CIMIC» та повноважень НКЦК у контексті координації ЦВС.

На сьогодні закон фіксує суб'єктний склад системи та принципи координації, але не виокремлює цивільно-військову взаємодію як самостійний принцип. Доцільно доповнити статтю, що визначає принципи державної політики у сфері кібербезпеки, положенням про «принцип інтегрованого цивільно-військового співробітництва у кіберпросторі», під яким розуміти системну взаємодію військових формувань, суб'єктів сектору безпеки і оборони, органів державної влади, операторів критичної інфраструктури та приватного сектору з метою забезпечення кіберстійкості держави.

Одночасно запровадження інституту цивільного кіберрезерву та регуляторних пісочниць дозволяє трансформувати ресурсний потенціал громадянського суспільства у контрольовану та легітимну силу. Це створює правовий «запобіжник», який захищає фахівця від кримінального переслідування, а державу – від хаотичних дій волонтерів, переводячи мережеву кібероборону в русло системного цивільно-військового співробітництва.

Другим напрямом є розроблення спеціального підзаконного акту – наприклад, «Положення про цивільно-військову взаємодію у сфері кібербезпеки», яке могло б бути затверджене рішенням Рада національної безпеки і оборони України та введене в дію указом Президента. У цьому документі варто визначити:

правові режими взаємодії (мирний час, кризова ситуація, воєнний стан);
механізми обміну інформацією між військовими структурами та приватними операторами;
процедури спільного реагування на масштабні кіберінциденти;
гарантії захисту комерційної та службової інформації;
питання відповідальності та координації.

Третій напрям стосується інституційної інтеграції. На базі НКЦК доцільно передбачити створення постійного механізму цивільно-військової кіберкоординації з представництвом Збройних Сил України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, а також операторів критичної інфраструктури та профільних асоціацій ІТ-бізнесу. Це дозволило б інституціоналізувати ту мережеву модель взаємодії, яка фактично вже існує.

Окремої уваги потребує гармонізація із стандартами НАТО. Імплементация принципів СІМІС у кіберпросторі може бути здійснена не шляхом прямого копіювання доктрин, а через адаптацію процедур планування, управління кризами та міжсекторальної координації. Важливо, щоб українська модель зберегла свою мережеву гнучкість, яка довела ефективність у період повномасштабної війни, але водночас набула нормативної визначеності.

У підсумку можна сформулювати стратегічний висновок. Українська кібербезпекова архітектура фактично вже функціонує за логікою розширеного цивільно-військового співробітництва. Проте відсутність чіткої правової артикуляції цієї моделі створює ризики фрагментації відповідальності та обмежує можливості її довгострокової інституціоналізації. Законодавче закріплення «Cyber-SIMIS» як складової системи кіберстійкості дозволить забезпечити правову визначеність, підвищити рівень координації та посилити інтеграцію України у євроатлантичний безпековий простір.

Водночас, структурна інтеграція цивільно-військового співробітництва у національну систему кіберстійкості передбачає багаторівневу взаємодію нормативних, організаційних і операційних елементів, які спільно формують цілісну архітектуру безпеки держави. З нормативної точки зору ключовим є забезпечення законодавчої та стратегічної бази, яка чітко регламентує повноваження державних органів, суб'єктів сектору безпеки і оборони, приватного сектору та громадянського суспільства в умовах кіберзагроз. У цьому контексті важливими є положення Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України та інших нормативних актів, що визначають порядок взаємодії державних структур із приватними організаціями, зокрема в питаннях обміну інформацією про інциденти та координації заходів реагування [92, с. 113]. Така формалізація має забезпечити юридичну передбачуваність, уникнення конфлікту повноважень і прозору відповідальність у разі кіберінцидентів, а також інтеграцію з міжнародними стандартами та практиками, зокрема з досвідом НАТО [172].

Організаційний вимір інтеграції ЦВС полягає у формуванні системи постійно діючих структур і координаційних механізмів. В Україні такими елементами є Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України, а також координаційні групи між Збройними Силами України, Службою безпеки України, Держспецзв'язку та іншими державними органами. Вони забезпечують інтеграцію зусиль військового та цивільного секторів, організацію обміну інформацією, спільне реагування на кібератаки та координацію ресурсів у кризових ситуаціях [172]. Організаційний аспект оптимізації ЦВС передбачає створення гнучкої мережевої структури, яка поєднує стратегічне планування та оперативне реагування. Це включає формування багаторівневих координаційних центрів, які забезпечують постійний обмін інформацією, інтегроване управління ресурсами та спільне планування заходів щодо кіберзахисту. Важливо, що такі структури повинні бути здатні адаптуватися до змін у кіберсередовищі,

оперативно залучати приватний сектор та громадські організації, а також підтримувати взаємодію з міжнародними партнерами для обміну досвідом та кращими практиками [92, с.114].

Операційний вимір інтеграції ЦВС полягає у реалізації конкретних заходів, спрямованих на підтримку національної кіберстійкості. До них належить оперативний обмін розвідувальною інформацією щодо кіберзагроз, спільне планування сценаріїв реагування на інциденти, розробка протоколів взаємодії між державними і приватними структурами та активне залучення громадянського суспільства до моніторингу та інформування про кіберзагрози. Важливо, що такі операційні механізми мають бути стандартизованими та інтегрованими в єдину систему, щоб забезпечити оперативність і передбачуваність реагування на кібератаки [92, с. 114]. При цьому технологічні рішення мають бути інтегровані в загальну архітектуру кіберстійкості, що дозволяє координувати дії всіх учасників ВЦС та забезпечує безперервний контроль за станом національної кібербезпеки [92, с. 114].

Синтез цих трьох вимірів створює мережеву, гнучку і стійку архітектуру ЦВС, яка здатна забезпечувати безперервну інтеграцію всіх суб'єктів національної системи кібербезпеки. Така інтеграція дозволяє ефективно поєднувати стратегічне планування з оперативним реагуванням, а також гарантує, що дії військових, державних органів, приватних компаній та громадських організацій координуються в режимі постійного обміну інформацією та спільної відповідальності. Відповідно, структурна інтеграція ЦВС в національну систему кіберстійкості стає не лише механізмом управління ризиками, а й системоутворюючим елементом, що підвищує здатність держави протистояти комплексним кіберзагрозам і забезпечує стійкість критичної інфраструктури та суспільних функцій.

Таким чином, оптимальна модель ЦВС має передбачати динамічну взаємодію між суб'єктами, стандартизовані протоколи обміну даними, узгоджені механізми оцінки ризиків та ефективності реагування, а також

регулярне проведення навчань і симуляційних вправ для відпрацювання спільних дій у кризових умовах. Така модель забезпечує інтеграцію всіх компонентів національної системи кіберстійкості – стратегічного, тактичного і операційного – і підвищує здатність держави протистояти складним гібридним загрозам, що поєднують кібернапади з фізичними, економічними та інформаційними викликами.

Проведений аналіз демонструє, що цивільно-військове співробітництво виступає ключовим системоутворюючим компонентом національної системи кіберстійкості України. Теоретико-концептуальний аналіз показав, що сучасні моделі ЦВС, зокрема міжнародні практики СІМІС НАТО, передбачають багаторівневу інтеграцію військових, державних і цивільних суб'єктів. Адаптація цих підходів до національного контексту дозволяє врахувати специфіку української кіберінфраструктури, гібридних загроз і потреб у міжсекторальній координації.

Нормативно-правова база ЦВС визначає правовий статус суб'єктів, регламентує порядок взаємодії та стандарти обміну інформацією. Аналіз показав, що існуючі законодавчі механізми створюють основу для координації, проте потребують подальшого розвитку формалізації державно-приватного партнерства, інтеграції громадянського суспільства та стандартизації протоколів обміну інформацією.

Організаційно-структурна та операційно-функціональна моделі ЦВС забезпечують багаторівневу координацію стратегічного, тактичного та операційного рівнів, інтеграцію державного і приватного секторів, а також участь громадянського суспільства у формуванні стійкої кіберархітектури. Ефективність існуючих механізмів залежить від швидкості реагування на інциденти, узгодженості процедур та рівня інтеграції всіх суб'єктів.

Розробка оптимальної моделі ЦВС передбачає комплексну інтеграцію нормативного, організаційного та технологічного вимірів, що забезпечує стандартизоване об'єднання ресурсів, аналітичну підтримку прийняття рішень та здатність системи адаптуватися до нових кіберзагроз. Така модель дозволяє

реалізувати принципи державно-приватного партнерства, ефективно залучати громадянське суспільство та забезпечувати оперативне реагування на складні гібридні атаки.

Законодавчі та інституційні перспективи розвитку ЦВС в Україні зосереджені на формалізації процедур взаємодії, стандартизації обміну інформацією, розширенні ролі приватного сектору та громадянського суспільства, а також на сумісності з міжнародними стандартами НАТО та ЄС. Реалізація цих заходів створює основу для динамічної, інтегрованої та адаптивної національної системи кіберстійкості, здатної до прогнозування, запобігання та протидії сучасним кіберзагрозам.

Висновки до розділу 2

Доведено, що інституціоналізація кіберстійкості є процесом переходу від статичного захисту периметра до динамічної моделі адаптації та відновлення систем. Визначено, що ефективність цього процесу забезпечується синергією трьох підходів: регулятивного (державні норми), стандартизованого (ISO, NIST) та маркетингового (ринкові стимули, кіберстрахування). Встановлено, що ключовим елементом сучасної інституціоналізації є імплементація стандартів Директиви NIS2, яка впроваджує жорстку відповідальність керівництва та обов'язковість звітування про інциденти. Це дозволяє трансформувати кіберстійкість із вузькотехнічного завдання на стратегічний компонент державного управління. Такий підхід створює умови для формування «культури стійкості», де кожен суб'єкт господарювання стає активним учасником системи національної безпеки, що підвищує загальну адаптивність критичної інфраструктури до гібридних загроз.

Дослідження суб'єктного складу підтвердило формування в Україні багаторівневої ієрархічної системи, де НКЦК при РНБО виконує роль

стратегічного координатора та методологічного хабу. Встановлено чіткий розподіл функцій: Адміністрація Держспецзв'язку та СБУ реалізують підхід регулювання, НКЦК забезпечує стандартизацію, а Мінцифра стимулює ринкові механізми розвитку галузі. Особливу увагу приділено міжнародній суб'єктності України, яка в умовах повномасштабної війни трансформувалася з реципієнта технологій на ключового донора практичного досвіду. Участь у CCDCOE NATO та мережі CSIRTs Network легітимізує українські протоколи відсічі агресії як основу для майбутніх міжнародних стандартів колективної стійкості. Зроблено висновок, що сучасна архітектура суб'єктів забезпечує інституційну цілісність системи, дозволяючи ефективно поєднувати національні оборонні спроможності з міжнародними механізмами взаємодії у кіберпросторі.

У ході дослідження доведено, що цивільно-військове співробітництво є фундаментом національної кіберстійкості, що трансформує класичну модель CIMIC у гнучку мережеву екосистему. Виявлено термінологічну прогалину в українському правовому полі, де фактична взаємодія суб'єктів у кіберпросторі випереджає її законодавче закріплення. За результатами аналізу сформовано авторське визначення дефініції «Cyber-CIMIC» та розроблено стратегічні правки до Закону України «Про основні засади забезпечення кібербезпеки України». Запропоновані зміни дозволяють інституціоналізувати роль НКЦК як стратегічного хабу, легалізувати статус волонтерських ІТ-спільнот та впровадити економічні стимули, такі як «регуляторні пісочниці», для приватних операторів критичної інфраструктури. Реалізація цих підходів забезпечить перехід від ситуативної координації до системної інтеграції ресурсів, що підвищить адаптивність держави до гібридних загроз та забезпечить сумісність із євроатлантичними стандартами безпеки.

Проведений аналіз доводить, що цивільно-військове співробітництво у сфері кібербезпеки (Cyber-CIMIC) є ключовим інструментом забезпечення національної стійкості. Встановлено, що українська архітектура вже функціонує за логікою розширеного мережевого партнерства, однак потребує

доктринальної формалізації для усунення термінологічних прогалин. Оптимальна модель «Cyber-CIMIC» передбачає дворівневу інтеграцію: нормативну — через законодавче закріплення інтегрованого принципу взаємодії у профільному законі, та організаційну — шляхом створення постійних координаційних механізмів при НКЦК. Ефективність цієї моделі забезпечується синергією між військовою спроможністю, державним регулюванням та інноваційним потенціалом приватного сектору. Таким чином, інституціоналізація «Cyber-CIMIC» дозволить Україні не лише ефективно протидіяти гібридним загрозам, а й трансформувати свій практичний досвід у глобальні стандарти безпеки нового покоління.

РОЗДІЛ 3

АНАЛІТИЧНА РОЗВІДКА СТРАТЕГІЧНИХ НАПРЯМІВ КІБЕРСТІЙКОСТІ В УКРАЇНІ

3.1. Методологія та процес аналітичної розвідки стратегічних напрямів кіберстійкості в Україні

Термін «аналітична розвідка» використовується для опису діяльності, яка застосовує аналітичні методи для збору, обробки та інтерпретації інформації про потенційну загрозу. Тобто, це процес збору, аналізу та інтерпретації інформації з метою виявлення та оцінки потенційних загроз, визначення можливих наслідків та розробки стратегій для їх запобігання або зменшення наслідків та створення звіту або рекомендацій для прийняття рішень [115, с. 49].

Цей термін часто використовується у контексті безпеки та оборони, де аналітична розвідка використовується для підготовки стратегій і тактик протидії потенційним загрозам, таким як терористичні акти, кібератаки та інші форми агресії. Термін «аналітична розвідка» також використовується в контексті розвідувальної діяльності та безпеки: це знання, які отримуються з розвідувальної діяльності та інших джерел, та які використовуються для розробки стратегій і тактик протидії потенційним загрозам [115, с. 50].

Переваги використання терміна «аналітична розвідка» полягають у тому, що він достатньо широко охоплює не тільки процес отримання інформації, а і її використання для прийняття рішень та планування дій. Відображає обидва аспекти процесу розвідки та аналізу, є більш загальним та універсальним терміном, що може застосовуватися в різних контекстах.

Таке розуміння аналітичної розвідки як цілісного процесу – від збору даних до формування стратегічних рекомендацій – створює необхідне підґрунтя для переосмислення ролі інтелектуального аналізу в управлінні

сучасними ризиками. Оскільки цей термін охоплює не лише механічну обробку інформації, а й її трансформацію у знання для прийняття рішень, виникає потреба в адаптації розвідувальних методик до динаміки сучасних загроз. У цьому контексті критичного значення набуває виокремлення двох сучасних підходів до аналітичної розвідки, що базуються на синергії методів Форсайту та OSINT (Open Source Intelligence), які дозволяють трансформувати загальне стратегічне бачення у конкретні, обґрунтовані рішення.

Використання Форсайт та OSINT дозволяє структурувати процес прийняття рішень через призму предиктивності та глибокої інформаційної поінформованості. Стратегічне прогнозування на основі Форсайту орієнтоване на довгострокову перспективу та роботу з невизначеністю. Форсайт дозволяє аналітичній розвідці не просто передбачати один варіант майбутнього, а конструювати альтернативні сценарії розвитку загроз. Це забезпечує виявлення «слабких сигналів» та точок перелому в кіберпросторі, що є ключовим для прийняття рішень щодо превентивної розбудови стійкості до того, як загроза стане критичною.

Водночас, інформаційне забезпечення через OSINT фокусується на глибинному аналізі відкритих джерел (соціальних мереж, технічних форумів, реєстрів даних) для отримання актуальних розвідувальних знань у реальному часі. У контексті прийняття обґрунтованих рішень OSINT стає фундаментом для верифікації гіпотез та оцінки потенційного впливу загроз. Це дозволяє аналітиці бути адаптивною, надаючи керівництву перевірену фактологічну базу для оперативного коригування стратегій протидії.

Синергія цих підходів формує модель інтелектуальної стійкості: OSINT забезпечує точність та актуальність даних «тут і зараз», тоді як Форсайт трансформує ці дані у стратегічні дорожні карти. Таке поєднання гарантує, що управлінські рішення будуть не просто реактивними відповідями на інциденти, а продуктом глибокого аналітичного синтезу, спрямованого на випередження супротивника.

У лютому 2014 року розпочалась російська збройна агресія проти України, яка велась також і в кіберпросторі. Майбутній директор американського Агентства національної безпеки Майкл Роджерс з цього приводу зазначав, що разом з військовою операцією із захоплення Криму, росія розпочала проти України кібервійну [1]. Кібервійною називають російські атаки й українські експерти [374].

Після початку збройної агресії російської федерації проти України, компанії, що спеціалізувалися на наданні послуг кібербезпеки, стали реєструвати зростання кількості кібератак на інформаційні системи в країні. Зазвичай кібератаки були націлені на приховане викрадення важливої інформації, ймовірніше для надання Росії стратегічної переваги на фронті. Жертвами російських кібератак ставали урядові установи України, країн ЄС, Сполучених Штатів, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, дисиденти [119].

Кібервійна містить хвилюючий феномен. Передові суспільства, які розвинули ці можливості, якраз і є найбільш вразливими до електронної війни. На противагу цьому, кібератака на Кубу, яка має один з найнижчих показників використання комп'ютерів у світі (17 користувачів на 1000 осіб) і нерозвинену цифрову інфраструктуру, матиме відносно невеликий вплив [277]. Країни Організації економічного співробітництва та розвитку (OECD) дедалі більше залежать від цифрових систем в управлінні своєю життєво важливою інфраструктурою [361]. SCADA-системи, спеціально розроблені для контролю промислових процесів, можуть дистанційно керувати компонентами водопостачання, енергетики, транспорту та зв'язку. Комп'ютерний хробак Stuxnet був створений з метою нападу на SCADA-системи і недвозначно показав, що деякі з таких систем можуть бути пошкоджені, що може призвести до значних наслідків. Більше того, точний масштаб загрози і необхідний захист залишаються непрозорими [277].

До цього часу, урядовці вважали, що критична інфраструктура розвинених країн може бути захищена шляхом використання все більш вдосконалених технічних рішень. Тим не менш, Stuxnet підтвердив, що більшість цифрових систем, незалежно від їхнього високого рівня захисту, все одно є вразливими.

Отже, щоб запобігти кібератакам, можливо, потрібно використовувати аналогові системи для моніторингу запасу електроенергії, води та інших важливих комунальних послуг. Наразі, занепокоєння можливістю кібератак на атомні електростанції вже призвело до свідомого урізноманітнення систем з поєднанням цифрових, аналогових і ручних [277]. Однак у двадцять першому столітті зробити це в основній інфраструктурі надзвичайно складно, оскільки інженери звернулися до цифрових рішень для підвищення операційної ефективності [422, с. 898].

Наприклад, інфраструктуру Великої Британії не можна вимкнути, як вимикач, частково тому, що вона все ще має певну «системну різноманітність». Частково це результат застарілих систем, а частково – результат випадковості. Небезпека полягає в тому, що це ненавмисне, але цінне джерело стійкості буде знищене в ім'я скорочення витрат і підвищення ефективності. Широке впровадження інтелектуального обліку є прикладом універсальної системи, яка містить вразливість, зумовлену прагненням до більшої ефективності та результативності [277].

Отже, різноманітність систем стала новим улюбленим словом у сфері кібербезпеки. Стійкість вимагає дедалі складнішого поєднання фізичної безпеки, безпеки персоналу, контролю закупівель і зміцнення систем разом з подальшими заходами для запобігання несанкціонованим або ненавмисним модифікаціям дизайну системи безпеки.

Крім того, впровадження злагоджених аналогових і людських систем безпеки суттєво змінило уявлення про інформаційну безпеку. До цього моменту спеціалісти з інформаційної безпеки головним чином займалися кіберзлочинністю, зазвичай проводили складні спроби проникнення в системи

безпеки банків і великих компаній. За більш ніж 10 років роботи в цій сфері було зроблено висновок, що більшість збоїв у системі безпеки є наслідком поєднання людської некомпетентності та зловмисності [388, с. 1]. Однак, зважаючи на загрозу серйозної кібервійни на державному рівні, експерти розглядають людей разом із системами як останню лінію захисту від витончених кібератак [277].

Серед фахівців з інформаційної безпеки була поширена ортодоксальна думка, що головною перешкодою для безпеки системи є люди, а не самі системи [152]. Вірогідною була думка, що більшість серйозних порушень безпеки виникають через недостатній рівень знань персоналу, а не через технічні неполадки. Проте поява комп'ютерного хробака Stuxnet, який був використаний для на ядерні центрифуги в Ірані, вказує на те, що такий підхід має бути переглянутий. Велика кількість людей почала вивчати майбутню кібербезпеку після виявлення складного шкідливого програмного забезпечення, яке шпигує за промисловими системами та підриває їх.

Відповідь на питання кіберстійкості, як у випадку Stuxnet, полягає в поєднанні різноманітних або. гібридних систем, які керують певною частиною національної інфраструктури. У той час навіть найбільш захищені системи могли бути піддані технічним атакам іззовні. У наступні десятиліття основним каталізатором інформаційно-комунікаційних технологій стане все ближчий зв'язок між інтернетом і людьми. Головною ціллю комерційних технологічних підприємств є безперешкодне об'єднання людини та інтернету. На сьогодні це виявляється в потужніших портативних пристроях, сполучених з хмарними технологіями.

Однак, майбутнє просунутого зв'язку між людиною та інтернетом – це прямий інтерфейс між комп'ютером і мозком, сфера, в якій медичні технології вже розширюють межі [228]. Вплив цього розвитку на кіберстійкість має певну вагу. Коли людина буде відправляти електронне повідомлення, «після роздумів і короткого кліпання очима» [277], кібербезпека стане ще важливішою, ніж на сьогодні. Щоб захистити нашу інфраструктуру, ми

повинні докладати рішучих зусиль, щоб впоратися з комерційними та культурними перешкодами, спрямованими на надмірну залежність від електронних систем.

Витрати на інтернет-безпеку також створюють серйозні труднощі, але в значно більшому розмірі. Це надзвичайно дорога і ризикована сфера, ніхто посправжньому не хоче нею володіти [277]. Однак більшість людей погоджується, що інтернет має вирішальне значення, і що його потрібно захистити.

Управління кібербезпекою є типовим прикладом міжурядової сфери, яка працює на регіональному рівні значно краще. У Європі існує власна кіберорганізація, Європейське агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency – ENISA), розташована на острові Кіпр. У практичній сфері ENISA виконує функцію координації регулювання та сприяє зближенню, але має обмежені можливості оперативних дій. Тим не менш, більшість ІКТ-бізнесу позитивно ставиться до ENISA, стверджуючи, що один набір регуляторних практик для Європи є кращим, ніж 26 [181, с. 58]. Масштаби телекомунікаційної галузі означають, що саме Європейське агентство, а не уряд, має більший операційний потенціал і, власне, досвід для забезпечення значущої кіберстійкості [277].

Будучи за своєю природою транснаціональними і часто використовуваними у контексті глобалізації, агентства Європейського Союзу, такі як ENISA, також мають схожі проблеми складності і невизначеності, які ставлять у скрутне становище національні уряди. Кіберстійкість може бути найбільш привабливою через те, що вона може використовуватися як рухома ціль. У тривалий період часу урядові програми та проекти не досягали успіху. Це було пов'язано з тим, що вони були надто вибуховими та не мали потенціалу для впровадження нових технологій, а також тому, що приватний сектор розвивався швидше, ніж уряд. Що ми знаємо напевно, так це те, що світ інформаційно-комунікаційних технологій прискорюється, а проблеми, які стоять перед урядом, зростають у своїх розмірах і складності [277].

Отже, в майбутньому враховуватиметься гібридизація процесів розвідки, безпеки, ризиків і стійкості для досягнення кіберстійкості ландшафту. Однак, короткостроково, це стає проблемою для управління, як з точки зору власності, так і з точки зору співпраці між державними й приватним секторами.

Форсайт – це складний, багатоетапний та безперервний процес, кінцевою метою якого є прийняття обґрунтованих рішень щодо забезпечення стратегічних планів для можливого різноманітного розвитку подій у майбутньому. Він дає змогу осмислити різні можливі варіанти майбутнього та стратегічно підготуватися до ймовірних сценаріїв. З середини 1950-х – початку 1960-х років форсайт як дисципліна перетворився на основний інструмент стратегічного планування як для приватних корпорацій, так і для державного сектору [277].

Форсайт продовжує розвиватися й змінюватися і сьогодні. Це значною мірою пов'язано з тим, що він орієнтований на дії, а отже, має відчутні результати; він є відкритим, тобто в рамках форсайту існує свобода мислити нестандартно або переосмислювати попередні уявлення; нарешті, він є міждисциплінарним, він об'єднує різні групи, які мають досвід у широкому діапазоні тем, таким чином забезпечуючи більш реалістичне і продумане можливе майбутнє.

У виданні ЄС «Що таке форсайт» зазначається: «Форсайт – це не пророцтво і не передбачення. Він не має на меті передбачити майбутнє – розкрити його так, ніби воно визначене наперед, – а допомогти нам його побудувати» [415].

Виділяють три основні переваги форсайту [246; 268]:

- генерація знань,
- сприяння відносинам із зацікавленими сторонами,
- посилення спроможності.

Знання допомагають окремим зацікавленим сторонам найкращим чином позиціонувати себе для майбутнього розвитку; маючи знання, вони можуть

бачити поза оманю, що майбутнє буде схожим на теперішнє, і уявляти собі передове майбутнє [246]. Розвиток таких знань і розуміння сприяє підвищенню зв'язків між зацікавленими сторонами, що у свою чергу посилює мережі, особливо у випадку кібербезпеки.

Форсайт сприяє посиленню спроможностей; результати форсайту дозволяють визначити, що є важливішим для організаційних спроможностей і спроможностей зацікавлених сторін. Визначення та підтримка цієї інформації є життєво важливими для розвитку та отримання ключових навичок, технологій та політики.

Застосування форсайту у сфері кібербезпеки наразі не є широко розповсюдженим [149, с. 7]. Проте, запровадження зазначених методів в галузь кібербезпеки сприятиме набуттю ще більш глибокого, розумного та взаємодіючого усвідомлення ризиків, а також стратегічних наслідків заходів забезпечення безпеки.

Щоб адекватно реагувати на майбутні загрози кібербезпеці та формувати більш безпечне суспільство, необхідно спиратися на висновки та дослідження спільноти фахівців з питань майбутнього та форсайту, щоб розробити процес застосування форсайту до кіберстійкості.

Для досягнення здатності розуміти можливості майбутнього, важливо належним чином розвивати кібербезпекову екосистему з метою вирішення та управління новими та майбутніми викликами.

Як кіберстійкість, так і форсайт отримують вигоду від багатогранного і міждисциплінарного середовища. Часто розумно об'єднувати системи з інших галузей з цієї самої причини. Вважається [246], що керівні принципи, практики, підходи, методи та інструменти як системного мислення, так і розробок, орієнтованих на користувача, можуть бути ключовими для формування правильного мислення [379] при підході до форсайту у сфері кібербезпеки.

Для того, щоб краще проілюструвати спектр методів, відповідні методи, системи та інструменти, як правило, групуються в шість категорій [382, с. 83].

Тим не менш, не всі прийоми можна визнати характерними для передбачення майбутнього. Також використовуються стратегічні методи планування та методи вирішення проблем, які часто включаються у діяльність форсайту.

Загалом, виділяються такі групи методів [415]:

- системи аналізу середовища
- аналіз тенденцій
- форсайт експертні групи
- сценарний метод
- морфологічний аналіз та ретроспективний аналіз
- методи аналізу кібербезпеки.

Системи аналізу середовища дають користувачам можливість ретельно вивчати обране середовище для виявлення слабких сигналів вхідних змін, які можуть мати значний вплив на майбутнє. Ці методи сприяють структурованому та аналітичному сприйняттю поточної ситуації з метою досягнення взаєморозуміння. Зазвичай, ці методи базуються на засадах діагностики.

Існують різні методи для сканування середовища, серед яких, наприклад, такі:

STEEP – система аналізу соціокультурних, технологічних, економічних, екологічних та політичних факторів певної сфери;

PESTLE – система аналізу політичних, економічних, соціокультурних, технологічних, правових та екологічних факторів певної сфери;

SWOT – система визначення та аналізу сильних і слабких сторін, можливостей і загроз для певного напрямку або організації.

Кожна з перерахованих систем дозволяє проводити систематичну оцінку характеристик, змін і впливів у зазначених областях, щоб отримати уявлення про навколишнє середовище. Крім того, існують інші відмінності цих ідей, які враховують інші сфери – вибір методу або сфери має ґрунтуватися на початковому аналізі цієї теми.

Аналіз тенденцій. Тенденція визначається певним трендом змін в часовому вимірі або появою нової моделі змін, яка зазвичай впливає на великі соціальні групи [245]. Методи аналізу тенденцій зазвичай слугують прогностичним або діагностичним цілям.

Тренди можна аналізувати різними способами – наприклад, за допомогою оглядів літератури, бібліометрії, текстового аналізу, патентного аналізу та аналізу впливу трендів. Ці методи виявляють поточні або нові тенденції і, як правило, досліджують причину, потенційний вплив, ймовірність і швидкість виникнення цих тенденцій [247].

Інші методи, що використовуються для аналізу тенденцій, включають [415]:

- причинново-наслідковий багаторівневий аналіз – сприяє визначенню рушійних сил шляхом отримання розуміння сприйняття учасників, таких як світогляд, цінності та культурні норми;
- тренд-радар – надає міжгалузевий погляд на нові та вже існуючі тенденції в цільовому середовищі;
- аналіз впливу трендів – аналіз впливу однієї або декількох можливих подій на екстраполяцію тренду в майбутнє;
- сканування горизонту – систематичний моніторинг поточних тенденцій, а також виявлення нових, актуальних подій у певній сфері за допомогою творчого процесу колективного осмислення.

Форсайт-експертні групи охоплюють широкий спектр методів і підходів. Експертні панелі та метод Дельфі є одними з найвідоміших складових сімейства форсайт-експертних груп. У обох випадках експерти висловлюють свою думку про майбутнє. Проте метод Дельфі полягає в більш структурованому підході до спілкування, щоб отримати відповіді від фахівців. Експерти зазвичай запрошуються для підтримки проекту з форсайту з прогностичними або рекомендаційними цілями.

Дельфі – це дослідницький метод, заснований на структурованому та ітеративному груповому спілкуванні між експертами, які висловлюють

судження з обраної теми. У першій послідовності різні експерти в певній галузі опитуються окремо щодо конкретної теми або питання. Потім збираються їхні анонімні відповіді, і експертів просять прокоментувати зібрані думки. Для досягнення консенсусу цей процес повторюється кілька разів. Такий підхід допомагає уникнути групового мислення, а отже генерує більше креативних ідей з різних точок зору. Весь процес можна проводити дистанційно, що полегшує залучення більш різноманітної групи експертів з усього світу. Цей метод може забирати багато часу, особливо коли є кілька ітерацій [415].

Японський національний інститут науково-технічної політики (NISTEP) проводить форсайт приблизно кожні п'ять років, більшість з яких ґрунтується на великому дослідженні за методом Дельфі, в якому беруть участь близько 2000 учасників [343].

Інші приклади методів, заснованих на експертних групах, включають [415]:

- зведені судження / груповий прогноз – логічно поєднує декілька індивідуальних суджень в узгоджені та колективні судження;
- дослідження ключових технологій (технологічне прогнозування) – застосовує набори критеріїв до критичних технологічних розробок з метою надання обґрунтованої оцінки.

Водночас існують також методи колективного форсайту, за яких інформація збирається у не експертному середовищі.

Серед найбільш поширених і відомих методів передбачення у форсайті є сценарні методи. Вони використовуються як інструменти дослідження для розмірковування про можливе, бажане або небажане майбутнє, але не для точного передбачення конкретного майбутнього. Крім того, ці методи можуть бути використані для створення та оцінки різних варіантів, щоб знайти найкращий підхід. Зазвичай вивчається кілька можливих сценаріїв майбутнього, щоб прийняти рішення, які можуть допомогти запобігти потенційним проблемам і пасткам.

Зазвичай на початку розробки сценаріїв проводиться діагностика, яка дозволяє об'єктивно розглянути основні фактори, що можуть вплинути на майбутнє питання, яке вивчається. Розгляд кількох потенційних варіантів майбутнього підвищує розуміння різних факторів, що можуть впливати на майбутнє. Ці знання дозволяють створити більш гнучкі, перспективні та адаптивні рішення.

Наприклад, сценарії можна розробляти різними методами [415]:

- ігри – розробка ігор або рольових сценаріїв для тестування можливих стратегій або рішень шляхом визначення можливих реакцій та наслідків їх реалізації;

- візія – погляд в ідеальне майбутнє для створення стратегії досягнення конкретних цілей;

- аналіз перехресного впливу – оцінює ймовірність настання певних подій у майбутньому шляхом оцінки ймовірності настання інших подій, а потім досліджує їхній взаємний зв'язок.

Морфологічний та ретроспективний аналіз включає в себе різноманітні методи, які зазвичай не мають взаємозв'язку, але мають однакові дві характеристики – намір передбачення та акцент на регресію подій і декомпозицію системи. Регресійний аналіз у форсайті дотримується підходу, подібного до статистичного регресійного аналізу. Однак регресійний аналіз у форсайті працює з якісними даними й суб'єктивною думкою, на відміну від кількісних методів визначення подій і тригерів подій, які можуть призвести до передбачуваної майбутньої події [139]. Однак декомпозиція ставить за мету розділення складних систем на менші компоненти для полегшення аналізу їх структури, динаміки взаємодії та впливу на систему в цілому.

Морфологічний аналіз – це творчий, евристичний, нормативний метод, який підтримує дослідження складних проблем і можливих рішень за допомогою багатовимірної матриці [415]. Це трудомістка групова справа, яка потребує фасилітації [295].

Бек-кастинг – ще один нормативний метод, який фокусується на обраному сценарії бажаного (або небажаного) майбутнього. Потім учасники рухаються назад у часі, щоб визначити рішення або події, які мають відбутися, щоб перетворити обраний сценарій на реальність [415].

За допомогою беккастингу організації можуть планувати, дії що їм слід вжити, та оцінювати потенційні наслідки. Це підвищує обізнаність про те, що майбутнє визначається багатьма факторами і що різні дії призводять до різних альтернативних результатів [295].

Прогнозування загроз – це багатоетапний метод, який передбачає уявлення небажаного майбутнього, а потім реконструкцію кроків і рішень, які необхідно вжити, щоб запобігти цьому майбутньому [415]. Він був розроблений, перш за все, для аналізу військового майбутнього. Прогнозування загроз поєднує в собі багато методів передбачення, включаючи Дельфі, науково-фантастичне прототипування, беккастинг і моделювання сценаріїв. Цей метод має визначений часовий горизонт – кожна діяльність спрямована на 10 років вперед [410, с. 82].

Інші методи, що входять до цієї групи [415]:

- аналіз технологічної послідовності – генерує імовірні часові рамки для технологічних послідовностей шляхом аналізу оцінок часу, необхідного для проміжних технічних кроків;
- розробка дорожньої карти – розробляється документ, який визначає кроки та етапи, необхідні для досягнення бажаного майбутнього;
- багатокритеріальний аналіз – порівнює можливі ідентифіковані рішення із зваженим набором критеріїв оцінки;
- синектика – сприяє новому і творчому мисленню, наприклад, уявляючи обрану проблему в незвичному, не пов'язаному з нею середовищі.

Кібербезпека є складовою системи, яка включає розгляд інцидентів і криз, а також ретельний аналіз майбутніх ризиків і загроз. Методи аналізу кібербезпеки є різновидами способів оцінювання ризиків. Хоча фокус кожного з них трохи відрізняється (наприклад, на суб'єкті загрози або на візуалізації),

загальна мета кожного з них полягає в тому, щоб знайти та визначити пріоритети ризику, а потім прийняти відповідні заходи. Цей підхід може бути використаний для постановки діагнозу, прогнозування або надання рекомендацій.

Найвідомішими методами, які добре себе зарекомендували в аналізі ризиків і моделюванні загроз є такі:

- оцінка ризику агента загрози (Threat Agent Risk Assessment (TARA) [371] – метод оцінки ризиків на основі загроз, який використовується для виявлення, оцінки та визначення пріоритетності ризиків. Він зосереджує увагу на суб'єктах загроз, їх мотивації та можливих методах;

- оперативно критична оцінка загрози, активу і вразливості (Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) [145] – комплексний метод оцінки для виявлення, ранжування та управління ризиками кібербезпеки;

- моделювання загроз [158] – метод концептуального аналізу, що використовується для виявлення потенційних вразливостей і розробки заходів на ранніх стадіях розробки додатків або послуг.

Існує багато систем і методів для моделювання загроз, одним з таких методів є Дерево атак. Дерева атак базуються на визначенні дерев можливих методів, які можуть допомогти зловмиснику досягти своїх цілей.

Незважаючи на те, що вони не повністю ідентичні, інструменти є платформами або допоміжними системами, які допомагають у застосуванні методів прогнозування. Незважаючи на те, що деякі з них спрямовані на оцифрування форсайту, інші лише мають на меті покращити ваш досвід форсайту на індивідуальному рівні. Під час вибору інструментів форсайту для конкретної діяльності слід розглянути інші потенційні джерела, оскільки деякі з них спеціально розроблені для певної аудиторії або ситуації.

Інструменти для фасилітації семінарів часто використовуються фасилітаторами воркшопів для полегшення комунікації під час воркшопів або для генерування креативних ідей від учасників.

Ось кілька відомих прикладів [415]:

- мозковий штурм, коли учасників заохочують генерувати велику кількість сирих, спонтанних ідей, надихаючись ідеями інших учасників, без негайного оцінювання;

- світове кафе, де велика група учасників може обговорити різні питання в структурований спосіб, по колу, в менших групах, і записати свої ідеї на великих аркушах паперу, щоб інші групи могли бачити й використовувати їх як довідник;

- Mind mapping – метод графічної фасилітації, який допомагає візуально організувати зібрану інформацію.

Існує кілька цифрових баз даних, які надають інформацію про інструменти, що стосуються форсайту.

Одним із джерел для визначення додаткових інструментів для форсайту є веб-сайт Service Design Tools [359], який описує та впорядковує інструменти на основі етапу процесу проектування, зацікавлених сторін та учасників, мети діяльності та бажаних методів візуалізації. Інші ресурси включають Платформу майбутнього (Futures Platform) [249], Інструментарій майбутнього врядування (Governance Futures Toolkit) [285] та Teach the Future [395], який має на меті надати викладачам інструменти для інтеграції форсайту в їхні навчальні програми.

Інструменти на основі штучного інтелекту (ШІ) можуть допомогти в таких видах форсайту, як оцінка поточного середовища, аналіз тенденцій або екстраполяція тенденцій. Хоча ці інструменти не є повсюдними, вони часто інтегровані в процес форсайту [303, с. 209–211]. Особливо корисним є використання ШІ для пошуку текстів й аналізу великих обсягів даних, таких як виявлення термінів і фраз, які вказують на нові або майбутні тенденції, або для підтримки огляду літератури. У більшості випадків для цього застосовується обробка реальної мови. Також інструменти, що базуються на штучному інтелекті, можуть допомогти у виборі сценаріїв.

Для кращого полегшення форсайту багато експертів рекомендують використовувати інструменти для спільної роботи (наприклад, цифрові дошки і додатки для нотаток), а також дослідницькі бази даних для камеральних досліджень і розпізнавання тенденцій. Важливо зазначити, що в експертному середовищі не завжди довіряють існуючим радарним базам даних та джерелам інформації для форсайту. Ці джерела рідко публікують деталі процесу збору та підготовки інформації, тому опитані експерти, як правило, покладаються на власні дослідження або першоджерела для визначення інформації, пов'язаної з трендами.

Інструменти для проведення конференцій часто використовуються для залучення учасників з різних географічних регіонів. Вони надзвичайно корисні для об'єднання різноманітних груп учасників. Однак, використання цих інструментів має і зворотний бік. Учасники можуть бути менш здатними повністю присвятити свою увагу онлайн-зустрічам (на відміну від особистих семінарів) через меншу інтерактивність віддалених семінарів і той факт, що деякі учасники можуть піддаватися спокусі робити кілька справ одночасно або приєднуватися до інших зустрічей. Крім того, рівень цифрової грамотності в групі може бути різним – через брак технічних навичок та обізнаності деякі учасники можуть бути не в змозі повноцінно та впевнено брати участь під час використання інструментів для проведення конференцій.

Поява нових загроз є складною, швидкоплинною та іноді непередбачуваною подією, особливо з урахуванням стрімкого приросту кіберінцидентів. Отже, часто може статися, що ймовірність та актуальність окремих загроз у багатьох випадках може раптово змінитися через непередбачувані інциденти, суспільні зміни або спонтанні інновації. Різнобічні глобальні ініціативи охоплюють широкий спектр тем, включаючи визначення кіберзагроз та класифікацію їх за рівнем небезпеки.

Багато загроз, відомих сьогодні, залишаться актуальними в майбутньому, але їх характер зміниться через зростання залежності, демократизацію та розвиток нових технологій.

Прикладом системної роботи з визначення майбутнього (форсайту) у сфері кібербезпеки є проведений аналіз за ініціативою ENISA у період з березня по серпень 2022 року [284], яким було визначено та ранжовано 21 загрозу, поширеність яких зростатиме до 2030 року. Було проведено серії семінарів та інтерв'ю з відповідними експертами за методом PESTLE та застосовано різноманітні підходи до методології.

Використана методологія ENISA складається з чотирьох етапів [246]. Перший, «спільне дослідження», – це фаза дослідження тенденцій та збору інформації, яка інтегрувала знання експертів, зворотний зв'язок та перевірку. На другому етапі, «групові семінари з прогнозування», збиралися групи експертів з досвідом роботи в одному з вимірів PESTLE для подальшого обговорення, вивчення, оцінки та визначення пріоритетів виявлених тенденцій.

Третій етап, «ідентифікація загроз», ґрунтувався на методології «кастингу загроз» для визначення нових викликів, які можуть виникнути впродовж наступних 10 років. Для цього невеликим групам експертів з кібербезпеки надавався сценарій, який поєднував пріоритетні тенденції.

На наступному етапі, визначені учасниками-експертами, загрози були оцінені за такими показниками, як імовірність, вплив, новизна і те, чи була ця загроза раніше визначена. Новизна розглядалася для того, щоб визначити пріоритетність менш відомих загроз. Акцент було зроблено на 10 кіберзагрозах з найвищим рейтингом, при цьому, суб'єктами загроз визначено чотири основні групи: держава-спонсор, кіберзлочинці, хакери-найманці та хактивісти [235].

Методологічно прогноз побудовано на основі поточної таксономії загроз ENISA [403], яка поділяє їх на такі категорії високого рівня:

- фізична атака (навмисна),
- ненавмисне пошкодження / втрата інформації або ІТ-активів,
- стихійні лиха (природні),
- збої / несправності,

- перебої в роботі,
- підслуховування / перехоплення / викрадення,
- недобросовісна діяльність / зловживання, а також правові аспекти.

Важливо зазначити, що ненавмисні загрози розглядаються як вразливості, які можуть бути використані суб'єктом загрози, а тому основний акцент зроблено на навмисних загрозах [246]:

- компрометація ланцюжка поставок програмних засобів;
- просунуті кампанії з дезінформації / операцій впливу;
- зростання авторитаризму цифрового нагляду / втрата приватності;
- людські помилки та застарілі системи в кіберфізичних екосистемах;
- цілеспрямовані атаки (наприклад, програми-вимагачі), посилені даними зі смарт-пристроїв;
- брак аналізу та контролю космічної інфраструктури та об'єктів;
- зростання сучасних гібридних загроз;
- дефіцит навичок;
- транскордонні постачальники послуг ІКТ як єдина точка відмови
- зловживання штучним інтелектом.

Різні види розвідки – військова, політична, економічна, соціальна, екологічна, медична та культурна – надають важливу інформацію для прийняття рішень.

Дуже часто помилково вважають, що розвіддані збираються лише таємними або прихованими методами, і хоча деякі розвідувальні дані дійсно збираються за допомогою таємних операцій і відомі лише на найвищих рівнях влади, інші розвідувальні дані складаються з інформації, яка є загальнодоступною. За даними Федерального бюро розслідувань (ФБР) США, які визнаються багатьма правоохоронними органами в усьому світі, що діють сьогодні, існують різні способи збору розвідувальної інформації, які в сукупності зазвичай називають «напрями збору розвідувальної інформації», що наведені в таблиці 3.1.

Напрями збору розвідувальної інформації

Напрями	Опис
Human intelligence (HUMINT)	Збір інформації може проводитися відкрито, коли поліцейські опитують свідків або підозрюваних під час виконання своїх службових обов'язків, або ж за допомогою спланованих, цілеспрямованих, таємних або негласних заходів. Особа, яка надає інформацію поліції в рамках негласних відносин, називається «агентом» або «джерелом». З огляду на зростаючі рівні ризику, безпеки, складності, правових та етичних міркувань, а також вимог щодо дотримання законодавства, правоохоронні органи, які використовують таємні джерела розвідувальної інформації, мають спеціальні підрозділи з підготовленими співробітниками.
Signals intelligence (SIGINT)	Базується на передачі електронного (радіо) сигналу, що можуть бути зібрані кораблями, літаками, наземними об'єктами або супутниками. Зазвичай SIGINT здійснюється військовими або розвідувальними службами, а не національними правоохоронними органами, хоча на федеральному та національному рівнях SIGINT може використовуватися правоохоронними органами для підтримки розслідувань тяжких злочинів, організованої злочинності та тероризму, які загрожують громадській безпеці.
Communications intelligence (COMINT)	Різновид SIGINT і стосується перехоплення комунікацій між двома або більше сторонами. Це може здійснюватися в режимі реального часу або перехоплюватися і зберігатися для майбутніх допитів. Як і SIGINT, COMINT може використовуватися правоохоронними органами для підтримки розслідувань організованої злочинності та тероризму, які становлять серйозну загрозу громадській безпеці.
Imagery intelligence (IMINT)	Також відома як фоторозвідка (PHOTINT), IMINT включає в себе аеро- і все частіше супутникові знімки, пов'язані з розвідкою. Традиційно прерогатива військових і розвідувальних відомств, IMINT все частіше використовується правоохоронними органами, які використовують повітряні засоби, включаючи гелікоптери, а останнім часом і безпілотні літальні апарати (БПЛА).
Measurement and signatures intelligence (MASINT)	Відносно маловідомий напрям збору даних, який стосується можливостей озброєнь і промислової діяльності. MASINT включає в себе поглиблену обробку і використання даних, зібраних за допомогою наземних і повітряних систем збору IMINT і SIGINT.
Telemetry intelligence (TELINT)	Використовується військовими і розвідувальними відомствами, іноді застосовується для позначення даних, що передаються зброєю під час випробувань в рамках міжнародного моніторингу з метою протидії розповсюдженню хімічної, біологічної, ядерної або радіологічної зброї.
Electronic intelligence (ELINT)	Вказує на електронні випромінювання, отримані від сучасної зброї та систем стеження. Як TELINT, так і ELINT можуть бути різновидами SIGINT і сприяти MASINT в рамках багатостороннього підходу до операцій зі збору розвідувальної інформації від військових і розвідувальних служб.

У цьому переліку спеціальних напрямів збору розвідувальної інформації OSINT знайшла своє місце і широко використовується місцевими та національними правоохоронними органами, розвідувальними службами та збройними силами. Враховуючи масштаб, доступність і високу віддачу від розвідки при мінімальних витратах ресурсів, OSINT є тим «клеєм», який об'єднує, доповнює і все більше підтверджує інші розвідувальні функції правоохоронних органів, що є важливими оперативними причинами того, чому OSINT швидко перетворилася на багате джерело інформації для виявлення сучасного злочинця.

За визначенням ФБР, OSINT – це розвідувальний напрям, що стосується розвідувальних даних, отриманих на основі «загальнодоступної інформації, яка збирається, використовується і своєчасно поширюється серед відповідної аудиторії з метою задоволення конкретних розвідувальних та інформаційних потреб». OSINT – це також розвіддані, отримані шляхом відкритого збору та аналізу загальнодоступної інформації з відкритих джерел, яка не перебуває під прямим контролем державних органів. OSINT походить від систематичного збору, обробки та аналізу загальнодоступної інформації у відповідь на потреби безпеки. [242]

Два важливих взаємопов'язаних терміни – *«відкрите джерело»* і *«загальнодоступна інформація»* – визначаються ФБР як:

- *відкрите джерело* – це будь-яка особа чи група осіб, які надають інформацію, не розраховуючи на конфіденційність – інформація, стосунки або і те, і інше не захищені від публічного розголошення. Інформація з відкритих джерел може бути загальнодоступною, але не вся загальнодоступна інформація є відкритим джерелом;

- *загальнодоступна інформація* – це дані, факти, інструкції або інші матеріали, опубліковані або трансльовані для широкого загалу; доступні за запитом представникам громадськості; законно побачені або почуті будь-яким випадковим спостерігачем; або надані на зборах, відкритих для широкої громадськості.

OSINT відноситься до широкого спектру інформації та джерел, які є загальнодоступними, включаючи інформацію, отриману із засобів масової інформації (газети, радіо, телебачення тощо), професійні та академічні записи (документи, конференції, професійні асоціації тощо), а також публічні дані (урядові звіти, демографічні дані, слухання, промови тощо). OSINT включає інтернет-спільноти та створений користувачами контент, такий як сайти соціальних мереж, сайти для обміну відео та фото, вікі та блоги. Вона також включає геопросторову інформацію, таку як паперові та електронні карти, атласи, довідники, плани портів, гравітаційні дані, аеронавігаційні дані, навігаційні дані, геодезичні дані, дані про рельєф місцевості, дані про навколишнє середовище та комерційні зображення.

Одним з найважливіших аспектів OSINT є цінність, яку вона додає поліцейським операціям у вигляді можливості отримувати своєчасну, надійну і дієву розвідувальну інформацію, пов'язану з розслідуванням або інцидентом, що розглядається. На додаток до традиційних методів розслідування і джерел інформації, OSINT демонструє значні успіхи в отриманні доступу до такої інформації та її зборі. Приклади варіюються від інформації, розміщеної в соціальних мережах як одного з найбільш можливих засобів доступу до розвідувальних даних з відкритих джерел, до даних про місцезнаходження або інформації про перегляд веб-сторінок. Але справжню цінність OSINT для правоохоронних органів набуває тоді, коли вона поєднується з аналітичними можливостями в режимі реального часу, забезпечуючи правоохоронні органи життєво необхідною ситуаційною обізнаністю для запобігання інцидентам, боротьби зі злочинністю та реагування на надзвичайні ситуації або більш масштабні кризові події.

OSINT має ключові характеристики, які забезпечують більшу частину необхідної вихідної інформації для будь-якої правоохоронної операції. Доступність, глибина та діапазон загальнодоступної інформації, яка міститься у відкритих джерелах, дозволяє правоохоронним органам задовольняти потреби в розвідувальній та інформаційній діяльності без використання або

підтримки спеціалізованих людських або технічних засобів збору інформації за низькою вартістю. Це також покращує збір інформації, оскільки інформація з відкритих джерел підтримує спостереження та розвідувальну діяльність, відповідаючи на розвідувальні та інформаційні запити. Вона також надає інформацію, яка покращує і використовує більше технічних засобів збору інформації. OSINT також здатна покращити виробництво розвідувальних даних. Як частина міждисциплінарних розвідувальних зусиль, використання і інтеграція загальнодоступної інформації і відкритих джерел гарантує, що аналітики мають можливість користуватися усіма джерелами загальнодоступної інформації для прийняття інформативних рішень.

Прийняття обґрунтованих рішень є основною роллю і важливою рисою будь-якого успішного поліцейського, особливо тих керівників, на яких покладено відповідальність за організацію і керівництво масштабними розслідуваннями або врегулювання кризових ситуацій, що виникають. Ефективне прийняття рішень, особливо на самому початку великих інцидентів або розслідувань, гарантує, що можливості не будуть втрачені, а потенційні напрямки розслідування будуть визначені та ретельно відпрацьовані [204]. Насправді, правоохоронці, які беруть участь у розслідуванні на ранніх стадіях, змушені боротися з браком достатньої інформації на початковому етапі, в той час, коли важливі рішення потрібно приймати швидко і інтуїтивно, але розвиток і доступність OSINT допомогли інформувати і значно поліпшити початкові дії поліції, що є життєво важливим для порятунку життів, запобігання катастрофам і ефективного реагування на події, що розгортаються.

Незважаючи на те, що для правоохоронних органів існують значні можливості використання потенціалу OSINT, всі співробітники правоохоронних органів повинні, працюючи з OSINT, особливо ті, що ведуть складні розслідування, переконатися, що ніщо не сприймається як належне, і не можна вважати, що речі є такими, якими вони здаються, або що правильні процеси та протоколи розвідки були дотримані належним чином. У будь-

якому розслідуванню немає місця для самозаспокоєння. Пошук підтвердження, повторна перевірка, перегляд і підтвердження всіх аспектів OSINT, які можуть спрямовувати розслідування, є ознаками ефективного аналітика, і вони повинні гарантувати, що жодна потенційна лінія розслідування не буде пропущена під час динамічного і швидкого розслідування, в тому числі операцій, які значною мірою покладаються на OSINT.

Для того, щоб розслідування було ефективним, воно може ґрунтуватися на гіпотезі або керуватися нею як відправною точкою. Для всіх розслідувань гіпотеза – це припущення, висунуте як основа для міркувань без сприйняття його істинності, і припущення, висунуте як відправна точка для подальшого дослідження відомих фактів [204]. Розробка та використання гіпотез є широко визнаним методом серед слідчих та аналітиків, який може бути використаний як засіб для встановлення найбільш логічного або ймовірного пояснення, теорії або висновку щодо того, чому і як було вчинено злочин. В ідеалі, перш ніж слідчі розроблятимуть гіпотезу, вони повинні мати достатньо достовірних матеріалів, на яких можна було б ґрунтувати гіпотезу, що традиційно включає дані про жертву, точні деталі інциденту або події, національні або міжнародні аспекти злочину, мотиви злочину і точний спосіб його вчинення. Але використання OSINT тепер надає новий, багатший і детальніший набір даних для обґрунтування гіпотези слідчого, а простий законний доступ до соціальних мереж дозволяє отримати особисту інформацію, зображення та посилання на друзів і знайомих, що прискорює та інформативно наповнює реакцію правоохоронних органів на злочини.

На відміну від інших напрямів збору розвідувальної інформації, OSINT не є виключною відповідальністю якогось одного відомства, а збирається всією спільнотою правоохоронних органів. Однією з переваг OSINT є її доступність, хоча велика кількість доступної інформації може ускладнити визначення того, що є цінним. Визначення джерела даних та їх достовірності також може бути складним. Тому дані OSINT все ще потребують перевірки та аналізу, щоб бути корисними для осіб, які приймають рішення у сфері

правоохоронної діяльності, і повинні бути належним чином оброблені разом з іншими розвідувальними даними, отриманими за допомогою інших методів збору інформації. Оскільки розвіддані складаються з інформації та даних, коли вони знаходяться у розпорядженні органів державної влади, на них поширюється дія різних законів про захист даних та розкриття інформації, які застосовуються до органів державної влади. Використовуючи OSINT, правоохоронні органи повинні дотримуватися своїх законних обов'язків щодо розкриття інформації, захисту інформації, а також виконувати свої дискреційні повноваження та обов'язки щодо розкриття інформації та обміну нею. Якщо розвідувальні дані коли-небудь будуть використані як докази в кримінальному провадженні, виникнуть інші міркування, а також існують правові вимоги щодо їх збору, обробки та зберігання. Керівники правоохоронних органів, які забезпечують управління розвідданими, несуть відповідальність за дотримання належного та професійного використання збору та аналізу інформації. Для налагодження, консолідації та професіоналізації процесу розвідки, особливо коли йдеться про використання OSINT, необхідно прийняти деякі базові принципи, наведені нижче [275]:

- розвідувальна діяльність повинна бути законною, переслідувати легітимну мету, бути необхідною і пропорційною;
- співробітники правоохоронних органів повинні бути належним чином обізнані, підготовлені та оснащені для виконання своєї ролі в процесі управління розвідувальною діяльністю;
- безпека та конфіденційність мають важливе значення для створення ефективного та професійного розвідувального середовища;
- організаційна та партнерська діяльність має ґрунтуватися на знанні проблем та їх контексту, чому сприяє розуміння розвідки;
- розвідка не слугує жодній меті, якщо вона не використовується;
- ефективне використання розвідки як інструменту вимагає об'єктивності і неупередженості як з боку аналітика, так і з боку подальшого користувача.

Усі розвідувальні дані мають бути оцінені для перевірки їхньої достовірності, і OSINT не є винятком, незважаючи на їхній вільний і відкритий доступ. Слідчі та аналітики правоохоронних органів несуть відповідальність за оцінку будь-якої розвідувальної інформації, яку вони надають, гарантуючи, що це буде точна і неупереджена оцінка, заснована на їхньому знанні переважаючих обставин, що існують на той час [204].

Збір інформації та подальший аналіз з метою формування розвідувальних даних не відбувається у вакуумі, і суспільні та політичні очікування від поліцейських-практиків полягають у тому, що їхня робота буде ґрунтуватися на розвідданих, спрямованих на запобігання та зменшення шкоди громадянам і громадам, яким вони служать. Це підкріплюється створенням встановлених моделей бізнес-процесів для впровадження підходів, заснованих на аналітиці, в культуру та операційну діяльність правоохоронних органів.

При роботі з розвідувальними даними, отриманими з відкритих джерел, зокрема, з соціальних мереж, необхідно належним чином керувати очікуваннями громадськості щодо конфіденційності, оскільки, незважаючи на те, що часто вони знаходяться у вільному доступі, значна частина інформації, розміщеної на таких сайтах, як Facebook і X (Twitter), розглядається зареєстрованими користувачами як особиста інформація. При роботі з OSINT, на відміну від більш традиційних закритих джерел розвідувальної інформації, занепокоєння розвідувального співтовариства зміщується з доступності інформації на ідентифікацію релевантної і точної інформації. З цих причин все частіше виникає необхідність перевіряти розвідувальні дані, отримані з відкритих джерел, за допомогою надійних закритих розвідувальних даних і досвіду професіоналів у сфері безпеки. Перевірка розвідданих у такий спосіб є особливо гострою темою, коли йдеться про контент у соціальних мережах, оскільки користувачі часто вирішують не розкривати або фальсифікувати особисту інформацію, яку вони надають на цих платформах [144].

З точки зору національної безпеки, рішення на основі OSINT повинні розширити можливості правоохоронних органів і органів безпеки, надаючи доступ до більш дієвих розвідувальних даних, які можуть підтримати існуючі процеси прийняття рішень, постановки завдань і координації діяльності. Ядро будь-якого OSINT-рішення має бути зосереджене на зборі та використанні даних, орієнтованих на Інтернет. Останнє включає розробку розширених можливостей і сервісів для збору, аналізу, візуалізації та об'єднання релевантних даних, на основі яких можна генерувати динамічні гіпотези в реальному часі.

Заходи боротьби зі злочинністю і тероризмом – онлайн і офлайн – стають все більш важливим елементом будь-якої стратегії національної безпеки. Якщо поглянути на сучасні підходи до боротьби з тероризмом у Великій Британії, то 4 принципи стратегії CONTEST [402] є фундаментальною основою заходів із запобігання, переслідування, захисту і підготовки до терору. Огляд цих чотирьох принципів і того, як OSINT може бути використаний для їх підтримки, можна знайти в таблиці 3.2.

Слід зазначити, що хоча цілі терористів і організованих злочинних груп відрізняються, зв'язки між терористичною і організованою злочинною діяльністю, схоже, зростають. Наприклад, під час теракту в Мюнхені (22 липня 2016 року), як вважають, виконавець нападу придбав зброю через «темну мережу». Злочинна діяльність, до якої причетні терористичні групи, або через зв'язки з окремими злочинцями і злочинними угрупованнями, або через власні операції, може включати торгівлю незаконними товарами і речовинами, такими як зброя і наркотики, торгівлю людьми, фінансове шахрайство, відмивання грошей і здирництво.

OSINT вже використовується як одне з ключових джерел розвідданих для національної безпеки, і його значення тільки зростає. І як демонструє таблиця 3.2, широта поточного та потенційного використання є величезною.

Огляд принципів стратегії CONTEST та їх застосування для OSINT

Компонента	Контекст компоненти	OSINT-пропозиції
Стратегія превенції	Стратегія превенції спрямована на боротьбу з радикалізацією людей, які підтримують міжнародну загрозу тероризму та організованої злочинності.	Виявлення терористичних наративів, впливових осіб та пропаганди через поверхневу мережу, особливо у протидії спробам залучення людей до тероризму шляхом «підбурювання та вербування», таким чином усуваючи фактори або першопричини, які можуть призвести до радикалізації та вербування в країні та на міжнародному рівні. Більш ефективний розвиток контр-екстремістських наративів та заохочення міжкультурного діалогу, що сприяє належному управлінню, демократії, освіті та економічному процвітання. Розуміння спільнот та сфер, що викликають стурбованість.
Стратегія переслідування	Стратегія переслідування спрямована на зменшення терористичної загрози шляхом підриву діяльності терористів та організованих злочинних угруповань та їхніх операцій	Збір розвідданих з темної мережі. Правовий та етичний процес збору доказів для забезпечення обвинувальних вироків. Міжнародна кооперація, що допомагає переслідувати та розслідувати терористичні загрози всередині та за межами національних кордонів, перешкоджати пересуванню та спілкуванню терористів і злочинців, руйнувати їхні мережі підтримки, перекривати фінансування та доступ до матеріалів для атак, а також притягати осіб до відповідальності.
Стратегія захисту	Стратегія захисту спрямована на зменшення вразливості держави до терористичних атак та активності організованої злочинності.	Проактивна оцінка загроз уразливих місць (наприклад, безпека кордонів) та соціальних сфер ризику, таких як сексуальна експлуатація дітей. Проактивна та оперативна оцінка загроз масовим скупченням людей. Захист національної критичної інфраструктури та зменшення її вразливості до атак, у тому числі шляхом посилення безпеки кордонів та транспорту.
Підготовча стратегія	Підготовка стратегії спрямована на забезпечення максимальної готовності населення і держави до наслідків терористичних атак і активності організованої злочинності	Підвищення стійкості громад. Підготовка до потенційних хімічних, біологічних, радіоактивних, ядерних та вибухових атак. Моделювання розвитку організованої злочинності. Раннє попередження про загрози для здоров'я.

Однак OSINT не може бути єдиним джерелом, на яке покладаються правоохоронні органи та служби безпеки. OSINT є найбільш потужним, коли він здатний доповнити існуючі розвідувальні дані із закритих джерел, надаючи додаткову інформацію і вказуючи напрямок, де може знадобитися подальша розвідка. Комбінований вплив OSINT і традиційних джерел розвідки відображає розвідувальний апарат національної безпеки країни.

Особи, які приймають рішення як у цивільній, так і у військовій сферах, діючи на стратегічному і тактичному рівнях, постійно стикаються з необхідністю прийняття більш швидких, надійних і краще обґрунтованих рішень. Аналітики, які інтерпретують дані, перетворюючи їх на змістовні розвіддані, стикаються з постійною боротьбою за те, щоб впоратися з постійно зростаючим обсягом, швидкістю, різноманітністю і перевіркою даних (*Volume, Velocity, Variety and Validation*) (далі – 4V) [144], великою кількістю формальних і неформальних (OSINT) джерел даних, щодо яких мають місце запитання до їх достовірності.

Прийняття більш обґрунтованих рішень проявляється у багатьох аспектах. На стратегічному рівні це можна побачити в таких ситуаціях, як, наприклад, питання про те, чи є достатні і достовірні розвідувальні дані про певну терористичну діяльність в країні. Або ж в операціях з підтримання миру, надання гуманітарної допомоги і ліквідації наслідків катастроф. Крім того, прийняття рішень у цьому контексті може виникнути при використанні правоохоронних органів проти серйозної організованої злочинності або тероризму. У всіх цих прикладах низка критичних факторів поєднується і посилюється. Це робить отримання все більшого обсягу даних 4V, які створюються, а отже, і потенційних даних, які необхідно враховувати як для короткострокового, так і для довгострокового аналізу, значним, зростаючим і постійно актуальним викликом.

Для військових ця потреба в прийнятті більш обґрунтованих рішень призвела до розробки і розгортання інтегрованої здатності збирати і поширювати інформацію за допомогою надзвичайно потужних сенсорів

(візуальних – оптичних і інфрачервоних, радіолокаційних – активних і радіоелектронних – пасивних), встановлених на різноманітних високовартісних повітряних, наземних і військово-морських платформах. Ця спроможність, відома як C4ISTAR (*Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance* (Командування, управління, зв'язок, комп'ютери, розвідка, спостереження, виявлення цілей та рекогносцирування)), охоплює спектр можливостей, які стосуються командування, управління, зв'язку, комп'ютерів, інформації/розвідки, спостереження, наведення на ціль і розвідки.

На початку 2000-х років ці можливості були доповнені групами геостационарних і навколоземних супутників, які ще більше розширили ці можливості і додали можливості визначення часу і місцезнаходження. Потреба в точних і своєчасних даних для прийняття рішень не менша і в цивільному світі. Хоча технології і доступ до бюджетів можуть дещо відрізнятися від військових, з нинішнім відносно недорогим доступом не лише до космічних зображень з відкритих джерел, а й до даних про час і місцезнаходження, голосового зв'язку і передачі даних, зростання технологічного прогресу в широкому спектрі датчиків, що генерують дані (як космічних, так і інших), означає, що ті ж самі проблеми швидкості, обсягу, неоднозначності і достовірності, з якими стикаються військові (тобто, 4Vs) в процесі прийняття більш поінформованих рішень, впливають і на цивільних остаточних користувачів правоохоронних органів.

Простір бою – це термін, який використовується для опису простору, в якому військові проводять свої операції під час воєнних дій. У мирний час цей термін можна було б краще описати як простір безпеки, де всі активи, люди, інформація, мережі та технології функціонують разом і розглядаються як система систем, якщо дивитися і розглядати їх як єдине ціле.

Дедалі більшого значення для цивільних органів влади і правоохоронних органів – незалежно від їх географічної чи територіальної юрисдикції – набуває наш дедалі складніший і взаємопов'язаний світ, в якому прийняття

рішень має відбуватися в умовах більшої складності, невизначеності і взаємозалежності; і в якому допоміжний розвідувальний цикл має йти в ногу з часом як з технологічної точки зору, так і з огляду на всі аспекти людського виміру.

Це можна побачити у відносинах суспільства з критичною інфраструктурою (КІ), від якої залежить здоров'я, добробут і саме виживання громадян, громад і суспільства в цілому. Тут суспільство і багато різноманітних і різних громад, в яких живуть громадяни, стали повністю залежними від багатьох секторів КІ та основних послуг, таких як транспорт, енергетика, охорона здоров'я, фінанси, продовольство і зв'язок, з якими нерозривно пов'язане їхнє здоров'я і благополуччя. КІ та мережа взаємопов'язаних і взаємозалежних систем, які її підтримують і лежать в її основі, як і згаданий вище безпековий простір прийняття рішень, також можуть бути описані як система систем.

Критичну інфраструктуру часто описують як «систему систем», яка функціонує за підтримки великих, складних, широко розподілених і взаємодоповнюючих ланцюгів постачання і мереж. Такі системи тісно пов'язані з економічним і соціальним добробутом та безпекою громад, які вони обслуговують. Вони включають не лише інфраструктуру, але й мережі та ланцюги поставок, які підтримують постачання необхідних продуктів або послуг [358, с. 505].

А всередині, поряд або на межі цієї системи систем КІ знаходяться багато різноманітних і нерозривно пов'язаних між собою різних спільнот, які часто називають екосистемами в залежності від того, як вони розвиваються, структуруються і функціонують. Саме на цьому тлі має відбуватися прийняття рішень щодо планування, підготовки, реагування та відновлення після значних техногенних, зловмисних або природних подій.

Ця залежність громад і суспільства експоненціально збільшується до ризиків, небезпек, загроз і вразливостей через саму природу того, як ця система систем взаємодіє для того, щоб функціонувати; з багатьма

невидимими і, по суті, невідомими взаємозалежностями і залежностями всередині і між ними. Коли система зазнає потрясінь, незалежно від того, чи є вони штучними, зловмисними або природними, вони можуть мати невідомі наслідки або каскадні ефекти, непропорційні події, що їх спричинили.

Саме тут численні особи, які приймають рішення, з багатьох різних цивільних організацій та правоохоронних органів (як на місцевому, так і на регіональному рівнях у межах окремих країн або в рамках транскордонного прикордонного співробітництва) повинні зібратися разом і ефективно співпрацювати задля досягнення низки спільних результатів. Ці результати проявляються у плануванні та підготовці до таких потрясінь, реагуванні на них та відновленні після них, а також у плануванні, підготовці, проведенні, а часто і перегляді або розслідуванні таких правоохоронних заходів, які можуть бути пов'язані з серйозною організованою злочинністю або тероризмом.

Саме в таких випадках складність притаманна самій системі. Саме в таких ситуаціях, коли багато різних організацій повинні працювати разом ефективно і результативно для досягнення спільного ефекту від їхніх колективних зусиль, невидимі наслідки або каскадні ефекти, що виникають через взаємозалежність самої системи, означають, що погано обґрунтоване прийняття рішень може призвести до втрат життів, а також до економічних витрат, фізичної шкоди або суспільного добробуту. OSINT є зростаючим і все більш важливим аспектом у прийнятті рішень правоохоронними органами в таких ситуаціях – і це було ще до того, як зростаюче використання соціальних мереж вивело на перший план відкритий код. Поява соціальних мереж як джерела розвідувальної інформації з відкритих джерел здебільшого призвела до розширення обсягу і спектру джерел OSINT, які тепер доступні для більшого кола аудиторії, користувачів і додатків. По суті, якщо система, в якій вона знаходиться і використовується, в даному випадку розвідувальний цикл, не є такою ж інтегрованою, як і система, в якій відбувається прийняття рішень, то застосування і цінність OSINT буде набагато менш ефективною, дієвою і значущою.

Світ переосмислюється завдяки відкритим джерелам. Загальнодоступна інформація може бути використана різними особами та організаціями для досягнення широкого спектру цілей, і правоохоронні органи все частіше ефективно використовують це безкоштовне та доступне джерело інформації. Хоча Інтернет та соціальні мережі позитивно збагатили суспільні комунікації та економічні можливості, ці технологічні досягнення змінили – і продовжують змінювати – саму природу злочинності, сприяючи появі нових витончених і технічно оснащених злочинців. Характер деяких «традиційних» видів злочинів трансформувався завдяки використанню комп'ютерів та інформаційно-комунікаційних технологій (ІКТ) з точки зору їхнього масштабу та охоплення, а загрози та ризики поширилися на багато аспектів суспільного життя. Також з'явилися нові форми злочинної діяльності, спрямовані на порушення цілісності комп'ютерів і комп'ютерних мереж. Загрози існують не лише для окремих осіб і бізнесу, але й для національної безпеки та інфраструктури.

Крім того, безмежний характер явища кіберзлочинності та транснаціональний характер торгівлі людьми, імпорту наркотиків і незаконного переміщення вогнепальної зброї, готівки та крадених товарів означає, що злочинці можуть планувати свої злочини з юрисдикцій по всьому світу, що робить правоохоронну діяльність особливо складною, і саме тому правоохоронні органи повинні максимально використовувати потенціал OSINT та шукати нові інноваційні способи запобігання злочинам. Прогресивні та далекоглядні правоохоронні органи, які заохочують, приймають та використовують можливості OSINT, будуть краще підготовлені до майбутніх викликів у сфері безпеки, і, як наслідок, матимуть більше можливостей для забезпечення безпеки громад, яким вони служать, а також для того, щоб вони почували себе в більшій безпеці.

Здатність правоохоронних органів використовувати можливості OSINT буде дедалі більше відрізнятися – розмежування між тими поліцейськими силами, які є лідерами, і тими, які просто сліднують за ними. Тому прийняття

правової та етичної бази для ефективного використання OSINT є вкрай необхідним не лише для того, щоб реалізувати переваги можливостей OSINT для запобігання злочинам, переслідування злочинців та підготовки до нових викликів і загроз, але й для підвищення ефективності та результативності послуг, які надають правоохоронні органи, а також для кращого захисту публічної інформації, якою вони користуються. Але поки OSINT залишається значною мірою нерегульованим серед правоохоронних органів, і жодна установа не має права власності або першості, непотрібне дублювання доступу та небажані посягання на конфіденційність даних громадян, ймовірно, будуть постійною особливістю зростаючого використання OSINT в майбутньому. Тому правоохоронні органи ніколи не повинні забувати, що неналежний доступ і використання OSINT лише посилює аргументацію на користь запровадження жорстких інструкцій, посилення законів і загалом обмеження вільного доступу до публічної інформації та її збору. Крім того, правоохоронним органам слід забезпечити, щоб використання всіх OSINT відповідало формальним процесам моделі управління розвідкою. Такий підхід дозволить зберегти і зміцнити довіру громад, яким вони служать, у тому, що доступ до їхньої загальнодоступної інформації здійснюється на законних підставах з метою боротьби зі злочинністю та забезпечення безпеки співгромадян.

Інформація з відкритих джерел отримується з газет, журналів, радіо, телебачення та Інтернету. Аналітики вже давно використовують таку інформацію як доповнення до засекречених даних, але систематичний збір інформації з відкритих джерел не був пріоритетом розвідувального співтовариства. Останніми роками, з огляду на зміни в міжнародному середовищі, особливо після подій 11 вересня, лунають заклики до більш інтенсивного і цілеспрямованого інвестування в збір і аналіз інформації з відкритих джерел. Однак дехто все ще наголошує на тому, що основним завданням розвідки залишається отримання і аналіз таємного контенту.

Зараз існує консенсус щодо того, що OSINT необхідно систематично здійснювати і він має стати важливим компонентом аналітичних процесів. Це було визнано різними комісіями і закріплено в законах. Загалом, зазначається про цінність використання OSINT в усіх аспектах повсякденної діяльності правоохоронних органів. Однак, ще не так давно, у 2016 році, не використовувалися терміни «соціальні медіа», «супутник» і «дрони», які експоненціально розвиваються, здешевлюються і використовуються все ширше. Таке зростання призвело до того, що під час холодної війни на OSINT припадало лише 10 % інформаційного забезпечення розвідки, а 90 % походило з закритих джерел. Сьогодні ситуація змінилася, і 90 % інформації і даних для розвідки надходить від OSINT.

Експоненціальне зростання доступності OSINT і його використання правоохоронними органами зумовлює необхідність забезпечення повної інтеграції OSINT, як він існує зараз і може розвиватися в майбутньому, з розвідувальними даними із закритих джерел; і все це в рамках загальної системи управління інформацією. Таким чином, можна досягти більш точного, своєчасного та належного використання інформації в повсякденному процесі прийняття рішень.

Дуже важливо, що це забезпечило б вищий рівень впевненості у використанні таких розвідувальних даних, оскільки обидва джерела надають взаємну підтримку, щоб запевнити як правоохоронні органи, так і громадян, яким вони служать, у тому, що рішення, які вони приймають, ґрунтуються на найбільш надійній, точній і достовірній інформації, доступній на той час, і що в результаті приймаються більш обґрунтовані рішення. Досягнення такого результату могло б зменшити ймовірну шкоду для політичної та розвідувальної спільнот.

Небезпечні високотехнологічні загрози глобального характеру, що мають високий потенційний вплив та руйнівні наслідки для життєдіяльності будь-якого суспільства, є невід'ємним наслідком розвитку новітніх технологій. І охорона суспільних відносин, інтересів людини, суспільства та

держави в сфері кіберпростору займає одне з пріоритетних місць в системі національної безпеки. Сучасний світ, враховуючи такі зміни та загальні тенденції, намагається впроваджувати механізми забезпечення кібербезпеки [44].

На основі соціологічної теорії (Ulrich Beck) інформаційне суспільство є суспільством ризику, у якому мають місце загрози різного змісту й характеру, а також обумовлений ними розподіл ризиків [160]. Саме тому сучасний безпековий менеджмент потребує нового рівня мислення, в основі якого адекватне сприйняття ризику і його ключова роль у методології пізнання безпекового довкілля, прогнозування майбутнього та зваженого прийняття управлінських рішень. Наразі, ключовими акцентами сучасних безпекових досліджень мають бути прикладні результати наукового аналізу, на основі емпіричного дослідницького підтвердження висунутих гіпотез, що зосереджують увагу на існуючих проблемах, ключових загрозах та підвищують обізнаність як суспільства у цілому, так і суб'єктів безпеки [307, с. 89; 351].

Проблемами кібербезпеки займається багато дослідників з різних галузей. Їх наукові інтереси охоплюють як розробку теоретичних моделей та формування відповідних методологій, так і дослідницькі інтереси прикладного характеру з визначеними безпековими аспектами. Багато робіт присвячено питанням управління інформаційною безпекою, різним його напрямом: управління ризиками в системі інформаційної безпеки [298; 341; 384]; управління інформаційними ресурсами в системі безпеки [319; 341; 354]; ефективності управління захистом інформації [319; 354; 420]. Особливу увагу зосереджено на виявленні вразливостей системи кібербезпеки, зокрема програмних продуктів, їх класифікації [304; 305; 331; 333; 384]. Зосереджуються на захисті інформації на основі локалізації аномалій, акцентуючи увагу на статистичних методах їх виявлення [140; 254; 353; 364; 424]. Щодо дослідження кіберзагроз – застосовуються методи, які гуртуються на кількісно-якісному

аналізі [89, с. 135] з використанням системи виявлення аномалій та виявлення вторгнень [68; 302], інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур [4] а також методах, заснованих на нечітких множинах [69].

Важливе дослідження проведено науковцями та фахівцями за ініціативою ENISA (*European Union Agency for Cybersecurity*) [145; 201; 233; 318; 389; 413], щодо *risk management frameworks and methodologies*, де проаналізовано усі відомі методології та системи управління ризиками кібербезпеки визначено їх *interoperability* та перспективність застосування.

Використання загальних методологічних підходів, сучасних методів управління ризиками та відповідних міжнародних стандартів визначили подальший підхід до методології подальшого аналізу та оцінки ризиків поширення кіберзагроз [65].

Сучасні розвинені безпекові системи, зокрема й у сфері кібербезпеки, характеризуються новаціями загальнонаукового та спеціального змісту, які створюють можливості передбачення із врахуванням взаємопов'язаних елементів, серед яких одним із основних інструментів є управління ризиками. Наразі, із врахуванням Резолюції генеральної асамблеї ООН та у межах розвитку глобальної культури кібербезпеки, упроваджуються механізми, серед яких одне з ключових місць займає ризик-орієнтований підхід – *учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації і її захисту* [117, с. 164].

Тож, очевидно, реалізуючи державну політику із врахуванням міжнародних стандартів, Україна активно розвивається і в цьому напрямі [26]. Зокрема, у Стратегії національної безпеки України, введеної в дію Указом Президента України від 14 вересня 2020 року № 392/2020 [109], зазначено, що *Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий*

спектр загроз, що передбачатиме оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей, а також поширення необхідних знань і навичок у цій сфері. Про ризик-орієнтований підхід щодо забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021-2025 років [110], а у Плані реалізації Стратегії кібербезпеки [108] (далі *План реалізації Стратегії*) чітко визначено завдання: «Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки ... розробити методики ідентифікації та оцінки кіберризиків ..., забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик» [117, с. 165].

Вочевидь, упровадження сучасних методологій потребує відповідного наукового супроводження, більше того, аналіз стратегічного характеру, що базується на емпіричній базі, сформованій широкою експертною думкою, реалізується безпосередньо в межах не лише кримінології, а й соціології, статистики та науки про дані (*Data Science*), що вимагає дотримання методологічних вимог. Саме тому, на нашу думку, є усі підстави стверджувати, що такі завдання вирішуються переважно в межах прикладного наукового дослідження, із врахуванням дослідницького досвіду та напрацюванням відповідної методології й інструментарію обробки та аналізу великих даних (*Big Data*) [117, с. 165].

Місце кіберстійкості в системі оцінки ризиків визначається переходом від точкового аналізу ймовірності інциденту до комплексного управління життєздатністю системи. В традиційних моделях ризик оцінюється як добуток імовірності на наслідки, де основні зусилля спрямовуються на зниження першого показника. Ризик-орієнтований підхід у контексті стійкості зміщує пріоритети в бік управління наслідками та обмеження радіуса ураження. Це передбачає трансформацію системи з реактивної (реагування на факт атаки) у проактивну та адаптивну. Комплексне управління життєздатністю базується на інтеграції процесів ризик-менеджменту безпосередньо в операційний цикл

системи, що дозволяє не просто усувати слабкі місця, а й створювати прогностні моделі поведінки під час кризи. Такий підхід забезпечує прозорий зв'язок між технічними заходами та стратегічними цілями національної безпеки, дозволяючи суб'єктам кібербезпеки діяти на випередження, вибудовуючи гнучку архітектуру захисту, здатну до самовідновлення та еволюції.

У межах підготовки пропозицій до розроблення нової Стратегії кібербезпеки, у 2024 році було започатковано дослідницький проєкт «Система кіберстійкості в Україні» та визначено наступні завдання:

- ідентифікація кіберзагроз та оцінювання ризиків поширення їх в Україні;
- визначення індикаторів, що характеризують інституційну спроможність кіберсистеми та кіберстійкість в Україні;
- побудова прогностної моделі на основі регресійного аналізу [26, с. 19].

Для проведення дослідження обрано ризик-орієнтований підхід у якості базового, який, на нашу думку, став основою для дослідження за обраним напрямом. Базовими засадами для реалізації визначених завдань оцінювання ризиків є міжнародний стандарт, імплементований до вітчизняного законодавства, так який у 2018 році прийнятий як національний стандарт, – ДСТУ ISO 31000:2018 [26, с. 19; 48].

На цій основі розроблено відповідний опитувальник, відповіді на запитання якого були конфіденційними і не потребували розкриття особистих даних експертів. Опитування проводилось в режимі ON-LINE шляхом заповнення анкет, в яких кожен індикатор оцінювався за двома характеристиками: «Ймовірність (Рівень оцінювання)» та «Можливі наслідки (Вплив)» за 3-4-5-бальною шкалою [26, с. 19].

Подальший аналіз проведено із застосуванням програмного забезпечення IBM SPSS Statistics. На основі сформованого синтаксису [308, с. 62–64] визначено інтегроване значення оцінки поширення загроз у сфері фінансової безпеки та подано у відсотковому значенні за шкалою від 0 до

100%. Таким чином, сформовано за рівнем ризику рейтинг кіберзагроз [26].

Для забезпечення комплексності аналізу, системного бачення проблем, врахування специфіки поширення кіберзагроз важливим вбачалося відображення специфіки регіону мешкання, власного досвіду та обізнаності респондентів щодо сфери кібербезпеки в Україні тощо [26, с. 19].

За суб'єктом, який представляє експерт (табл. 3.3) найбільшу частку склали представники обласних військових адміністрацій (20,1 %) районних військових адміністрацій (8,5 %), які сукупно сформували майже третину генеральної експертної сукупності [26, с. 19].

Таблиця 3.3

Розподіл експертів за суб'єктом (органом)

Суб'єкт (орган)	%
Національний координаційний центр кібербезпеки (РНБО)	0,6
Кабінет міністрів України	0,2
міністерство або інший центральний орган виконавчої влади	13,0
Державна служба спецзв'язку та захисту інформації України	13,3
обласна військова адміністрація	20,1
районна військова адміністрація	8,5
правоохоронний орган	15,5
розвідувальний орган	0,8
контррозвідувальний орган	0,2
постачальник ІКТ послуг	0,5
критична інфраструктура	15,8
громадська організація	0,6
освітня (наукова) установа	10,6

Значною експертною вибіркою характеризуються групи представників об'єктів критичної інфраструктури (15,8 %), правоохоронних органів (15,5 %), Державної служби спецзв'язку та захисту інформації України (далі ДССЗІ) (13,3 %) та центральних органів виконавчої влади (далі ЦОВВ) (13,0 %) [26, с. 19].

Водночас, недостатньо охопленими виявились експертні групи з представників розвідувальних та контррозвідувальних органів (0,8 % та 0,2 %

-відповідно), підприємств-постачальників ІКТ послуг (0,5 %) та фахового спрямування громадських організацій (0,6 %) [26, с. 20].

Опитуванням було охоплено усі регіони України (табл. 3.4), серед яких майже третину даних сформовано експертною думкою столичного регіону (Київ – 31,9 %) [26, с. 20].

Таблиця 3.4.

Регіональний розподіл експертного середовища

Регіон	%
Вінницька обл.	1,7
Волинська обл.	0,9
Донецька обл.	14,3
Дніпропетровська обл.	1,7
Житомирська обл.	0,5
Закарпатська обл.	1,4
Запорізька обл.	1,9
Івано-Франківська обл.	6,3
м.Київ	31,9
Київська обл.	6,6
Кіровоградська обл.	1,3
Луганська обл.	0,8
Львівська обл.	3,2
Миколаївська обл.	0,7
Одеська обл.	1,8
Полтавська обл.	1,6
Рівненська обл.	1,0
Сумська обл.	3,8
Тернопільська обл.	0,9
Харківська обл.	2,3
Херсонська обл.	5,4
Хмельницька обл.	1,4
Черкаська обл.	1,1
Чернівецька обл.	5,1
Чернігівська обл.	2,7

Загалом представники усіх регіонів прийняли участь в опитуванні але з певною перевагою з Донецької (тимчасово переміщених) (14,3%), Київської (6,6 %), Івано-Франківської (6,3 %), Херсонської (5,4 %) та Чернівецької (5,1 %) областей [26, с. 20].

Не дивлячись на те, що кіберзагрози переважно характеризуються зовнішніми факторами поширення, особливо у період воєнного стану та російської агресії, все ж важливим є залучення експертів з усіх регіонів України. Кожен регіон має свої особливості щодо розташування на їх територіях об'єктів критичної інфраструктури, а тому і можуть по особливому проявлятися різноманітні кіберзагрози. Водночас, регіональні аспекти по-різному можуть характеризувати кіберстійкість, залежно від активності регіональної влади та окремих суб'єктів кібербезпеки.

Опитуванням охоплено і експертів, які представляють різні галузі та сфери (табл.3.5) [26, с. 20].

Таблиця 3.5

Галузевий розподіл експертного середовища

Галузь діяльності	%
державне управління	40,1
енергетичний комплекс	3,3
фінанси/банки/страхування	1,8
інфраструктура/транспортна система	2,2
телекомунікаційні послуги	30,5
цифрові послуги	17,2
оборонно-промисловий комплекс	4,8

Найбільша експертна вибірка представляє державне управління (40,1 %), телекомунікаційні (30,5 %) та цифрові (17,2 %) послуги. Значно меншою, але все ж наявною є думка експертів оборонно-промислового (4,8 %) та енергетичного (3,3 %) комплексів, а також інфраструктура (транспорт) (2,2 %) та фінансова система (1,8 %) [26, с. 20].

Окремий інтерес викликає аналіз експертної вибірки за досвідом діяльності у сфері кібербезпеки (табл. 3.6) [26, с. 20].

Таблиця 3.6

Експертна вибірка за досвідом діяльності у сфері кібербезпеки

Досвід діяльності за фахом кібербезпеки	%
до 1 року	37,3
1–3 роки	27,6
3–10 років	23,3
10–20 років	8,2
понад 20 років	3,7

Найбільшою групою експертів у генеральній експертній сукупності виявились фахівці з досвідом до 1-го року (37,3 %) та в інтервалі 1-3 років (27,6 %). Достатньо помітною у відносному значенні також є група експертів з досвідом 3-10 років (23,3 %). Водночас, найменш вираженою експертна вибірка з досвідом 10-20 років (8,2 %) та понад 20 (3,7 %) років. Такий розподіл на нашу думку є закономірним, так як відображає переважно експертне середовище державного сектору суб'єктів представлених у дослідженні (орієнтовно близько 80 % за даними табл.3.3) [26, с. 20].

Водночас, враховуючи значний обсяг опитувальника (1025 індикаторів), напруженість при його осмисленні та заповненні, а також припускаючи можливість помилкових тверджень респондентів, для виокремлення найбільш надійної інформації з отриманих даних, забезпечуючи статистичні обґрунтування процедури обмеження вибірки [259; 309] було здійснено відбір анкет лише тих експертів, які надавали логічно узгоджені відповіді [26, с. 20].

Експертів, які взяли участь в опитуванні та пройшли фільтри надійності згруповано за категорією посад експертів (табл. 3.7) [26, с. 20].

Зазначена експертна вибірка забезпечила формування базової сукупності даних, отриманих від лише тих експертів, які надавали логічно узгоджені відповіді.

Таблиця 3.7

Категорії посад респондентів

Категорія посади	Відсоток у загальній кількості надійної вибірки, %
оперативний працівник	17.7
керівник оперативного підрозділу	4.6
аналітик	1.4
керівник аналітичного підрозділу	0.3
інспектор (старший інспектор)	76.0

Незважаючи на те, що після фільтрування даних залишилося 40,35 % початкової вибірки, якість результатів суттєво зросла. Це можна бачити на прикладі оцінювання індикаторів за експертними вибірками щодо надійності (табл. 3.8) [26].

Таблиця 3.8

Аналіз за фільтром логічної помилки

НАЗВА ІНДИКАТОРА	ОЦІНКА ймовірності	Вибірка		Статистична значущість	Pearson Chi-Square	Cramer's V
		Ненадійна частина	Надійна частина			
1.1. порушення конфіденційності (розголошення даних)	низька	23,3%	15,7%	0,004	10.868	.117
	середня	41,3%	37,6%			
	висока	35,5%	46,79%			
7.1. Суб'єкти, які здійснюють (ініціюють) кібератаки на об'єкти в Україні: держава-спонсор	низька	17.6%	11.1%	0,001	14.102	.142
	середня	22.1%	14.6%			
	висока	60.3%	74.3%			

Порівнюючи розподіл оцінювання за групами експертів, що були відібрані за фільтром відсутності логічних помилок, у порівнянні з тими, хто цей фільтр не пройшов, можна бачити, різниця в розподілах є значною, зокрема:

щодо кіберзагрози як порушення конфіденційності (розголошення даних) – 23,3% ненадійних експертів вказали на низький рівень ймовірності, в

той час як надійні обрали цей варіант у 15,7% випадків. Варіант «висока ймовірність» був обраний ненадійною частиною експертів у 35,5% випадків, а надійною – 46,79%. Ця різниця є не тільки статистично значущою (критерій $\chi^2 = 10.868$, $p < 0.004$), але й величина ефекту є достатньо значною (V Крамера = 0.117, $p < 0.004$)

Щодо суб'єктів, які здійснюють (ініціюють) кібератаки на об'єкти в Україні: держава-спонсор – 17,6 % ненадійних експертів вказали на низький рівень ймовірності, в той час як надійні обрали цей варіант у 11,1 % випадків. Варіант «висока ймовірність» був обраний ненадійною частиною експертів у 60,3 % випадків, а надійною – 74,3%. Ця різниця є не тільки статистично значущою (критерій $\chi^2 = 14.102$, $p < 0.001$), але й величина ефекту є достатньо значною (V Крамера = 0.142, $p < 0.001$). Аналогічні тенденції спостерігаються і по інших важливих питаннях анкети.

Таким чином, обмеження вибірки на основі перевірки на логічну помилку є статистично значущим та забезпечує надійність експертної вибірки для подальшого репрезентативного аналізу.

Одним з результатів стало те, що було оцінено ризики поширення кіберзагроз та визначено ті з них, що характеризуються найвищим рівнем (рис.3.1). Водночас, в межах дослідницького інтересу, варто перш за все, звернути увагу на варіативність оцінювання кіберзагроз за середнім значенням генеральної експертної сукупності та вибірки на основі виділення експертних груп за досвідом фахової діяльності у сфері кібербезпеки [26,с. 21-22].

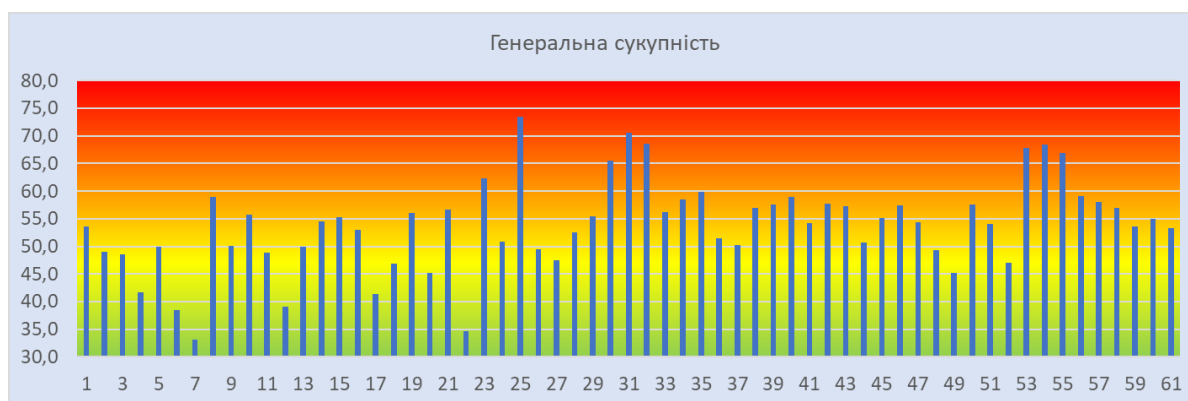


Рис. 3.1 Варіативність оцінювання кіберзагроз за середнім значенням генеральної експертної сукупності

За середнім значенням, в межах генеральної експертної сукупності, оцінювання ризиків поширення кіберзагроз є достатньо варіативним і певним чином формує базові засади виявлення найзначніших загроз та визначення пріоритетних напрямів у формуванні стратегічного бачення в системі кібербезпеки [66].

Водночас, використовуючи додаткові дані, що характеризують ризики сформовані на основі експертної вибірки за ознакою досвіду фахової діяльності у сфері кібербезпеки, достатньо помітними є певні розбіжності в оцінювання рівня ризику за окремими кіберзагрозами (рис.3.2) [66, с.71].

Як бачимо, певною варіативністю характеризується і оцінювання ризиків поширення кіберзагроз між різними групами експертів, які розподіляються за фаховим рівнем у сфері кібербезпеки.

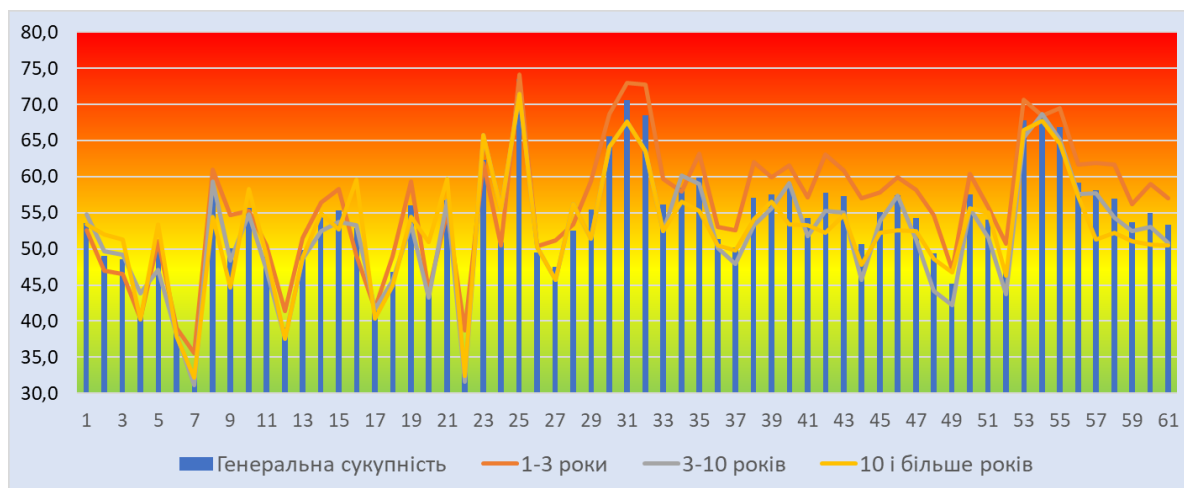


Рис. 3.2 Варіативність оцінювання кіберзагроз за експертною вибіркою щодо досвіду фахової діяльності у сфері кібербезпеки

Зазначений підхід вказує на необхідність у подальшому більш глибокого аналізу кіберзагроз із врахуванням особливостей експертної вибірки. Саме такий підхід дає можливості більш глибоко досліджувати тенденції поширення кіберзагроз на основі ризик-орієнтованого підходу, і як наслідок більш обґрунтовано підходити до формування стратегічних напрямів у сфері

кібербезпеки та враховувати специфіку й певну особливість думок експертного середовища [66, с.72].

Таким чином, сучасна кібербезпека потребує комплексного підходу, що включає розвиток кіберстійкості, управління ризиками та стратегічний аналіз загроз. Головним інструментом є ризик-орієнтований підхід, що базується на зборі та обробці аналітичних даних. Україна активно розвиває державну політику у сфері кібербезпеки, імплементуючи міжнародні стандарти. Дослідження показують, що оцінка кіберзагроз варіюється залежно від досвіду та спеціалізації експертів. Важливим є врахування регіональних та галузевих особливостей, що дозволяє формувати ефективні механізми захисту. Створення прогностичних моделей, заснованих на статистичному та регресійному аналізі, є ключовим етапом у боротьбі з кіберзлочинністю. Розвиток наукового супроводу, використання технологій аналізу великих даних та залучення широкого кола експертів сприятимуть посиленню кіберстійкості держави та суспільства [26; 66].

3.2. Обґрунтування стратегічних напрямів кіберстійкості на основі аналізу кіберзагроз

Продовжуючи аналіз, із врахуванням висновків попереднього розділу (3.1.), для більш обґрунтованого визначення пріоритетів щодо розробки стратегічних напрямів кіберстійкості в Україні, із врахуванням сучасних викликів, зосередимо увагу на визначенні ключових кіберзагроз за рівнем ризику їх поширення, із врахуванням думки експертів на основі вибірки за досвідом їх фахової діяльності у сфері кібербезпеки.

Для аналізу кіберзагроз ми використали певне групування за їх однорідністю, зокрема:

- *кіберзагрози класифіковані за порушенням базових характеристик захищеності (безпеки);*

- різновиди кібератак;
- кібератаки на об'єкти розподілені за специфікою сфери (галузі);
- використання кібератак як елементу гібридної війни проти України;
- використання кібератак у якості деструктивних інформаційно-психологічних операцій (ІПСО);
- кібертероризм росії проти України.

Аналіз ризиків кіберзагроз, класифікованих за порушення базових характеристик захищеності (безпеки) (табл. 3.9), дозволяє зробити кілька важливих висновків щодо пріоритетності різних видів загроз у контексті базових характеристик безпеки.

Таблиця 3.9

Рівень ризику кіберзагроз, пов'язаних з порушенням базових характеристик захищеності, із врахуванням експертного досвіду

Кіберзагрози класифіковані за порушенням базових характеристик захищеності (безпеки):	Досвід			
	Середнє, %	1-3 роки	3-10 років	більше 10 років
порушення конфіденційності (розголошення даних)	53,62	52,53	54,82	53,44
порушення цілісності (неавторизована модифікація)	49,08	47,01	49,66	52,02
порушення доступності (недоступні сервіси)	48,54	46,49	49,19	51,32
порушення достовірності (не істинні / не коректні дані)	41,69	40,30	43,88	40,18
порушення надійності (система не може виконувати функцію / функції)	49,97	51,08	47,11	53,34
порушення спостережуваності (не можливо визначити поточний стан системи)	38,41	39,01	38,09	37,85
відмову від авторства (не достовірні дані щодо користувача / автора)	33,13	35,55	31,16	32,19

Найбільш значущими загрозами є ті, що пов'язані з порушенням конфіденційності, цілісності, доступності та надійності систем. Зокрема, ризик порушення конфіденційності (розголошення даних) складає 53,62%, що вказує на високий рівень загрози для приватності користувачів та організацій. Порушення цілісності (неавторизовані модифікації) також має високий рівень ризику (52,02%), оскільки несанкціоновані зміни в даних можуть призвести до серйозних наслідків для надійності інформації. Окрім того, порушення доступності (недоступність сервісів) (51,32%) є критичним ризиком, оскільки він може паралізувати роботу організації або сервісу, спричиняючи зупинку критичних функцій. Порушення надійності (коли система не може виконувати свої функції) має ризик 53,34%, що свідчить про серйозні наслідки для

організацій, де порушення в роботі системи може призвести до значних труднощів або навіть повної зупинки роботи.

З іншого боку, ризик деяких інших загроз є меншим. Порушення достовірності даних (неістинні чи некоректні дані) має менший рівень ризику – 40,18%. Хоча це може призвести до помилок і неточностей, такі наслідки не завжди є настільки критичними, як порушення інших базових характеристик безпеки. Аналогічно, порушення спостережуваності (неможливість визначити поточний стан системи) з ризиком 37,85% є менш значущою загрозою, оскільки хоча важливо мати прозорість щодо стану системи, відсутність цієї прозорості не завжди веде до негайних і серйозних наслідків. Що стосується відмови від авторства (недостовірні дані про користувача чи автора), то цей ризик є ще нижчим – лише 32,19%, хоча підробка ідентифікаційних даних може мати юридичні наслідки, її ймовірність впливу на систему є порівняно низькою.

Отже, загалом можемо зазначити, що найбільшу увагу варто приділяти захисту від загроз, що порушують конфіденційність, цілісність, доступність та надійність систем, оскільки ці загрози мають високий рівень ризику (вище 50%). Водночас, менш критичними є загрози, пов'язані з достовірністю даних, спостережуваністю та відмовою від авторства, де ризики не перевищують 40%.

Водночас, для детального аналізу ризику поширення кіберзагроз за рівнем досвіду експертних груп, варто звернути увагу на зміни в оцінках ризиків у залежності від того, який досвід мають учасники. Зауважимо, що ризики можуть оцінюватися по-різному для експертів з різним досвідом, зокрема для груп з 1-3 роками, 3-10 роками та більше 10 років досвіду.

Різний рівень ризику для різних типів загроз може бути зумовлений специфікою самих загроз та їх впливом на організацію. Загрози, пов'язані з *конфіденційністю* і *цілісністю* (53,62 % та 49,08 % відповідно) даних, зазвичай вважаються більш серйозними, оскільки їх порушення може мати катастрофічні наслідки для організації, включаючи втрату довіри клієнтів,

фінансові санкції, або витік персональних даних. Тому експерти з більшим досвідом можуть оцінювати ці загрози як більш ймовірні та критичні (53,44 % та 52,02 % відповідно), враховуючи попередній досвід роботи з подібними ситуаціями. З іншого боку, загрози *спостережуваності* чи *відмови від авторства* (38,41 % та 33,13 % відповідно) можуть виглядати менш загрозливими через їх менший вплив на функціональність систем, і це може призвести до того, що їх ризик буде знижено у порівнянні з іншими.

В результаті аналізу ризиків поширення кіберзагроз серед різних груп експертів з різним досвідом можна зробити кілька важливих висновків. Для групи з 1-3 роками досвіду характерна більш обережна або навіть перебільшена оцінка ризиків, оскільки ці експерти ще не мають достатньо практичного досвіду і схильні бути надзвичайно обережними, оцінюючи потенційні загрози. Це може бути пов'язано з їх прагненням уникнути потенційних загроз через невеликий досвід у реальних ситуаціях. Вони ще можуть не розрізняти потенціал різних типів загроз і схильні оцінювати їх як більш критичні.

З іншого боку, експерти з досвідом 3-10 років, які вже зіштовхувалися з різними ситуаціями, зазвичай мають більш збалансовані оцінки, оскільки здатні розрізняти реальні загрози і оцінювати їх ймовірність на основі практичного досвіду. Вони вже знайомі з різними типами загроз і розуміють, які з них є більш ймовірними в реальних умовах. Такі експерти, ймовірно, мають краще розуміння того, що деякі загрози можуть бути менш серйозними, ніж вони здаються на перший погляд. Це дозволяє їм знижувати оцінку ризиків порівняно з менш досвідченими колегами.

Водночас експерти з більш ніж 10 роками досвіду можуть мати схильність до більш високої оцінки ризиків, оскільки вони ретельно враховують навіть менш ймовірні загрози, спираючись на великий досвід роботи з різними інцидентами і розвитком технологій. Вони мають більш глибоке розуміння як наслідків загроз, так і нових викликів, які можуть виникати в майбутньому.

Загалом, відмінність в оцінках ризиків серед експертних груп з різним досвідом зумовлена глибиною розуміння загроз, рівнем обізнаності та досвідом вирішення реальних інцидентів. Тому для кожної групи важливо враховувати не лише їх рівень досвіду, а й характер самих загроз, щоб сформулювати максимально точну і ефективну стратегію управління ризиками.

Враховуючи попередній аналіз ризиків кіберзагроз, можна сформулювати кілька пріоритетів для стратегування кіберстійкості в Україні. Ці пріоритети повинні бути спрямовані на мінімізацію найбільших ризиків для національної безпеки, економіки та інфраструктури, з урахуванням реальних загроз, які можуть виникнути в умовах сучасних кіберзагроз. Зокрема,

1. Забезпечення конфіденційності та захисту персональних даних.

Оскільки порушення конфіденційності (розголошення даних) має один з найвищих рівнів ризику (53,62%), цей аспект має стати основним пріоритетом у визначенні стратегічного напрямку кіберстійкості в Україні. У зв'язку з цим необхідно посилити механізми захисту персональних даних, розробити чіткі правила обробки, зберігання та передачі інформації, а також забезпечити суворі штрафи та санкції для порушників. Важливо також забезпечити надійне шифрування та захист інформації від несанкціонованого доступу, зокрема в умовах постійних кібероперацій і кібератак.

2. Посилення захисту цілісності та доступності інформаційних систем.

Оскільки ризики, пов'язані з порушенням цілісності (неавторизовані модифікації) та доступності (недоступність сервісів), оцінюються як дуже високі (52,02% і 51,32% відповідно), важливо розробити стратегії для мінімізації цих загроз. Це включає впровадження систем захисту від DDoS-атак, регулярне оновлення програмного забезпечення, а також розробку планів аварійного відновлення для збереження безперебійної роботи критичних державних і комерційних систем. Окрім того, слід забезпечити захист від несанкціонованих змін даних, створюючи механізми моніторингу та виявлення будь-яких змін у критичних системах.

3. Посилення надійності національної інфраструктури.

Враховуючи високий ризик порушення надійності (53,34%) систем, ключовим пріоритетом є забезпечення надійності критичних інфраструктур. Потрібно розробити та впровадити стратегії з резервування та дублювання важливих функцій і послуг, щоб навіть у разі технічних збоїв чи атак система могла продовжувати виконувати свої функції. Системи мають бути стійкими до внутрішніх і зовнішніх загроз, а також повинні мати механізми для автоматичного відновлення в разі порушень.

4. Покращення моніторингу та спостережуваності систем.

Зважаючи на менший, але все ж важливий ризик порушення спостережуваності (37,85%), слід розвивати можливості для моніторингу стану інформаційних систем в реальному часі. Це включає використання сучасних інструментів для виявлення аномальних або підозрілих дій, автоматичну генерацію звітів про інциденти та аналіз даних для прогнозування потенційних атак. Стратегічні плани мають включати також впровадження стандартів для прозорості в діяльності державних і приватних компаній у сфері кібербезпеки.

5. Покращення виявлення та запобігання фальсифікації даних.

Необхідно звернути увагу на загрози, пов'язані з відмовою від авторства (недостовірні дані щодо користувачів/авторів), хоча ризик цієї загрози є відносно меншим (32,19%). Проте, зважаючи на важливість забезпечення достовірності даних у цифрову епоху, треба розвивати стратегії, що забезпечують автентифікацію та підписання даних, а також запобігання підробці цифрових ідентифікацій. Це може включати вдосконалення технологій верифікації та підтвердження авторства для важливих документів і транзакцій.

6. Розвиток людського капіталу в сфері кібербезпеки.

Одним з ключових аспектів є підготовка та навчання фахівців з кібербезпеки. Необхідно інвестувати в підвищення кваліфікації спеціалістів, які зможуть ефективно реагувати на нові та складні загрози. Оскільки різні

рівні досвіду експертів можуть призводити до різних оцінок ризиків, важливо забезпечити безперервне навчання та обмін досвідом між різними групами фахівців для підвищення загальної компетенції в цій галузі.

7. Розробка національної політики кібербезпеки.

Крім технічних аспектів, вкрай важливо розробити чітку національну політику кібербезпеки, що включає не лише правові та організаційні заходи, але й міжнародну співпрацю для боротьби з транснаціональними кіберзагрозами. Це включає розвиток стандартів і норм для захисту державних та приватних систем, а також активну участь у міжнародних ініціативах з кібербезпеки.

Таким чином, пріоритетні напрями формування кіберстійкості в Україні повинні бути націлені на мінімізацію найзначніших ризиків, таких як порушення конфіденційності, цілісності та доступності інформаційних систем. Потрібно посилити захист критичної інфраструктури, забезпечити надійність і стійкість систем, а також впровадити ефективні механізми моніторингу і запобігання фальсифікації даних. Успішна реалізація цих пріоритетів дозволить Україні забезпечити високий рівень кібербезпеки на національному рівні і знизити вразливість перед зовнішніми та внутрішніми загрозами.

Аналізуючи дані про ризики поширення різних типів кібератак, можна визначити, які загрози є найзначнішими, а які – менш важливими. За даними (табл. 3.10), загрози з ризиком більше 50% є найзначнішими і вимагають особливої уваги у формуванні кіберстійкості.

Шкідливе програмне забезпечення (Malware) має найвищий ризик поширення – 58,99%. Це свідчить про те, що шкідливі програми є одними з найбільш поширених кіберзагроз і можуть мати серйозний вплив на системи, викликаючи витік даних, знищення інформації або захоплення контролю над комп'ютерами.

Іншою значущою загрозою є фішинг (Phishing) з ризиком 55,73%. Фішинг є популярною технікою для отримання доступу до конфіденційних

даних користувачів через обман, що може призвести до серйозних фінансових втрат або втрати приватності.

Таблиця 3.10

Кіберзагрози за видами кібератак, із врахуванням експертного досвіду

Кібератаки за видами:	Досвід			
	Середнє, %	1-3 роки	3-10 років	більше 10 років
Шкідливе програмне забезпечення (Malware)	58,99	60,99	59,30	54,45
Веб-атаки (Web-based Attacks)	50,11	54,64	48,36	44,64
Фішинг (Phishing)	55,73	55,31	54,82	58,30
Атаки на веб-додатки (Web application attacks)	48,85	50,46	47,11	49,09
Спам (Spam)	39,13	41,43	37,62	37,55
Атака на відмову в обслуговуванні (Denial of service)	49,87	51,55	48,67	48,89
Крадіжки особистих даних (Identity theft)	54,55	56,45	52,42	54,96
Злом (порушення) даних (Data breaches)	55,36	58,26	53,78	52,73
Інсайдерська загроза (Insider threat)	52,92	49,12	53,31	59,62
Ботнети (Botnets)	41,40	41,74	41,58	40,38
Фізичне втручання, пошкодження, крадіжки та втрати (Physical manipulation, damage, theft and loss)	46,81	48,97	45,60	44,94
Витік інформації (Information leakage)	55,98	59,29	53,41	54,45
Програма вимагач (Ransomware)	45,18	44,17	43,25	50,91
Кібершпигунство (Cyberespionage)	56,68	55,11	56,70	59,72
Криптоджекінг (шкідливий майнінг) (Cryptojacking)	34,59	38,70	31,58	32,39

Також важливими загрозами є злом (порушення) даних (Data breaches) з ризиком 55,36% та крадіжка особистих даних (Identity theft), яка має ризик 54,55%. Оскільки ці атаки призводять до витоку або крадіжки конфіденційної інформації, вони можуть мати масштабні наслідки для приватних осіб і організацій, зокрема в аспектах фінансових втрат і репутаційних пошкоджень.

Ще однією важливою загрозою є витік інформації (Information leakage), що має ризик 55,98%. Ця загроза є особливо важливою в контексті корпоративної безпеки, оскільки навіть незначний витік може призвести до серйозних наслідків для бізнесу.

Кібершпигунство (Cyberespionage) з ризиком 56,68% також є однією з найбільших загроз, оскільки воно може призвести до витоку важливої або навіть секретної інформації, що створює серйозні проблеми для національної безпеки.

Окрім високих ризиків, є також загрози з меншим його рівнем, тобто з ризиком менше 50%. Це, зокрема, атаки на веб-додатки (Web application

attacks), ризик яких становить 48,85%. Хоча ці атаки можуть мати негативний вплив, їх рівень ризику є меншим порівняно з іншими загрозами, але все одно їх не можна ігнорувати.

Атака на відмову в обслуговуванні (Denial of Service) має ризик 49,87%, що також вказує на досить високий потенціал для порушення доступності сервісів, хоча така атака зазвичай має тимчасовий характер. Інсайдерська загроза (Insider threat) з ризиком 52,92% – це менш поширена загроза, але вона все одно є серйозною, оскільки може бути важко виявлена.

Програма-вимагач (Ransomware), хоча й має ризик 45,18%, є дуже актуальною, оскільки може спричинити серйозні фінансові втрати і втрату даних, але її поширення є менш вірогідним порівняно з іншими загрозами.

Загрози, які мають найменший ризик поширення, включають фізичне втручання, пошкодження, крадіжки та втрати з ризиком 46,81%, а також спам з ризиком 39,13%. Хоча ці загрози можуть створювати проблеми, їх вплив є менш серйозним порівняно з іншими типами атак.

Найменший ризик поширення має криптоджекінг (шкідливий майнінг), що має ризик 34,59%. Ця загроза є найменш ймовірною, але може спричинити фінансові втрати через використання ресурсів для незаконного майнінгу криптовалют.

Отже, загрози, що мають найвищий рівень ризику, включають шкідливе програмне забезпечення, фішинг, злом даних, крадіжки особистих даних, витік інформації та кібершпигунство, тому вимагають пріоритетної уваги в стратегіях кіберстійкості. Водночас, загрози з меншим рівнем ризику, такі як атаки на веб-додатки, DDoS-атаки, інсайдерські загрози і програми-вимагачі, все одно потребують заходів щодо запобігання та захисту.

Аналізуючи ризик кібератак за різними експертними групами, із врахуванням досвіду, ми можемо виявити різницю в оцінці цих загроз в залежності від того, скільки часу кожен експерт працює в галузі кібербезпеки. Це дозволяє зрозуміти, чому ризик для різних груп може варіюватися.

Експерти з 1-3 роками досвіду оцінюють ризик більшою мірою з позиції актуальних загроз, які вони зустрічали у своїй практиці. Вони можуть бути більш чутливими до нових типів атак, таких як шкідливе програмне забезпечення та фішинг, які активно поширюються, оскільки ці атаки є частими в їхньому досвіді. Наприклад, шкідливе програмне забезпечення має для цієї групи найвищий рівень ризику – 60,99%, оскільки вони часто стикаються з новими варіантами шкідливих програм, що розповсюджуються через електронну пошту або вебсайти.

Експерти з досвідом 3-10 років мають більш глибоке розуміння кіберзагроз, тому вони можуть оцінювати ризик з урахуванням більш загальної картини загроз в організаціях та національному рівні. Вони також звертають увагу на такі загрози, як фішинг (54,82%), крадіжка особистих даних (52,42%), злом даних (53,78%) та кібершпигунство (56,7%), оскільки вони вже мають досвід виявлення та аналізу складніших атак, орієнтуючись на більш тривалі та цілеспрямовані кампанії атак. Ці загрози оцінюються як значущі через їхній довготривалий характер і здатність чинити великий вплив на безпеку.

Експерти з більш ніж 10-річним досвідом мають досвід боротьби з найскладнішими та найнебезпечнішими загрозами, зокрема кібершпигунством, яке оцінюється в них як дуже серйозна загроза з рівнем ризику 59,72%. Вони більш схильні бачити ширшу картину загроз, включаючи атаку на відмову в обслуговуванні і атаку на веб-додатки (Web application attacks), де на перший план виходить важливість забезпечення відмовостійкості і захисту критичної інфраструктури. Вони також розглядають інсайдерські загрози, оскільки такі загрози можуть бути важко виявити та вони мають тривалий характер.

Це пояснюється тим, що експерти з більшим досвідом мають більше практичного досвіду в управлінні складними ситуаціями і кризовими ситуаціями, які включають не тільки технічні аспекти, а й стратегії та організаційні проблеми. Це дає їм більш чітке розуміння довготривалих

наслідків атак, таких як кібершпигунство чи інсайдерські загрози, оскільки вони здатні оцінити потенційний масштаб цих атак з точки зору стратегічної загрози для національної безпеки чи корпоративної репутації.

Водночас, експерти з меншим досвідом можуть більше зосереджуватися на сучасних і поширених загрозах, таких як фішинг та шкідливе програмне забезпечення, тому що ці загрози часто зустрічаються у їхній практиці. Вони менш схильні до аналізу більш складних або специфічних загроз, які можуть бути менш очевидними, наприклад, атаки, що пов'язані з інсайдерами або високотехнологічні загрози.

Зміни в оцінці ризику можна пояснити тим, що з досвідом експерти розвивають більш детальне розуміння як технічних аспектів, так і загрози в більш широкому контексті – від тактики атаки до стратегії управління інцидентами. Більш досвідчені аналітики можуть прогнозувати потенційні наслідки атак, розуміють важливість багаторівневих систем безпеки і здатні оцінювати стратегії, які мають довгостроковий ефект, а не тільки миттєві наслідки.

У результаті ми бачимо, що оцінка ризику кіберзагроз за різними експертними групами залежить від рівня досвіду і способу їхнього мислення. Менш досвідчені експерти зосереджуються на нових і широко поширених загрозах, таких як фішинг та шкідливе програмне забезпечення, тоді як більш досвідчені фахівці розглядають більш складні й довготривалі загрози, такі як кібершпигунство, інсайдерські загрози та атаки на інфраструктуру.

Враховуючи попередній аналіз оцінки ризиків кібератак за різними групами експертів, а також виявлені відмінності в їхніх оцінках за рівнем досвіду, можна сформулювати додаткові пріоритети для розробки стратегічних напрямів кіберстійкості в Україні, зокрема:

1. Пріоритет на захист від шкідливого програмного забезпечення та фішингу.

На основі аналізу ризиків, шкідливе програмне забезпечення та фішинг є найбільш розповсюдженими загрозами, зокрема серед молодших експертів з

1-3 роками досвіду. Це означає, що ці загрози є найбільш актуальними на сьогодні для широкого спектра організацій та приватних користувачів в Україні. Стратегії кібербезпеки повинні зосереджуватися на посиленні заходів для боротьби з цими типами атак:

- розширення та вдосконалення системи виявлення та захисту від шкідливого програмного забезпечення;
- впровадження комплексних тренінгів для співробітників з виявлення фішингових атак;
- розробка і впровадження спеціалізованих інструментів для виявлення і блокування фішингових кампаній.

2. Захист від крадіжки даних та зломів інформаційних систем.

Крадіжка особистих даних та зломи даних є серйозними загрозами, що виявилися найбільш значущими для більш досвідчених експертів (3-10 років та більше 10 років досвіду). Оскільки ці загрози можуть призвести до серйозних наслідків для безпеки національних інтересів, критичної інфраструктури та особистих даних громадян, стратегія має включати:

- створення та впровадження комплексних механізмів захисту даних, особливо у сфері фінансів, охорони здоров'я та інших критичних секторах;
- вдосконалення нормативної бази для забезпечення захисту персональних даних та запобігання витокам даних;
- використання багаторівневого підходу до безпеки, включаючи шифрування даних та регулярні перевірки на вразливості.

3. Пріоритет на захист інфраструктури від кібершпигунства та інсайдерських загроз.

Для експертів з досвідом більше 10 років важливими загрозами є кібершпигунство та інсайдерські загрози. Це особливо важливо в контексті національної безпеки, де стратегічні і політичні дані можуть бути піддані ризику витоку або маніпулювання. Таким чином стратегії кіберстійкості повинні зосереджуватися на:

- підвищення рівня захисту критичної інфраструктури, включаючи енергетичний сектор, транспортні мережі та державні органи;
- впровадження політик контролю доступу до чутливої інформації в організаціях, зокрема в державних установах;
- створення спеціальних підрозділів для моніторингу і реагування на інсайдерські загрози, а також розробка стратегій для мінімізації ризику зловживань зсередини організацій.

4. Посилення захисту від атак на веб-додатки та DDoS-атак.

Атаки на веб-додатки та атаки на відмову в обслуговуванні (DDoS) оцінюються як значущі загрози з більш високим ризиком у групах з досвідом 3-10 років. Ці загрози можуть вплинути на доступність веб-сервісів, що є критичним для функціонування державних та комерційних систем в Україні. Для боротьби з цими загрозами стратегія має включати:

- вдосконалення захисту веб-додатків за допомогою сучасних інструментів виявлення вразливостей та миттєвого реагування;
- розробка та впровадження заходів для захисту від DDoS-атак, включаючи системи виявлення і блокування таких атак в реальному часі;
- створення резервних планів для забезпечення доступності важливих державних і комерційних онлайн-сервісів у разі кібернападів.

5. Впровадження нових технологій та інструментів для боротьби з криптоджекінгом.

Попри те, що криптоджекінг є менш значущою загрозою з оцінкою ризику 34,59%, ця загроза має тенденцію до зростання через розвиток криптовалют та майнінгових технологій. З огляду на це стратегії кібербезпеки повинні враховувати нові типи атак:

- впровадження механізмів моніторингу та аналізу активності на комп'ютерах і мережах для виявлення аномалій, пов'язаних з майнінгом криптовалют;
- співпраця з правоохоронними органами та іншими країнами для виявлення та ліквідації мереж майнінгових ботнетів;

6. Підвищення обізнаності та навчання для зниження ризиків від популярних загроз.

Оскільки фішинг, шкідливе програмне забезпечення і витік інформації мають високий ризик поширення, важливим аспектом є освітні програми для населення, співробітників державних установ і компаній, а тому пріоритети включають:

- організацію регулярних тренінгів і кампаній з підвищення обізнаності серед користувачів;
- впровадження політик для забезпечення належного використання захищених каналів зв'язку, а також систем автентифікації.

Таким чином, необхідно сконцентруватися на посиленні захисту від найбільш розповсюджених загроз (шкідливе програмне забезпечення, фішинг, злом даних), одночасно враховуючи важливість захисту національної інфраструктури від більш складних загроз, таких як інсайдерські загрози та кібершпигунство. Крім того, важливо вдосконалювати механізми для боротьби з новими технологіями атак, такими як криптоджекінг.

Аналізуючи ризики кібератак на різні об'єкти інфраструктури, можна виокремити декілька ключових моментів (табл. 3.11). Згідно з оцінкою ризику, енергетичний комплекс, фінансовий сектор, оборонно-промисловий комплекс та державна безпека є найзначнішими об'єктами з точки зору кіберзагроз. Ці сектори мають високий рівень ризику, і тому вони потребують найвищого пріоритету в рамках стратегії кібербезпеки.

Водночас менш значущими загрозами є атаки на забезпечення питною водою, суспільно важливі інформаційні ресурси та транспортну систему, хоча й вони потребують уваги, але меншої у порівнянні з іншими критичними секторами.

Більш детальний узагальнений підхід дає можливість також виділити певні особливості. Найбільший ризик від кібератак спостерігається в енергетичному комплексі, де рівень ризику становить 73,50%. Цей сектор є надзвичайно критичним для функціонування країни, оскільки будь-які

порушення в енергетичних мережах можуть призвести до масштабних перебоїв з електропостачанням, що вплине на всі інші галузі економіки і національну безпеку. Ще одним критичним сектором є оборонно-промисловий комплекс, ризик для якого становить 70,58%. Атаки на ці об'єкти можуть призвести до серйозних наслідків для обороноздатності країни, оскільки забезпечення оборони є одним з основних пріоритетів для безпеки держави.

Таблиця 3.11

Рівень ризиків щодо кібератак, із врахуванням експертного досвіду

Кібератаки на об'єкти:	Досвід			
	Середнє, %	1-3 роки	3-10 років	більше 10 років
телекомунікаційних послуг	62,37	61,87	65,79	64,64
транспортної системи	50,90	50,46	55,47	56,33
енергетичного комплексу	73,50	74,20	71,46	72,21
забезпечення питною водою	49,47	50,31	50,30	51,52
суспільно важливих інформаційних ресурсів	47,51	51,14	45,65	46,45
системи управління технологічними процесами	52,51	53,35	56,17	56,88
органів державної влади	55,40	59,29	51,42	51,71
фінансового та банківського сектору	65,57	68,73	64,07	64,08
оборонно-промислового комплексу	70,58	72,96	67,61	67,50
державної безпеки	68,52	72,76	63,56	63,43
правоохоронних органів	56,18	59,75	52,43	53,00

Фінансовий та банківський сектор з ризиком 65,57% також є однією з найзначніших загроз. Атаки на цей сектор можуть викликати серйозні економічні наслідки, включаючи порушення платіжних систем, фінансові збитки і зниження довіри до банківської системи. Державна безпека оцінюється з ризиком 68,52%. Кібератаки на органи державної безпеки можуть серйозно порушити роботу систем розвідки, контррозвідки і національної безпеки, що матиме негативні наслідки для цілісності держави. Телекомунікаційний сектор з ризиком у 62,37%. Телекомунікації є основою для зв'язку між різними секторами державної і приватної сфер, тому атаки на ці системи можуть серйозно порушити обмін інформацією, що має критичне значення для національної безпеки та ефективного функціонування країни.

Менш значущими загрозами виступають атаки на правоохоронні органи (56,18%) і системи управління технологічними процесами (52,51%). Хоча ці сектори є важливими для забезпечення правопорядку та технологічної безпеки, рівень їхнього ризику не перевищує 60%, що означає меншу ймовірність серйозних наслідків порівняно з іншими критичними об'єктами.

Транспортна система (50,90%) та забезпечення питною водою (49,47%) мають менш високий ризик, але атаки на ці сектори можуть створити значні проблеми в повсякденному житті громадян, призводячи до порушень в транспортних перевезеннях чи доступі до життєво важливих ресурсів.

Найменший рівень ризику спостерігається для суспільно важливих інформаційних ресурсів (47,51%), що вказує на меншу ймовірність масштабних атак, проте ці системи все одно потребують уваги для запобігання потенційним загрозам.

Продовжуючи розгляд відмінностей в оцінці ризиків поширення кіберзагроз серед експертних груп за рівнем досвіду, важливо звернути увагу на кілька додаткових аспектів, які можуть впливати на ці відмінності.

Більш досвідчені експерти, наприклад, більш зважено оцінюють ризик кібератак на об'єкти енергетичного комплексу (71,46% – 72,21%) та суспільно важливих інформаційних ресурсів (45,65% - 46,45%), у порівнянні з молодшими працівниками (74,2% та 51,14% відповідно). Маючи багатший досвід, вони можуть точніше оцінювати рівень загрози, ґрунтуючись на своїх знаннях про історичні випадки атак, специфічні вразливості та потенційні наслідки для критичних інфраструктур. Вони також можуть бути більш обережними і готовими до швидкого реагування на нові, навіть менш очевидні загрози.

З досвідом приходить більш глибоке розуміння специфічних слабкостей у кожному секторі, що дозволяє досвідченим експертам точніше оцінювати ризики для конкретних об'єктів інфраструктури. Досвідчені спеціалісти, швидше за все, мають досвід в оцінці довгострокових тенденцій в області кібербезпеки. Вони можуть прогнозувати зміни в типах атак і розвитку загроз,

враховуючи як швидко змінюється технологічний ландшафт. Вони більше фокусуються на потенційних уразливостях, які можуть виникнути в майбутньому через зміну технічних умов чи розвиток нових технологій. Молодші спеціалісти можуть мати обмежений досвід у виявленні довгострокових загроз і врахуванні специфічних аспектів інфраструктури, що підвищує або знижує її вразливість. Наприклад, молодші спеціалісти можуть недооцінювати складність атак на транспортну систему (50,46% у порівнянні з ризиком 55,47% – 56,33% на думку більш досвідчених працівників), вважаючи її менш уразливою до кіберзагроз порівняно з іншими секторами, такими як фінансовий (68,52% у порівнянні з ризиком 64,07% – 64,08% на думку більш досвідчених працівників).

Більш кваліфіковані працівники розуміють важливість того, щоб бути готовими до більш складних, «невидимих» загроз, що можуть виникнути внаслідок інновацій в області кіберзагроз. Це спричиняє вищу оцінку ризику для об'єктів телекомунікаційних послуг (65,79% – 64,64%) та транспортної системи (55,47% – 56,33%), де атаки можуть мати складні наслідки, у порівнянні з менш досвідченими (61,87% – 50,46%), вважаючи їх менш уразливими або більш захищеними від атак. Вони мають досвід у виявленні неочевидних вразливостей, які можуть бути непомітними для менш досвідчених спеціалістів. Наприклад, вони можуть знати про можливість кібератак через новітні методи фішингу чи програмне забезпечення, яке інші могли б не врахувати. Вони усвідомлюють важливість забезпечення функціонування цих об'єктів для економічної стабільності та національної безпеки, тому вони більш схильні оцінювати ці загрози як найважливіші.

Як правило, працівники з більшим фаховим досвідом у сфері кібербезпеки мають доступ до більш широкої інформації про нові кіберзагрози, інноваційні методи атак, зміну тактики злоумисників та кіберзагрози, які з'являються внаслідок технологічних інновацій. Вони можуть передбачати розвиток атак, які спричиняють нові виклики для безпеки в конкретних секторах. Наприклад, вплив штучного інтелекту на методи атак

чи поширення нових типів шкідливого програмного забезпечення можуть бути відомими лише досвідченим спеціалістам, які вже стикаються з подібними проблемами в інших контекстах. Водночас, вони також можуть бути більш обізнаними в питаннях застосування новітніх технологій для кіберзахисту, що дозволяє їм точніше прогнозувати розвиток кіберзагроз у майбутньому. Більш досвідчені експерти можуть застосовувати складніші методи аналізу та реагування на кіберзагрози, використовуючи перевірені стратегії та технології для нейтралізації загроз.

Підсумовуючи, можна стверджувати, що різниця в оцінці ризику поширення кіберзагроз серед експертів різного рівня досвіду в основному зумовлена різницею в глибині розуміння загроз, наявності досвіду в реальних ситуаціях, здатності передбачати майбутні зміни в технологіях і розвитку кіберзагроз. Досвідчені експерти, завдяки своєму багаторічному досвіду, можуть точніше оцінити ризики і передбачити потенційні загрози, тоді як нові експерти можуть мати схильність недооцінювати або спрощувати ці загрози через обмежене розуміння і досвід. І з врахуванням зазначеного, можна сформулювати низку пріоритетів для розробки кіберстійкості в Україні. Ці пріоритети мають враховувати як сучасні загрози, так і можливі майбутні виклики, особливо з урахуванням розвитку новітніх технологій. Зокрема:

1. Посилення захисту критичної інфраструктури. Стратегічні сектори, такі як енергетичний комплекс, оборонно-промисловий комплекс, фінансові установи та системи управління технологічними процесами, повинні стати основою для розвитку національної кібербезпеки. Оскільки ці сектори отримали високі оцінки ризику поширення атак, важливо забезпечити їх надійний захист від кіберзагроз. Це включає посилення систем моніторингу, запровадження ефективних заходів для боротьби з новими видами атак (наприклад, шкідливим програмним забезпеченням, фішингом, атаками на веб-додатки).

2. Розвиток системи раннього попередження та реагування на загрози передбачає впровадження передових технологій для раннього виявлення

кіберзагроз, таких як штучний інтелект та аналіз великих даних. Досвідчені експерти зазначають важливість виявлення і реагування на загрози ще на ранніх етапах. Це дозволить знизити можливі наслідки від атак і забезпечити швидке відновлення в разі інцидентів.

3. Підвищення кваліфікації та розвиток кадрів у сфері кібербезпеки. Враховуючи відмінності в оцінках ризиків серед експертів різного рівня досвіду, необхідно розробити програми підвищення кваліфікації для спеціалістів з кібербезпеки на всіх рівнях. Інвестиції в навчання та професійний розвиток дозволять не лише підвищити загальний рівень знань серед нових спеціалістів, а й забезпечити кращу підготовленість до боротьби з новими видами загроз. Важливо створити постійно діючу систему для оновлення знань відповідно до нових викликів і тенденцій у сфері кіберзагроз.

4. Забезпечення взаємодії між державними органами та приватним сектором передбачає формування налагодженої ефективної взаємодії між державними органами, приватними компаніями та міжнародними партнерами для обміну інформацією про кіберзагрози та уразливості. Оскільки кіберзагрози мають глобальний характер, важливо створити платформу для взаємодії і координації дій з урахуванням специфіки різних секторів економіки. Спільні зусилля дозволять швидше реагувати на загрози та ефективно їх нейтралізувати.

5. Інвестування в інноваційні технології та дослідження забезпечує активне залучення наукових установ і технологічних компаній до досліджень у сфері кібербезпеки та розробки нових інструментів захисту. З урахуванням швидкого розвитку технологій, таких як штучний інтелект та машинне навчання, необхідно інвестувати в дослідження і розробку нових рішень для боротьби з кіберзагрозами. Це допоможе Україні залишатися на крок попереду від потенційних зловмисників.

6. Адаптація політик безпеки до нових реалій цифрової трансформації, зокрема розвитку Інтернету речей (IoT), 5G та інших новітніх технологій. Нові технології несуть з собою як великі можливості, так і нові виклики в сфері

кібербезпеки. Оцінка та врахування цих загроз має стати важливим елементом стратегії кібербезпеки України.

7. Створення національної кіберзахисної стратегії з чіткими стандартами. Стратегія кіберстійкості повинна включати розробку стандартів і протоколів для захисту критичних об'єктів, а також впровадження єдиних підходів до реагування на кіберінциденти. Ці стандарти мають бути адаптовані до сучасних викликів і підтримувати використання найкращих міжнародних практик у галузі кібербезпеки. Окрім того, важливо забезпечити постійну адаптацію стратегії з урахуванням розвитку технологій та змін у зовнішньополітичній ситуації.

Таким чином, для забезпечення національної безпеки та стійкості до кіберзагроз Україна повинна зосередитися на розвитку комплексної стратегії кіберстійкості, яка враховує не тільки технічні аспекти, а й організаційні, кадрові та правові складові. Важливо інвестувати в новітні технології, забезпечити захист критичної інфраструктури, покращити підготовку кадрів і сприяти міжнародній співпраці для протидії кіберзагрозам. Такий підхід дозволить створити надійний захист для країни та її громадян в умовах швидко змінюваного кіберсередовища.

Подальший аналіз зосереджується на виділенні найбільш значущих загроз, що використовуються як елемент гібридної війни проти України. Цей аналіз дозволяє визначити основні пріоритети для захисту від кібератак, спрямованих на інформаційну та політичну стабільність України, а також підкреслює важливість зміцнення міжнародної підтримки та боротьби з пропагандою в рамках гібридної війни (табл. 3.12).

Перша значуща загроза – це дискредитація військово-політичного керівництва України, для якої середній рівень ризику становить 59,91%. Цей тип атак є важливим елементом гібридної війни, оскільки підрив авторитету керівництва може серйозно вплинути на внутрішню політичну стабільність і міжнародне сприйняття України. Іншою суттєвою загрозою є поширення в світі ідей «руського світу», який оцінено на рівні 57,57%. Ці ідеї

використовуються як інструмент пропаганди для створення проросійських настроїв на міжнародній арені. Ще однією важливою загрозою є зниження світової підтримки України, де рівень ризику становить 58,46%. Кібератаки, спрямовані на підлив міжнародної підтримки, є важливим інструментом ослаблення України, оскільки без міжнародної підтримки країна вразлива до економічного та політичного тиску.

Таблиця 3.12

Ризики використання кібератак у гібридній війні, із врахуванням експертного досвіду

Використання кібератак як елементу гібридної війни проти України з метою:	Досвід			
	Середнє, %	1-3 роки	3-10 років	більше 10 років
зниження світової підтримки України	58,46	57,89	60,13	56,53
дискредитації військово-політичного керівництва України	59,91	63,16	58,98	55,26
інспірування міжнародних конфліктів на кордонах України	51,40	53,06	50,11	50,53
інспірування міжнародного тиску на Україну	50,20	52,58	47,88	49,79
інспірування розколу в українській владі	57,02	61,98	53,32	54,11
поширення в світі ідей т.зв. «руського світу»	57,57	59,88	55,66	56,53

Не менш важливим є інспірування розколу в українській владі, де ризик оцінюється на рівні 57,02%. Подібні кібератаки можуть призвести до внутрішнього розбрату та політичної дестабілізації, що є однією з основних цілей гібридної війни. Менш значущими є загрози, пов'язані з інспіруванням міжнародного тиску на Україну (50,20%) та інспіруванням міжнародних конфліктів на кордонах України (51,40%). Обидві ці загрози мають рівень ризику, що трохи перевищує 50%, але оцінка їх значущості не є такою високою, як у попередніх випадках. Вони вважаються менш актуальними у довгостроковій перспективі, оскільки міжнародні контрзаходи і адаптація політичних стратегій можуть знизити їх ефективність.

Таким чином, найбільш значущими загрозами є ті, що стосуються дискредитації політичного керівництва, поширення ідей «руського світу», зниження світової підтримки України та розколу в українській владі. Всі ці

загрози пов'язані із психологічними та інформаційними аспектами гібридної війни, і вони мають високу значущість у короткостроковій та середньостроковій перспективі.

Аналізуючи ризик поширення кібератак на основі вибірки з експертних груп за рівнем досвіду, можна виявити, що оцінки ризику можуть значно варіюватися залежно від досвіду експертів. Важливою частиною будь-якої стратегії кіберстійкості є адекватна оцінка потенційних загроз і ризиків. Знову ж таки, якщо різні групи експертів оцінюють ці загрози по-різному, це може призвести до неповних або неефективних стратегій. Для більш точного прогнозування важливо враховувати різні аспекти ризику та застосовувати комплексний підхід, який поєднує технічні, соціальні, політичні і стратегічні компоненти. Об'єднання досвіду нових і досвідчених експертів дозволяє створити більш збалансовану і об'єктивну картину ризиків. Молодші експерти можуть внести свіжий погляд і нові технологічні рішення, в той час як досвідчені фахівці здатні надати історичну та стратегічну перспективу, що дозволяє створювати більш точні прогнози і визначати пріоритети в розробці стратегії кіберстійкості.

В оцінювання ризиків кібератак як елементу гібридної війни прослідковується тенденція більш високого рівня ризику за оцінкою менш досвідчених фахівців (з досвідом 1-3 роки фахової діяльності у сфері кібербезпеки). І у більшості випадків цей ризик є вищим від середнього, наприклад, дискредитація військово-політичного керівництва України (63,16% у порівнянні з 59,91%) чи інспірування розколу в українській владі (61,98% у порівнянні з 57,02%). Для нових експертів, які мають лише кілька років досвіду, часто важко оцінити повний спектр кіберзагроз, особливо в контексті глобальних і довготривалих атак. Їх оцінки можуть бути менш обґрунтованими через обмежену практику та недостатнє розуміння складних, багатофакторних атак, таких як гібридні війни або інформаційні кампанії. Молодші експерти можуть не мати повного розуміння комплексних кібератак, таких як дискредитація військово-політичного керівництва (61,98% у

порівнянні з 57,02%) чи поширення ідей «руського світу» (59,88% у порівнянні з 57,57%). Ці загрози часто не є прямими технічними атаками, а більше мають інформаційний та психологічний характер, що може бути складно для новачків виявити або оцінити на основі лише технічних знань.

Гібридні атаки, такі як дискредитація політичного керівництва, поширення ідей «руського світу» та інші форми інформаційних кампаній, складно піддаються кількісному оцінюванню, що може ускладнити їх оцінку для молодших експертів. Ці атаки часто мають непрямий ефект, що потребує глибшого розуміння психології та соціальної динаміки, а також здатності відстежувати та аналізувати довгострокові тенденції в суспільних настроях.

Досвідчені експерти, які працюють у сфері кібербезпеки більше 10 років, мають глибше розуміння загроз та можуть передбачити можливі напрямки еволюції атак. Вони можуть оцінювати ризик більш обґрунтовано, враховуючи тенденції з минулого та актуальність нових атак. Вони можуть схилитися до більш обережних оцінок, оскільки знають, що ризики можуть змінюватися з часом, а прогнозування в довгостроковій перспективі завжди є складним завданням. Саме тому в оцінювання ризиків кібератак як елементу гібридної війни прослідковується тенденція меншого рівня ризику за оцінкою більш досвідчених фахівців. І у більшості випадків цей ризик є нижчим від середнього, наприклад, дискредитація військово-політичного керівництва України (55,26% у порівнянні з 59,91%) чи інспірування розколу в українській владі (54,11% у порівнянні з 57,02%).

Саме тому для точного оцінювання кіберзагроз важливо об'єднувати підходи з різним досвідом та перспективами, оскільки кожна група експертів може внести важливі аспекти в оцінку загроз. Враховуючи попередній аналіз оцінювання ризиків кіберзагроз та фактори, що впливають на їх оцінювання залежно від досвіду експертів, можна сформулювати пріоритети для розробки стратегії кіберстійкості в Україні, зокрема:

- 1. Посилення заходів протидії гібридним загрозам*

Оскільки високий ризик оцінюється для загроз, які використовують кіберзагрози в якості елементів гібридної війни (зниження світової підтримки України, інспірування розколу в українській владі, дискредитація військово-політичного керівництва), потрібно розробити стратегії кіберзахисту, які включають не тільки технічні, але й інформаційні та психологічні контрзаходи. Важливим аспектом є боротьба з дезінформацією та контрпропагандою на міжнародному рівні, що повинно включати активну взаємодію з міжнародними партнерами.

2. Впровадження стратегії інформаційної війни.

Враховуючи, що кібератаки часто використовуються як елемент гібридної війни, стратегія кіберстійкості повинна включати в себе заходи для протидії інформаційним маніпуляціям. Це включає захист від атак на політичне керівництво, поширення ідей «руського світу», а також інспірування міжнародних конфліктів. У цій сфері важливо створити потужну систему моніторингу та реагування на інформаційні атаки, які можуть впливати на внутрішню і міжнародну політику.

3. Розвиток інфраструктури для захисту від гібридних атак.

Аналіз ризиків також показує, що атаки, спрямовані на політичну дискредитацію і внутрішні конфлікти в країні, мають високий рівень загрози (до 62% у випадку інспірування розколу в українській владі та інші). Тому важливо забезпечити координацію між державними і приватними організаціями для протидії таким атакам. Це включає вдосконалення механізмів захисту від фальшування інформації, а також посилення протидії фішингу, спаму та іншої дезінформації.

4. Забезпечення прозорості та відкритості інформації.

Іншою важливою складовою стратегії має бути робота з підвищення прозорості і відкритості даних, аби уникнути маніпулювання інформацією. Створення механізмів для швидкої і вірогідної перевірки джерел інформації дозволить знизити вплив інформаційних кібератак, а також зміцнити довіру громадян до органів влади.

5. Посилення національної кіберрозвідки.

Оскільки кібератаки часто мають складну, багатозначну природу, стратегія кіберстійкості повинна включати створення спеціалізованих органів з кіберрозвідки. Ці органи повинні здійснювати постійний моніторинг кіберпростору, виявляти потенційні загрози та надавати оперативну інформацію про можливі атаки. Також важливо співпрацювати з міжнародними організаціями для обміну даними і прогнозування кіберзагроз.

Аналізуючи дані щодо використання кібератак як елементу деструктивних інформаційно-психологічних операцій (ІПСО), можна виокремити кілька найзначніших загроз, що становлять високий ризик для України (табл. 3.13). Найбільш значущими є загрози, спрямовані на дискредитацію органів влади та підриг їхніх повноважень, з рівнем ризику 58,91%. Це свідчить про те, що кібератаки, спрямовані на ослаблення державних інституцій, можуть мати серйозні наслідки для стабільності країни.

Таблиця 3.13

Ризики використання деструктивних ІПСО, із врахуванням експертного досвіду

Використання кібератак у якості деструктивних інформаційно-психологічних операцій (ІПСО) з метою:	Досвід			
	Середнє, %	1-3 роки	3-10 років	більше 10 років
дискредитації органів влади та підриг владних повноважень	58,91	61,53	59,15	53,37
соціально-політичної поляризації суспільства	54,24	57,08	51,77	53,26
інспірування суспільної недовіри до органів влади	57,81	63,05	55,32	52,21
негативного впливу на настрої в українському суспільстві	57,34	60,88	55,03	54,74
підбурювання до акцій громадянської непокори (демонстрації, мітинги)	50,69	56,97	45,65	47,79
дискредитації СОУ	55,12	57,84	53,83	52,21
деморалізації о/с СОУ	57,39	59,96	57,32	52,53
поширення антиукраїнських настроїв	54,31	58,17	51,26	52,42
розпалювання міжнаціональної ворожнечі	49,39	54,69	44,22	48,63
розпалювання міжрелігійної ворожнечі	45,17	47,15	42,22	46,74
розповсюдження проросійського наративу	57,54	60,34	55,66	55,58
нагнітання соціально-економічної напруги через економічні інструменти	54,00	55,78	51,54	55,05
провокації порушення громадського порядку	47,10	50,73	43,71	46,32

Ще однією значною загрозою є інспірування суспільної недовіри до органів влади, де рівень ризику досягає 57,81%. Цей тип кібератак має на меті знищення довіри громадян до влади, що може підригати основи демократичної системи. Аналогічно, негативний вплив на настрої в

українському суспільстві з ризиком 57,34% вказує на те, що маніпуляції громадською думкою через кібератаки можуть мати довгострокові дестабілізуючі наслідки.

Розповсюдження проросійського нарративу також є серйозною загрозою з оцінкою 57,54%. Цей напрямок свідчить про спроби впливати на громадську думку не тільки всередині країни, але й за її межами, сприяючи підвищенню рівня антиукраїнських настроїв. Інші значущі загрози включають соціально-політичну поляризацію суспільства (54,24%) та підбурювання до акцій громадянської непокорності (50,69%), що свідчить про високий ризик ескалації протестних настроїв та порушень громадського порядку в Україні.

Водночас, деякі загрози мають менш виражену деструктивну силу. Наприклад, розпалювання міжнаціональної ворожнечі (49,39%) і міжрелігійної ворожнечі (45,17%) є менш серйозними порівняно з іншими загрозами, хоча можуть мати негативні наслідки в окремих соціальних чи етнічних групах. Також меншою є загроза провокацій порушення громадського порядку (47,10%), хоча така діяльність здатна тимчасово дестабілізувати ситуацію.

Загалом, найбільше занепокоєння викликають кібератаки, спрямовані на піддрив довіри до органів влади, маніпуляцію громадськими настроями та розповсюдження проросійського нарративу. Водночас загрози, пов'язані з міжнаціональними чи міжрелігійними конфліктами, хоча й мають певний рівень ризику, не є настільки критичними у порівнянні з іншими видами атак.

І знову прослідковується тенденція в оцінюванні ризиків кібератак у якості деструктивних інформаційно-психологічних операцій (ІПСО) більш високого рівня ризику за оцінкою менш досвідчених фахівців (з досвідом 1-3 роки фахової діяльності у сфері кібербезпеки). І у більшості випадків цей ризик є вищим від середнього, наприклад, дискредитація органів влади та піддрив владних повноважень (61,53% у порівнянні з 58,91%) чи інспірування суспільної недовіри до органів влади (63,05% у порівнянні з 57,81%). Їх оцінки є значно вищими і негативного впливу на настрої в українському суспільстві

(60,88% у порівнянні з 57,34%) чи розповсюдження проросійського нарративу (60,34% у порівнянні з 57,54%). Ці загрози більше мають інформаційний та психологічний характер, що може бути складно для новачків виявити або оцінити на основі лише технічних знань.

Досвідчені експерти, які працюють у сфері кібербезпеки більше 10 років, схиляються до більш обережних оцінок, оскільки знають, що ризики можуть змінюватися з часом, а прогнозування в довгостроковій перспективі завжди є складним завданням. Саме тому в оцінювання ризиків кібератак у якості деструктивних інформаційно-психологічних операцій (ІПСО) прослідковується тенденція меншого рівня ризику за оцінкою більш досвідчених фахівців. І у більшості випадків цей ризик є нижчим від середнього, наприклад, дискредитація Сил оборони України (СОУ) (52,21% у порівнянні з 55,12%) чи деморалізація особового складу СОУ (52,53% у порівнянні з 57,39%). Експерти з більш ніж 10-річним досвідом вважають, що Збройні Сили України, а також силові структури, уже мають достатньо механізмів для підтримки високого рівня морального духу та протидії деморалізації через інформаційні війни. Вони розуміють, що такі організації мають досвід боротьби з психологічними операціями і є стійкими до інформаційних атак, що намагаються знизити їх ефективність або моральний дух.

Загалом, експерти з більшим досвідом оцінюють стійкість та здатність українського суспільства протистояти антиукраїнським настроям через багаторічний досвід реагування на інформаційні атаки, що спрямовані на послаблення національної ідентичності. Вони враховують, що в Україні вже є розвинена система моніторингу та реагування на дезінформацію, а також значні зусилля з боку держави та неурядових організацій, спрямовані на зміцнення національного спротиву та боротьбу з ворожою пропагандою.

Із врахуванням цього аналізу можливим є доповнення пріоритетних напрямів щодо розбудови кібербстійкості в Україні такими:

1. Посилення інформаційної безпеки та протидії інформаційним атакам. Ризик поширення антиукраїнських наративів, дискредитація органів влади та розповсюдження проросійського наративу є одними з найбільших загроз для України. Інформаційні атаки, що включають фальшиві новини, пропаганду, та кібератаки на медіа-платформи, можуть сильно вплинути на міжнародний імідж країни і на соціальну згуртованість. Тому необхідно розробити стратегії для активного моніторингу медіапростору, оперативного реагування на інформаційні атаки та створення контрзаходів для захисту національного інформаційного простору, включати навчання і підготовку спеціалістів з кібербезпеки для боротьби з інформаційними атаками.

Покращення механізмів реагування на інформаційно-психологічні операції та кібератаки, спрямовані на внутрішню політичну стабільність. Деструктивні інформаційно-психологічні операції, що спрямовані на підрив стабільності всередині країни, можуть спричинити соціально-політичну поляризацію, підбурювання до акцій громадянської непокори, і навіть спровокувати внутрішні конфлікти. Розробка та впровадження механізмів, що дозволяють швидко виявляти та нейтралізувати кіберзагрози, які спричиняють внутрішньополітичні та соціальні конфлікти, є важливою складовою кіберстійкості у суспільстві.

Таким чином, пріоритети щодо кіберстійкості в Україні мають бути орієнтовані на зміцнення національної безпеки в умовах гібридних війн, інформаційних атак і кіберзагроз. Вони повинні охоплювати всі рівні, від національної інфраструктури до персональної безпеки громадян, і сприяти інтеграції національних зусиль.

Аналіз ризиків кібертероризму з боку росії проти України показує, що найбільш значущими загрозами є ті, що пов'язані з атакою на критичну інфраструктуру країни (табл. 3.14). Зокрема, загроза завдання шкоди інформаційним системам, комп'ютерним та телекомунікаційним мережам має найвищий рівень ризику – 67,77%. Атаки на ці системи можуть паралізувати основні функції держави, зокрема в енергетичному, транспортному та

комунікаційному секторах, що має критичне значення для національної безпеки.

Наступною важливою загрозою є створення надзвичайної ситуації техногенного характеру з ризиком 68,42%. Такі атаки можуть призвести до аварій і катастроф, що мають серйозні наслідки для життя громадян, економіки та стабільності країни. Блокування роботи систем життєзабезпечення (66,85%) також є великою загрозою, оскільки це може призвести до порушень у наданні основних послуг, таких як енергопостачання, водопостачання та інші критичні функції.

Таблиця 3.14

Ризики кібертероризму, із врахуванням експертного досвіду

Кібертероризм росії проти України з метою:	Досвід			
	Середнє, %	1-3 роки	3-10 років	більше 10 років
завдання шкоди інформаційним системам, комп'ютерним та телекомунікаційним мережам	67,77	70,68	65,41	66,48
створення надзвичайної ситуації техногенного характеру	68,42	68,48	68,72	67,73
блокування роботи систем життєзабезпечення	66,85	69,50	65,23	64,65
створення кризових явищ у певних галузях або сферах	59,16	61,63	57,60	57,21
масової загибелі людей	58,10	61,86	57,72	51,26
порушення стабільності в суспільстві	56,90	61,63	54,35	52,29
викликання широкого суспільного резонансу та розголосу	53,67	56,14	52,45	51,03
викликання соціального невдоволення	55,01	59,03	53,10	50,57
злякування населення, створення атмосфери незахищеності та загрози повторення акту кібертероризму	53,30	57,05	50,86	50,46

Створення кризових явищ у певних галузях або сферах (59,16%) є менш безпосередньо загрозливим, однак ця загроза має великий потенціал для довгострокового впливу на економіку і соціальну стабільність України. Також важливою є загроза масової загибелі людей (58,10%), хоча її ймовірність дещо нижча, порівняно з іншими типами атак, вона все одно може бути частиною більш масштабних кібертерористичних атак.

Загроза порушення стабільності в суспільстві (56,90%) є серйозною, адже атаки можуть спричинити соціальне невдоволення, яке призведе до політичної та соціальної дестабілізації. Це також стосується викликання широкого суспільного резонансу та розголосу (53,67%), що хоч і може мати

тимчасовий ефект, але посилює загальну атмосферу невизначеності і стресу серед населення.

Менш суттєвими є загрози викликання соціального невдоволення (55,01%) та створення атмосфери незахищеності (53,30%). Вони, хоч і можуть мати певний вплив на громадську думку та соціальні настрої, не є настільки руйнівними для державної безпеки порівняно з атаками на фізичну інфраструктуру.

На основі цього аналізу можна стверджувати, що найвищі пріоритети в стратегії кіберстійкості повинні бути спрямовані на захист критичних інфраструктурних систем, таких як енергетика, телекомунікації, транспор та життєзабезпечення. Також потрібно акцентувати увагу на забезпеченні національної безпеки в разі техногенних катастроф та створенні ефективних засобів реагування на кібертерористичні атаки, спрямовані на порушення стабільності в суспільстві та державних інститутах.

Аналіз ризику поширення кіберзагроз із урахуванням вибірки експертних груп за рівнем досвіду дозволяє виявити важливі відмінності в оцінці загроз. Експерти з меншим досвідом оцінюють рівень загрози як більш значущий, оскільки вони часто стикаються з безпосередніми, практичними проблемами, наприклад, завдання шкоди інформаційним системам, комп'ютерним та телекомунікаційним мережам (70,68%), блокування роботи систем життєзабезпечення (69,5%) чи викликання соціального невдоволення (59,03%). Це може бути результатом недавніх змін у технологіях чи невеликих, але реальних інцидентів, які викликали увагу у цих експертів. Вони можуть мати більшу схильність до реакції на конкретні, вже виявлені проблеми, ніж до оцінки потенційної шкоди в майбутньому. Молодші експерти можуть бути більш орієнтовані на технічні аспекти кібербезпеки. Вони можуть бути більш чутливими до технічних проблем і загроз, з якими стикаються безпосередньо в їхній роботі, таких як хакерські атаки або зараження мереж шкідливим ПЗ. Це може відображати актуальні проблеми, з якими вони зустрічаються в реальному часі.

Для досвідчених експертів (більше 10 років) ризик деяких загроз ще нижчий. Наприклад, завдання шкоди інформаційним системам, комп'ютерним та телекомунікаційним мережам (66,48%), блокування роботи систем життєзабезпечення (64,65%) чи викликання соціального невдоволення (50,57%). Це може бути пов'язано з їхнім глибоким розумінням як технічних, так і організаційних аспектів кіберзахисту. Досвідчені експерти більше довіряють стабільним, перевіреним методам захисту, які застосовуються для нейтралізації більшості загроз. Їхня оцінка може бути менш чутливою до деяких видів атак, оскільки вони зазвичай мають змогу передбачити зміни в характері загроз та застосувати нові стратегії захисту. Досвідчені експерти, можливо, з часом виявили, що такі загрози, як соціальне невдоволення, є більше питанням довгострокової стабільності та політичних процесів, а не безпосереднім результатом кібертероризму. Крім того, досвідчені спеціалісти можуть оцінювати вплив кібертероризму як менш потужний для тривалих змін у суспільному порядку, оскільки більшість кризових ситуацій з часом можуть бути подолані за допомогою розвинених заходів кібербезпеки.

Враховуючи аналіз, можна сформулювати кілька ключових додаткових пріоритетів щодо розбудови кіберстійкості в Україні, які повинні орієнтуватися на оцінку ризиків, які були визначені на основі даних експертної групи.

Зміцнення інфраструктури критичних секторів.

Враховуючи високий ризик кібертероризму, спрямованого на об'єкти інфраструктури, особливо енергетичний комплекс, транспортну систему, фінансові та банківські установи, необхідно акцентувати увагу на посиленні захисту цих секторів. Особливу увагу слід приділити технологічним системам, що забезпечують життєдіяльність держави, таких як системи життєзабезпечення, та розробити спеціалізовані плани реагування на можливі кіберінциденти в цих сферах.

Інтеграція кіберзахисту в національну безпеку.

Оскільки кібертероризм може мати серйозні наслідки для національної безпеки, стратегія кібербезпеки повинна бути інтегрована в загальний контекст національної безпеки країни. Це включає співпрацю між державними органами, військовими структурами, правоохоронними органами і приватними компаніями, що спеціалізуються на кіберзахисті. Зміцнення національних органів кібербезпеки повинно стати пріоритетом для забезпечення ефективної оборони від зовнішніх і внутрішніх загроз.

Таким чином, узагальнюючи викладене, основними пріоритетами для розбудови кіберстійкості України є зміцнення захисту критичної інфраструктури, посилення боротьби з кібертероризмом та гібридними загрозами, а також розвиток технологій, підвищення кваліфікації кадрів і інтеграція кібербезпеки в систему національної безпеки. Україні важливо мати системний підхід до кіберзахисту, орієнтуючись на ефективну інтеграцію технологій, стандартів, освітніх програм і міжнародної співпраці для збереження стабільності в умовах сучасних кіберзагроз.

3.3. Методологічні засади та діагностика кіберстійкості національної інформаційної інфраструктури

Зростаюча залежність громадян, бізнесу та суспільства від кіберінфраструктури поставила національну безпеку під значний ризик непередбачуваних і невідомих загроз. Високий рівень взаємозв'язку в сучасному суспільстві відкрив багато шляхів для кібератак, в тому числі внутрішні та зовнішні загрози і вразливості в мережах ланцюгів постачання [218]. Як наслідок, маломасштабні шкідливі програми, доступні на чорному ринку, завдають шкоди, неспівмірної з їхньою вартістю та складністю. Більше того, швидке розгортання передових технологій для розподілу критично важливих послуг (наприклад, електроенергії) свідчить про те, що в майбутньому атаки на інфраструктуру можуть мати руйнівні наслідки

для громадянського суспільства [394]. Незважаючи на постійний прогрес в управлінні ризиками в кіберпросторі, очевидно, що передбачення і запобігання всім можливим атакам і збоям в роботі неможливе для нинішніх або майбутніх інфраструктурних кіберсистем [28, с. 133].

У сучасних умовах перманентної цифрової конфронтації концепт «кіберстійкість» набуває статусу фундаментальної категорії національної безпеки. На відміну від традиційного розуміння кібербезпеки, яка фокусується переважно на створенні захисного бар'єру навколо інформаційних активів, кіберстійкість визначає здатність складної системи не лише протистояти деструктивному впливу, а й зберігати цілісність під тиском. Як вже було з'ясовано у попередніх розділах, сутність стійкості полягає у переході до динамічної моделі життєздатності, що охоплює чотири критичні стадії: передбачення загроз, поглинання зовнішніх стресів без втрати системних функцій, швидке відновлення після інциденту та адаптація через вивчення отриманого досвіду. Об'єктивною передумовою актуалізації цього концепту є зростаюча залежність критичних сервісів держави від цифрової інфраструктури, де будь-який простій трансформується у значні економічні збитки та соціальну напругу. Таким чином, кіберстійкість є інтегральною характеристикою системи, що дозволяє їй функціонувати в умовах неминучої компрометації окремих її сегментів.

За визначенням (Merriam-Webster) [367], стійкість – це здатність відновлюватися після нещастя або легко пристосовуватися до змін. У системах, що надають критично важливі послуги, стійкість характеризується чотирма можливостями: планувати/готуватися, поглинати, відновлюватися та адаптуватися до відомих і невідомих загроз [225; 282]. Впровадження комплексного плану забезпечення стійкості кіберінфраструктури систем має на меті зменшити потенційні збитки та сприяти швидкому відновленню після атаки. Однак, сучасні концепції та методи, що обговорюються як способи підвищення стійкості, часто об'єднують стійкість (тобто здатність протистояти і швидко відновлюватися після невідомих і відомих загроз) і ризик (тобто,

добуток ймовірності настання несприятливої події та величини спричиненої нею шкоди [301, с. 19]). Зокрема, регуляторні органи закликають до розробки та впровадження стандартів, заснованих на оцінці ризиків, для захисту критичної інфраструктури від кіберзагроз, проте підходи, що базуються на оцінці ризиків, не обов'язково створюють стійкість [351, с. 362]. Натомість, стійкі системи повинні використовувати узагальнюючі концепції, що відрізняються від оцінки ризиків, але доповнюють її, для інформування і підтримки співпраці між різними відомствами, відповідальними за критично важливі об'єкти інфраструктури. Більше того, додаткова плутанина виникає через змішування надійності і стійкості, пов'язаних між собою але різних властивостей систем. Надійність означає ступінь, до якого система здатна протистояти неочікуваним внутрішнім чи зовнішнім подіям або змінам без погіршення продуктивності системи [197]. Стійкість, з іншого боку, відноситься до здатності системи відновлювати або регенерувати свою продуктивність після неочікуваного впливу, що призводить до погіршення її роботи. З цієї причини необхідно вжити заходів для використання більш узагальнених концепцій стійкості та їх інтеграції з підходами до управління, що базуються на ризик-орієнтованому підході [28, с.133-134].

Більше того, обговорення стійкості, що зустрічаються в літературі, часто зосереджені на одній операційній області (напр., фізичній, інформаційній, когнітивній або соціальній) і не відображають взаємозв'язки між компонентами системи для інформування в цих сферах. В інженерній літературі методи оцінки стійкості часто зосереджуються на мережах, що складаються з однорідних елементів (наприклад, мережа комунікаційних пристроїв або мережі соціальних істот). Реальні мережі складаються з технологічних, соціологічних, екологічних та економічних компонентів таким чином, що комбінація взаємопов'язаних фізичних елементів, пристроїв зв'язку, людей і сил навколишнього середовища утворюють єдине ціле [273, с. 280-282]. Стійкість є властивістю всієї системи і повинна оцінюватися відповідно. Наприклад, у випадку атаки, система може повідомити про стан і

дії окремих комп'ютерів і серверів (фізичний домен). Інформація повинна ефективно та оперативно передаватися відповідним особам, які приймають рішення, які використовують цю інформацію для оцінки шкоди і визначення відповідної реакції на атаку (когнітивна сфера). Визначивши осіб, які приймають рішення, і делегуючи системні ресурси конкретним особам, можна чітко визначити, хто повинен діяти на основі інформації, що надходить з фізичного домену. Стійкість системи значною мірою залежить від ефективності міждоменної комунікації та координації на кожному етапі циклу управління [28, с.134].

Водночас, науковий аналіз потребує чіткого розмежування понять «вразливість» та «стійкість», оскільки вони відображають різні вектори стратегічного мислення. У зарубіжній науковій літературі [269; 271] запропоновано вразливість визначати як невід'ємну властивість певної системи (наприклад, фізична, технічна, організаційна та культурна), що може використовуватися супротивником для негативного впливу (заподіяння шкоди або збитків) на цю систему. Разом з вразливістю розглядається термін «намір», під яким розуміється бажання або мотивація супротивника атакувати ціль і спричинити несприятливі наслідки. Зокрема наголошується на дефініції «спроможність», яка пояснюється здатністю і спроможністю атакувати ціль і спричинити несприятливі наслідки.

Тобто, вразливість (англ. vulnerability) – це слабкі місця, які можуть бути використані для нанесення шкоди системі, організації, чи навіть цілим суспільствам. Водночас, вразливість системи в кіберпросторі – це слабе місце або недолік у системі, програмному забезпеченні, процесах або людському факторі, яке може бути використане зловмисниками для нанесення шкоди або несанкціонованого доступу.

У контексті кібербезпеки, вразливості можуть включати:

- технічні вразливості: *програмні помилки, незахищені мережеві протоколи, недостатні механізми аутентифікації;*

- вразливості пов'язані з процесом основної діяльності: *недостатні або застарілі політики безпеки, відсутність регулярних аудитів безпеки, неналежна підготовка та навчання персоналу, відсутність планів реагування на інциденти;*

- фізичні вразливості: *недостатня захищеність фізичних об'єктів, відсутність контролю доступу до критичних елементів інфраструктури;*

- людський фактор: *відсутність обізнаності щодо кібербезпеки, недбалість у поводженні з конфіденційною інформацією, психологічні атаки, фішинг тощо.*

Прикладами такої ситуації можуть бути – вразливість в операційній системі, яка дозволяє зловмиснику отримати доступ адміністратора, або недоліки в конфігурації веб-сервера, які можуть бути використані для SQL-ін'єкцій.

Таким чином, парадигма вразливості зосереджена на внутрішніх дефектах системи: слабких місцях у коді, архітектурі чи людському чиннику, що можуть бути використані зловмисником. Такий підхід має реактивний характер, оскільки спрямований на «закриття дір» та мінімізацію площини атаки.

Натомість концепція кіберстійкості переміщує фокус уваги на безперервність функціонування критичних процесів. В межах цієї дихотомії стійкість не заперечує наявності вразливостей, але пропонує механізми їх нейтралізації через надмірність ресурсів, сегментацію та автономність підсистем.

У кібербезпеці стійкість передбачає [23, с. 40]:

- проактивні заходи: *виявлення та усунення вразливостей до того, як вони будуть використані; регулярне оновлення систем і програмного забезпечення; проведення навчань та тестування на проникнення;*

- реактивні заходи: *ефективне та швидке реагування на інциденти; наявність планів реагування на інциденти та відновлення; моніторинг і аналіз подій безпеки в режимі реального часу;*

- відновлення: здатність швидко відновлюватися після інцидентів; мінімізація простоїв і зниження втрат; проведення післяінцидентного аналізу для поліпшення процесів;

- адаптація: постійне вдосконалення процесів безпеки на основі отриманих уроків; гнучкість у зміні стратегій та підходів у відповідь на нові загрози; використання передових технологій і практик для підвищення захищеності.

Прикладами кіберстійкості може бути система, яка автоматично виявляє та блокує підозрілі дії до того, як вони завдадуть шкоди, або організація, яка має чітко визначений план дій на випадок кібератаки і може швидко відновити нормальну роботу після інциденту.

Узагальнення визначених аспектів подано у таблиці у формі порівняння (табл. 3.15).

Таблиця 3.15

Порівняння характерних аспектів вразливості кіберсистеми та кіберстійкості

Аспект	Вразливість системи	Кіберстійкість
Фокус	Визначення та усунення слабких місць	Забезпечення безперервності та швидкого відновлення
Проактивні заходи	Виявлення та усунення вразливостей	Виявлення загроз, навчання персоналу, оновлення систем
Реактивні заходи	Усунення наслідків після використання вразливості	Ефективне реагування на інциденти, моніторинг
Відновлення	Не є основним фокусом	Швидке відновлення після інцидентів, мінімізація простоїв
Адаптація	Вразливості можуть повторюватися, якщо не усунути	Постійне вдосконалення на основі отриманих уроків
Підхід	Реактивний, орієнтований на окремі слабкі місця	Комплексний, орієнтований на безперервність та гнучкість
Приклади методів	Оновлення, налаштування безпеки	План реагування на інциденти, резервне копіювання, симуляції

Причинами всечастішого використання цих термінів є те, що сучасні загрози стають більш складними та координованими, що вимагає глибшого розуміння вразливостей та розробки стійких стратегій захисту. Кіберзлочинці використовують нові методи атаки, тому організації повинні постійно адаптуватися, щоб бути стійкими до нових загроз. Регуляторні органи та стандарти безпеки постійно оновлюються, щоб відповідати новим викликам, що вимагає від організацій оцінювати свої вразливості та підвищувати стійкість.

Крім того, аналіз великих кібератак показує, що відсутність стійкості може мати катастрофічні наслідки для організацій та суспільств в цілому. Саме тому зі збільшенням залежності від цифрових технологій, важливо забезпечити стійкість цих технологій до різних видів загроз.

Порівняльний аналіз свідчить, що якщо стратегія «мінімізації вразливостей» прагне ідеальної захищеності, то стратегія «забезпечення стійкості» прагне максимальної витривалості. У нашій методології це підтверджується тезою про те, що стійка система спроможна поглинати удар навіть тоді, коли вразливість була успішно експлуатована.

Загалом, використання термінів «вразливість» та «стійкість» підкреслює важливість комплексного підходу до безпеки, який включає не лише захист від атак, але й готовність до них, швидке реагування та ефективне відновлення. Це дозволяє забезпечити безперервність бізнес-процесів та мінімізувати негативні наслідки від потенційних інцидентів.

Таким чином, вразливість системи та кіберстійкість – це два взаємопов'язані, але відмінні аспекти кібербезпеки. Вразливість зосереджується на ідентифікації та усуненні слабких місць, тоді як кіберстійкість охоплює здатність системи протистояти, адаптуватися та швидко відновлюватися після кібератак або інших інцидентів. Разом вони складають комплексний підхід до забезпечення безпеки в кіберпросторі.

Водночас робляться різні спроби визначити і кількісно оцінити вразливість і стійкість особливо в аналізі ризиків.

Можемо зазначити, що стійкість системи є проявом властивостей системи. Стійкість – це вектор, який залежить від часу. Водночас стійкість визначається як здатність системи витримувати серйозні порушення в межах прийнятних параметрів деградації та відновлюватися в межах прийнятного часу та сукупних витрат і ризиків. [412, с. 293]

Крім того, розглядаючи стійкість, можна стверджувати, що стійкість аналогічна до вразливості, а саме: її не можна просто виміряти в єдиній одиниці виміру; її важливість полягає в кінцевих багатовимірних результатах (наслідках) системи для будь-яких конкретних впливів (загроз). У даному контексті варто звернути увагу, що наслідок, який розглядається як частина вимірювання ризику, насправді є вихідною точкою моделі системи і, що вхідна точка моделі системи є паралельним до поняття загрози.

Досліджуючи окреслену проблему, зауважимо, що ризик, пов'язаний з кібератакою на систему кіберінфраструктури, дійсно, буде залежати не тільки від стійкості системи, але й від типу та складності кібератаки. Це пояснюється тим, що стійкість системи можна виміряти лише з точки зору конкретної загрози (вхідного сигналу) і часу відновлення системи, а також пов'язаних з нею сукупних витрат і ризиків. Таким чином, різні атаки призведуть до різних наслідків (вихідних траєкторій) для однієї й тієї ж стійкої системи. [269]

При оцінюванні ризиків терміни «вразливість системи» та «кіберстійкість» займають ключові ролі, але підходять до цього з різних сторін. Вразливість системи визначає потенційні точки, через які загрози можуть бути реалізовані. У контексті оцінювання ризиків, вразливість передбачає врахування наступних аспектів:

- ідентифікацію ризиків: *вразливості є вихідними даними для виявлення ризиків; знання про існуючі вразливості дозволяє прогнозувати, які загрози можуть бути реалізовані та з якими наслідками;*

- аналіз ризиків: оцінка вразливостей допомагає визначити ймовірність реалізації ризиків та можливий вплив на організацію; це включає як кількісний (вірогідність реалізації вразливості), так і якісний аналіз (потенційний вплив на систему);

- пріоритизацію заходів: на основі виявлених вразливостей можна розставити пріоритети для заходів з безпеки; вразливості з високим рівнем ризику вимагають першочергової уваги та ресурсів для їх усунення.

Водночас у контексті оцінювання ризиків кіберстійкість передбачає наступні аспекти:

- зниження ймовірності реалізації ризиків: включає заходи, що спрямовані на зменшення ймовірності реалізації вразливостей; це проактивні заходи, такі як регулярне оновлення програмного забезпечення та систем, моніторинг кіберзагроз;

- мінімізацію впливу ризиків: оцінка кіберстійкості допомагає визначити, наскільки швидко та ефективно організація зможе відновитися після інциденту; це включає наявність планів відновлення, систем резервного копіювання, навчання персоналу;

- вдосконалення процесів: постійний аналіз та вдосконалення процесів кіберстійкості дозволяють організації адаптуватися до нових загроз та змін у зовнішньому середовищі; це включає післяінцидентний аналіз та впровадження отриманих уроків.

Порівняльний аналіз у контексті оцінювання ризиків подано у таблиці 3.16.

Таким чином, у контексті оцінювання ризиків, терміни «вразливість системи» та «кіберстійкість» виконують різні, але взаємодоповнюючі ролі. Вразливість системи допомагає виявити та оцінити ризики тоді як кіберстійкість визначає здатність організації протистояти цим ризикам та ефективно відновлюватися після інцидентів. Комплексний підхід до оцінювання ризиків включає як виявлення та усунення вразливостей, так і

розвиток стійкості для забезпечення безпеки та безперервності бізнес-процесів.

Таблиця 3.16

Порівняння характерних аспектів вразливості кіберсистеми та кіберстійкості у контексті оцінювання ризиків

Аспект	Вразливість системи	Кіберстійкість
Фокус	Ідентифікація слабких місць, через які можуть бути реалізовані ризики	Протистояння, адаптація та відновлення після реалізації ризиків
Роль у процесі оцінювання	Вихідні дані для ідентифікації та аналізу ризиків	Заходи для зниження ймовірності та мінімізації впливу ризиків
Підхід	Реактивний: фокус на виявленні та усуненні слабких місць	Проактивний та реактивний: фокус на підготовці, реагуванні та відновленні
Взаємозв'язок	Оцінка вразливостей дозволяє визначити потенційні ризики	Врахування кіберстійкості дозволяє мінімізувати вплив та швидко відновлюватися після ризиків
Приклади заходів	Аудит безпеки, виправлення помилок, оновлення політик	Планування реагування на інциденти, системи резервного копіювання, навчання персоналу

Враховуючи взаємозв'язок між стійкістю та ризиками, не дивно, що підвищення стійкості системи дає значні переваги в управлінні ризиками; підвищення стійкості системи є невід'ємною частиною процесу управління ризиками. Фундаментальною перевагою є те, що прийнятний рівень залишкового ризику для системи (тобто прийнятний рівень доступної безпеки) може бути визначений для кожного класу сценаріїв загроз. Більш конкретно, через імовірнісну природу загроз, при виникненні класу сценаріїв загроз, результати (наслідки) найкраще представляти за допомогою функцій розподілу ймовірностей. Отримані ризики з точки зору часу відновлення та сукупних витрат можуть бути розраховані різними способами, включаючи очікувану величину ризиків або умовну очікувану величину ризику крайніх значень [270]. І, зрештою, можна оцінити компроміси між різними рівнями

ризиків і витрат, пов'язаних з кожною інвестицією (наприклад, через забезпечення готовності) в стійкість системи. Той факт, що рівень серйозності наслідків, спричинених загрозою для системи, використовується як метрика, за допомогою якої оцінюється вектор стійкості системи – і враховуючи, що входи і, відповідно, виходи системи мають імовірнісний характер – неминуче призводить до наступних трьох основних питань в управлінні ризиками: *Що можна зробити і які варіанти доступні? Якими є пов'язані з цим компроміси з точки зору всіх відповідних витрат, вигод і ризиків? Як впливають поточні рішення на майбутні варіанти?* [270; 272] Оскільки відповіді на ці питання настільки специфічні для кожної системи і до кожного сценарію, вони не дають можливості присвоїти системі загальні та абсолютні оцінки стійкості системи.

Важливість стійкості як стану здатності системи протистояти вимушеним змінам її організаційної структури, функціональності та операційної безперервності призвела до розробки показників спроможності як аналогів стійкості. Дійсно, з'являється кілька систем оцінки для вимірювання стійкості кіберсистем. Наприклад, Інститут інженерії програмного забезпечення Карнегі-Меллона розробляє Рамку інженерії стійкості (Resilience Engineering Framework, REF) [195], яка визначає вектор з 21 сфери спроможностей, які можна виміряти за шкалою розвиненості, що продемонструє, які практики кібербезпеки і стійкості можуть бути найбільш ефективно інтегровані в загальні і часті управлінські рішення. Основна ідея полягає в тому, що якщо існують зрілі бізнес-процеси і якщо вони належним чином інтегрують загальні рішення з рішеннями щодо безпеки, то організація з більшою ймовірністю побачить, зрозуміє і відреагує на кіберзагрозу таким чином, щоб зменшити наслідки і звести до мінімуму час і витрати на відновлення.

З іншого боку, спроби охарактеризувати стійкість системи певним числовим дескриптором (метрикою) і використовувати цю метрику для порівняння стійкості різних систем можуть ввести в оману, якщо ми не будемо припускати, що ці різні системи піддаватимуться однаковим загрозам і

однаковим рівням таких загроз з однаковою ймовірністю. З огляду на різноманітність функціональних можливостей і конфігурацій сучасних інфраструктурних систем (і, зокрема, кіберсистем), а також враховуючи величезну невизначеність, пов'язану з цими відмінностями і загрозами, яким може піддаватися будь-яка така система, нерозумно присвоювати будь-якій з цих систем числову шкалу або число стійкості.

Таким чином, можна зробити важливий висновок, що стійкість системи може бути виміряна з точки зору безлічі підстанів, які характеризують цю систему в певний період часу і під впливом певних загроз. Це зовсім інше питання, однак, абстрактно спрогнозувати час відновлення та сукупні витрати і ризики, пов'язані з будь-яким невизначеним фантомним набором сценаріїв загроз. Тут знову ж таки, ризик, як міра ймовірності та тяжкості негативних наслідків [326], може бути оцінений лише для конкретного сценарію загрози в будь-який період часу.

Зважаючи на викладене та враховуючи безпрецедентні масштаби та серйозність ризиків, стійкість повинна виходити за межі будь-якої глобальної інфраструктури зосереджуючись на окремих організаціях. Разом з тим, вимірювання ефективності стійкості системи може бути досягнуто, наприклад, через унікальну функціональність цієї конкретної системи та її реакції (виходи) на конкретні входні дані. А оскільки такі входи є ймовірнісними, то й виходи також є ймовірнісними, а це означає, що стійкість системи – оскільки вона вимірюється з точки зору реакції на входи – може бути виміряна (кількісно оцінена) лише в ймовірнісних термінах і для конкретних входів.

Для планування та оперативних рішень показники кіберстійкості мають важливе значення і забезпечують засоби для визначення і визначення пріоритетності потреб, моніторингу прогресу і розподілу ресурсів [225]. Проте, спроби експертів зібрати показники кіберстійкості не дають такої інформації. Наприклад, огляд, проведений Науковою радою з питань оборони (Defense Science Board – DSB) [394] не знайшов у літературі жодних показників, які були б корисними оборонним системам для управління

кіберризиками. Крім того, показники, розроблені DSB [394] були визначені як неповні, оскільки вони ігнорують процеси управління стійкістю [323]. Незадовільний стан розуміння та визначення показників стійкості не викликає здивування, особливо у сфері кібербезпеки. Дійсно, навіть показники кіберризиків є недостатньо зрозумілими і прийнятими, хоча ризик можливо, є більш вивченим поняттям, ніж стійкість. Існуючі на сьогодні алгоритми оцінки кіберризиків покладаються здебільшого на простих евристичках, таких як суми вразливостей у балах або кількість таких речей, як відсутні патчі, відкриті порти тощо. Такі показники широко розглядаються як слабкі та потенційно оманливі [159; 296]. Наприклад, індивідуальні оцінки вразливостей, як правило, є суб'єктивними та потенційно неточними; прості суми не враховують, як вразливості розподілені між хостами або у часі; вони також не враховують топологію мережі, роль та динаміку міжхостової взаємодії, ні нелінійну взаємодію між вразливостями, ні наміри зловмисника та потенційно неточну інформацію, ні наявність чи відсутність відповідних механізмів мережевого захисту, ні те, як компроміс може вплинути на місію організації [311]. Загалом, сувора теорія або моделі того, як різні фактори можуть поєднуватися в кількісну характеристику справжніх кіберризиків, бракує так само, як і суворої емпіричної перевірки показників кіберризиків. Подібні, а можливо, й більші недоліки та обмеження впливають на показники кіберстійкості. Запропонований в літературі підхід на основі матриці стійкості інтегрує чотири системні здібності планувати/готуватися, поглинати, відновлюватися і адаптуватися до відомих і невідомих загроз [225] з чотирма операційними доменами (фізичний, інформаційний, когнітивний та соціальний), що пропонує ефективний метод для класифікації показників стійкості [28, с. 135].

Нещодавні досягнення в сфері стійкості визначили кілька важливих атрибутів ефективних показників для кіберсистем, призначених для оборони та критичної інфраструктури. У звіті 2013 року про «Стійкі військові системи і сучасні кіберзагрози» (Resilient Military Systems and the Advanced Cyber

Threat) Наукової Ради з питань оборони (DSB) [394] рекомендується, щоб показники були:

- *достатньо широкими*, щоб їх можна було використовувати в різноманітному діапазоні систем;
- *достатньо точними* для вимірювання конкретних системних процесів і компонентів [28, с. 135].

Важливо зазначити, що DSB слова «показники» і «вимірники» визначаються по-різному. Вимірник – це кількісний або якісний засіб фіксації атрибуту певної системи або компонента системи [147]. Показник – це засіб для порівняння якості двох або більше систем або компонентів системи через застосування вимірника [147]. Наприклад, продуктивність системи в умовах кіберзбою буде показником, де швидкість передачі даних через неї буде вимірником пов'язаним з цим показником. Лінков та ін. [323] стверджують, що поєднання доктрини мережецентричної війни (Network-Centric Warfare – NCW) [146] і визначення Національної академії наук [225] стійкості до катастроф може бути використане для розробки показників, які відповідають цим критеріям. Національна Академія наук (National Academy of Sciences – NAS) визначає чотири етапи циклу управління подіями, які система повинна підтримувати для того, щоб бути стійкою:

- *планування/підготовка*: закладення основи для забезпечення доступності послуг та функціонування активів під час руйнівної події (несправності або атаки);
- *поглинання*: підтримка найбільш важливих функцій активів та доступність послуг під час відбиття або ізоляції збоїв у роботі;
- *відновлення*: відновлення всіх функцій активів та доступність сервісів та їх функціональність як до події;
- *адаптація*: використовуючи знання, отримані під час події, зміна протоколу, конфігурації системи, навчання персоналу або інші аспекти для досягнення більшої стійкості [28, с. 135-136].

Доктрина мережецентричної війни (NCW) визначає чотири сфери, які створюють загальну обізнаність про ситуацію і забезпечують децентралізоване прийняття рішень, а саме:

- *фізична*: фізичні ресурси, можливості і структура цих ресурсів;
- *інформаційна*: інформація та розвиток інформації про фізичну сферу;
- *когнітивний*: використання інформаційного та фізичного доменів для ухвалення рішень;
- *соціальний*: організаційна структура та комунікація для ухвалення когнітивних рішень [28, с. 136].

Лінков та ін. [323; 324] об'єднали визначення чотирьох функцій системи NAS і чотирьох доменів NCW, щоб створити загальну матрицю показників стійкості та адаптовано до кіберсистем (табл. 3.17). Ними запозичено багато показників з літератури [148; 167]. Показники доповнюються оцінкою їхніх наслідків на різних етапах і в різних сферах, так що відомі показники на одному з етапів циклу управління подіями або в межах однієї операційної сфери мають прямий вплив на показники в інших сферах [28, с. 136].

Таблиця 3.17

Матриця кіберстійкості [323]

	планувати/готуватися	поглинати	відновлюватися	адаптуватися
фізична				
інформаційна				
когнітивна				
соціальна				

Окремі сегменти матриці містять показники, які вимірюють здатність системи управляти несприятливими подіями та представляють конкретні показники для оцінки стійкості кіберсистеми. При інтерпретації матриці кожен сегмент відповідає на питання: «Як реалізується спроможність (*планувати/готуватися, поглинати, відновлюватися, адаптуватися*) системи до кіберподії в (*фізичній, інформаційній, когнітивній, соціальній*) сфері?». При цьому, сегменти в колонках (*поглинати, відновлюватися, адаптуватися*) відображають спроможності, які система повинна продемонструвати, щоб

бути стійкою до збоїв, тоді як колонка (планувати/готуватися) зосереджується на розумінні та документуванні структури та функцій системи [28, с. 136].

Показники, розроблені на основі матриці стійкості, не обов'язково можуть бути виміряні прямими методами, їх слід генерувати за допомогою спеціальних заходів, розроблених для кожної системи окремо. Це можуть бути як кількісні дані, так і якісні показники, які потім оцінюються технічними експертами та зацікавленими сторонами, пов'язаними з конкретною системою. Наприклад, показники, визначені для здатності кіберсистеми поглинати збої в інформаційній сфері, включають в себе здатність передавати дані, а також включає в себе здатність передавати дані відповідальним зацікавленим сторонам і особам, що приймають рішення. Цей показник може бути найкраще представлений комбінацією кількісних даних і якісних вимірників, таких як кількість зацікавлених сторін, типи залучених стейкхолдерів, ієрархія управління, кількість резервів в системах передачі інформації та частота обміну інформацією [28, с. 137].

Зростаюча складність кіберсистем та кіберзагроз вимагає інтеграції процесів управління ризиками та процесу управління стійкістю. Часто загроза не розпізнається доти, доки вона не проявиться в кіберсистемі, а отже може бути пропущена в сценаріях загроз, які розглядаються в рамках оцінки ризиків. Кіберстійкість, гнучка за своєю природою, може забезпечити основу для боротьби з кіберзагрозами і життєздатність критично важливих кібер-активів і послуг. Управління стійкою кіберсистемою з використанням цієї концепції визнає і підкреслює взаємодію між кожним доменом організації на кожному етапі управлінського циклу – фактор, який не враховується в інших підходах до забезпечення стійкості [28, с. 137].

Стійкість кіберсистеми залежить від ефективного функціонування всіх аспектів організації протягом усього циклу управління подіями в чотирьох визначених сферах. Ключовою перевагою використання матриці стійкості і є прозорий зв'язок між сферами впродовж усього циклу управління заходами. Як результат, системне застосування визначення NAS об'єднує всі компоненти

організації в гетерогенну систему кіберінфраструктури, бізнес-функцій та зовнішніх суб'єктів. Однак аналіз цієї системи сам по собі не дає інформації про те, як стійкість виникає з системних взаємодій. Натомість, організація та вимірювання цих компонентів як підсистем, дозволяє визначити, як ці різномірні компоненти взаємодіють, щоб стати стійкими [28, с. 137].

Протягом усього процесу заповнення матриці взаємозалежність показників, етапів і доменів є критично важливою. Додаючи показник, слід враховувати, як він впливає на інші в матриці. Матриця стійкості не є вичерпним посібником, але натомість може бути використана для визначення та прив'язки системних заходів до проектування та експлуатації складних систем. По-перше, розроблені показники можна узагальнити для багатьох систем, таким чином, їх можна використовувати для порівняльної оцінки стійкості системи. Крім того, постійний моніторинг і звітність можуть інформувати керівництво про зміни, що вносяться як особами, що приймають рішення, так і системними операторами. Найважливіше те, що цей підхід може бути використаний для розподілу ресурсів щодо підвищення стійкості [28, с.138].

Для переведення концепції кіберстійкості у площину практичного управління в дослідженні у подальшому застосовано зазначену інтегровану матричну модель. Цей підхід базується на синергії якісних експертних суджень та кількісних метрик, що дозволяє структурувати складну архітектуру кіберсистеми. Матриця побудована як двовимірна система координат: по одній осі розташовані етапи управлінського циклу заходи (планування/передбачення, поглинання удару, відновлення та адаптація), а по іншій – функціональні домени системи (фізичний, інформаційний, когнітивний та соціальний). Таке компонування забезпечує цілісність аналізу, оскільки дозволяє відстежити, як заходи в одному домені (наприклад, технічне зміцнення інформаційної сфери) корелюють із результатами в іншому (наприклад, швидкістю ухвалення рішень у когнітивній сфері). Головною перевагою даної моделі є її здатність виявляти нелінійні зв'язки та

забезпечувати прозорість між технічними параметрами та управлінською ефективністю протягом усього життєвого циклу інциденту.

Наповнення матриці здійснюється через систему специфічних індикаторів, розроблених для кожного сегмента окремо. Важливо підкреслити, що показники кіберстійкості не завжди піддаються прямому вимірюванню інструментальними методами. Тому методологія передбачає генерацію метрик на основі комбінованих даних: від об'єктивної статистики технічних систем до оцінок фахівців та стейкхолдерів. Кожен показник у матриці (наприклад, рівень резервування потужностей у фізичному домені або час поширення критичної інформації в інформаційному) розглядається не ізольовано, а в контексті його впливу на загальну витривалість системи. При додаванні або зміні індикатора враховується принцип взаємозалежності: зміна рівня спроможності в інформаційній сфері автоматично створює нові умови для функціонування соціального домену (координації). Такий підхід дозволяє отримати не статичний «зріз» безпеки, а динамічний профіль стійкості, придатний для стратегічного прогнозування.

В основі запропонованої методології лежить розуміння сучасної кіберсистеми як гетерогенної мережі, де стійкість є емерджентною властивістю (такою, що виникає лише в результаті взаємодії частин). Міждоменна комунікація стає ключовим чинником «живучості»: здатність системи швидко перерозподіляти інформаційні потоки у разі руйнування фізичних вузлів безпосередньо залежить від підготовленості когнітивного домену (персоналу). Методологія акцентує увагу на тому, що критично важливою є не лише стійкість окремого вузла, а саме збереження зв'язків між ними. Це дозволяє системі трансформуватися під час атаки, ізолюючи уражені сегменти без зупинки базових сервісів. Отже, матриця стає інструментом візуалізації та кількісного вимірювання цієї мережевої стійкості, перетворюючи розрізнені технічні дані у зрозумілу модель для ухвалення державних рішень.

Для візуалізації та систематизації проведеного аналізу, нижче наведено сформовану Матрицю показників кіберстійкості (табл. 3.18), яка об'єднує чотири етапи життєвого циклу управління інцидентами та чотири операційні домени системи. Дані в таблиці відображають кількісну оцінку спроможностей за кожним сегментом.

Таблиця 3.18

Матриця показників кіберстійкості національної кіберінфраструктури (%)

Операційні домени	Планувати / Готуватися	Поглинати (витримувати удар)	Відновлюватися	Адаптуватися
Фізичний (ресурси та структура)	54,39	54,48	54,55	54,36
Інформаційний (дані та обмін інформацією)	54,96	54,54	55,14	54,80
Когнітивний (ухвалення рішень)	52,62	52,23	52,59	53,74
Соціальний (організація та комунікація)	51,75	52,42	52,26	53,10

Джерело: сформовано автором на основі обробки результатів емпіричного дослідження та описаної методологічної рамки.

Відповідно до зазначеної методології етап «Планувати / Готуватися» відображає рівень розуміння та документованості структури і функцій системи у відповідній сфері. Етапи «Поглинати», «Відновлюватися» та «Адаптуватися» характеризують спроможності, які система реально демонструє під час та після виникнення несприятливих подій (кібератак). Перехресний аналіз значень показує, що найвищий рівень стійкості наразі забезпечується в інформаційному домені на етапі відновлення (55,14%), тоді як найбільш критичною точкою є планування та підготовка в соціальному домені (51,75%).

Ця матриця є ключовим аналітичним інструментом для переходу до наступного етапу дослідження – аналізу здатності системи до поглинання ударів та швидкості відновлення ресурсів.

Перехід до емпіричного етапу дослідження передбачає верифікацію теоретичної моделі через кількісне оцінювання реального стану вітчизняної кіберінфраструктури. На основі розробленої матриці кіберстійкості було проведено аналіз поточного рівня реалізації спроможностей у чотирьох ключових операційних сферах: фізичній, інформаційній, когнітивній та соціальній. Отримані результати дозволяють ідентифікувати не лише загальний рівень готовності системи, а й виявити структурні диспропорції, що впливають на загальну живучість держави в цифровому просторі.

Аналіз етапу «*планувати/готуватися*» у системі кіберстійкості є визначальним, оскільки він закладає фундамент для забезпечення доступності послуг та функціонування активів безпосередньо під час руйнівної події. Цей етап фокусується на глибокому розумінні та документуванні структури і функцій системи, що дозволяє прогнозувати потенційні ризики та готувати відповідні сценарії реагування.

На основі розрахункових даних Матриці кіберстійкості (табл. 3.18), аналіз етапу планування за доменами демонструє наступні результати:

інформаційний домен (54,96 %): демонструє найвищий рівень готовності в розрізі планування. Це свідчить про сформованість процесів збору, опрацювання та розвитку інформації про стан фізичної інфраструктури, а також про наявність дієвих механізмів інформаційного обміну на технічному рівні. Високий показник у цьому домені є критично важливим, оскільки саме інформаційна обізнаність стає базою для функціонування всіх інших елементів стійкої системи. Це також свідчить про якісну роботу з ідентифікації ризиків, де знання про існуючі вразливості дозволяє прогнозувати типи загроз та їхні наслідки. Висока оцінка вказує на системне використання методик аналізу та звітування про вразливості.

фізичний домен (54,39 %): показник відображає належний рівень інвентаризації та документування фізичних ресурсів і можливостей інфраструктури і оцінюється як стабільно середній. Планування у цій сфері забезпечує базу для технічної живучості об'єктів критичної інформаційної

інфраструктури. Показник відображає наявність необхідної матеріально-технічної бази та можливостей її експлуатації для забезпечення безперервності сервісів. Слід зауважити, що фізична стійкість є «фундаментом», на якому базуються інформаційні потоки, і її стабільність (понад 54 %) є позитивним сигналом для загальної архітектури захисту.

когнітивний домен (52,62 %): вказує на певний розрив між наявністю інформації та стратегічним плануванням її використання для ухвалення рішень. Показник свідчить про потребу в посиленні форсайту та розробці більш детальних сценаріїв дій для осіб, що приймають рішення. Ця сфера, що відповідає за використання інформації та ресурсів для ухвалення оперативних і стратегічних рішень, демонструє дещо нижчі результати порівняно з технічними доменами. Це вказує на наявність певних бар'єрів у процесах перетворення сирих даних у дієві управлінські рішення в умовах дефіциту часу або високої невизначеності. Зниження показника в цій зоні створює ризики затримок у реагуванні на складні, багатовекторні кібератаки.

соціальний домен (51,75 балів): оцінка організаційної структури та комунікації для ухвалення рішень є найнижчою в загальному профілі спроможностей. Такий результат свідчить про об'єктивні складнощі в налагодженні ефективної міжвідомчої та міжсекторальної взаємодії, а також про потребу в удосконаленні ієрархії управління та протоколів децентралізованого прийняття рішень. Соціальний домен є найбільш критичною ланкою, оскільки саме він забезпечує злагодженість дій усіх суб'єктів системи кіберстійкості під час кризи.

Детальний аналіз зазначених показників дозволяє дійти висновку про наявність «технологічного випередження» в системі: технічні та інформаційні можливості (фізичний та інформаційний домени) розвиваються швидше, ніж управлінські та комунікаційні механізми (когнітивний та соціальний домени). Така диспропорція створює ризик, при якому наявні ресурси можуть бути використані не повною мірою через недосконалість процесів управління та координації. Отже, пріоритетом розвитку інституційної спроможності має

стати не лише нарощування технічних засобів, а насамперед інвестиції в когнітивну та соціальну складові стійкості, що дозволить перетворити окремі успішні компоненти на єдину, злагоджену та високоефективну національну систему.

Таким чином, етап «планувати/готуватися» у вітчизняній моделі потребує зміщення фокусу з суто технічного аудиту вразливостей на розробку комплексних організаційних планів (соціальний домен) та вдосконалення систем підтримки ухвалення рішень (когнітивний домен).

Аналіз здатності до поглинання та відновлення є наступним критичним етапом емпіричного дослідження та оцінкою динамічних характеристик системи – її спроможності витримувати безпосередній деструктивний вплив (*поглинання*) та здатності до максимально швидкої рекуперації втрачених функцій (*відновлення*). У межах запропонованої методології ці два етапи складають «активну фазу» кіберстійкості, де система демонструє свою реальну живучість під час та одразу після інциденту.

Під поглинанням у дослідженні розуміється спроможність системи підтримувати найбільш важливі функції активів та доступність сервісів безпосередньо під час відбиття або ізоляції збоїв у роботі. Кількісний аналіз за доменами дозволяє ідентифікувати «інерційну міцність» вітчизняної кіберінфраструктури:

технологічна стійкість: фізичний (54,48) та інформаційний (54,54) домени демонструють майже ідентичні показники здатності до «буферизації» удару. Це свідчить про те, що технічна архітектура систем має певний запас міцності, що дозволяє локалізувати аномалії на рівні мережевих протоколів та обладнання без миттєвої деградації всього контуру.

управлінська гнучкість: когнітивний (52,23) та соціальний (52,42) домени мають дещо нижчі значення. Це вказує на те, що в момент гострої фази атаки процеси ухвалення рішень та міжвідомчої координації стають менш стабільними, ніж технічні алгоритми. Таким чином, здатність системи

«поглинати» стрес на рівні людського фактора та організаційних структур є меншою, ніж на рівні заліза та коду.

Водночас, відновлення визначається як здатність системи регенерувати свою продуктивність після неочікуваного впливу, що призвів до погіршення її роботи. Метою цього етапу є повернення всіх функцій активів та сервісів до стану, що передував події. Емпіричні дані фіксують наступні тенденції:

пріоритетність даних: найвищий показник у всій матриці зафіксовано в інформаційному домені на етапі відновлення – 55,14 %. Це підтверджує стратегічну орієнтацію суб'єктів кібербезпеки на першочергову рекуперацію даних та відновлення інформаційних потоків.

фізична рекуперація: показник відновлення фізичних ресурсів (54,55) корелює з високим рівнем підготовки інженерного персоналу та наявністю розроблених планів безперервності бізнесу.

соціальна інерція: соціальний домен на етапі відновлення демонструє показник 52,26 %, що є одним із найнижчих значень у цьому циклі. Це вказує на те, що після нейтралізації технічної загрози організаційні структури та комунікаційні канали відновлюються повільніше, що може призводити до тривалого періоду «управлінського ехо» після інциденту.

Таким чином, порівняльний аналіз здатності до поглинання та відновлення дозволяє зробити висновок про формування в Україні «техноцентричної моделі стійкості». Система демонструє кращу готовність до технічного витримування ударів та відновлення цифрових активів, ніж до швидкої стабілізації когнітивних та соціальних зв'язків. Середнє значення показників у діапазоні 52,2 – 55,1 % вказує на стабільний, проте недостатній рівень стійкості, оскільки для критично важливих систем цей показник має наближатися до значень понад 75-80 балів. Таким чином, основною проблемою є не відсутність технічних можливостей, а недостатня ефективність міждоменної комунікації та координації, від яких залежить швидкість переходу від поглинання удару до повноцінного функціонування.

Завершальним етапом аналізу матричної моделі є оцінка здатності системи до адаптації, що визначається як спроможність використовувати знання, отримані під час інциденту, для зміни протоколів, конфігурацій та навчання персоналу з метою досягнення вищого рівня стійкості у майбутньому. Адаптація є найбільш інтелектуально містким процесом, оскільки вона перетворює досвід подолання криз на стратегічний актив держави.

На основі розрахункових даних (див. табл. 3.18), потенціал адаптації вітчизняної кіберінфраструктури характеризується наступними показниками:

інформаційна адаптивність (54,80 %): цей показник є найвищим у стовпці адаптації, що вказує на сформовану здатність системи до технічного перегляду алгоритмів захисту та оновлення баз даних загроз на основі проведеного аналізу інцидентів. Це свідчить про наявність механізмів зворотного зв'язку в технічних підсистемах, що дозволяє автоматизувати процес «навчання» мережі.

когнітивна адаптація (53,74 %): високий рівень у когнітивній сфері відображає позитивну динаміку в інтеграції отриманого досвіду в процесі ухвалення рішень. Це вказує на те, що особи, які приймають рішення, схильні до перегляду стратегій та тактик протидії на основі пост-інцидентного аналізу.

соціальна адаптація (53,10 %): показник демонструє здатність організаційних структур до гнучкої зміни протоколів взаємодії та комунікації. Хоча соціальний домен традиційно є найбільш інертним, значення вище 53 % свідчить про готовність державних інституцій до інституційного самовдосконалення.

фізична адаптація (54,36 балів): показник відображає спроможність до зміни архітектури фізичних ресурсів та можливостей системи у відповідь на виявлені критичні вразливості.

Узагальнюючи результати, можна стверджувати, що стадія адаптації (середній показник ~54 %) демонструє вищу стабільність порівняно з етапом поглинання або планування у гуманітарних доменах (когнітивному та

соціальному). Це вказує на те, що система краще вчиться на реальних помилках, ніж готується до гіпотетичних сценаріїв. Такий стан справ підтверджує тезу про те, що стійкість системи є вектором, який залежить від часу та конкретних входних сигналів (загроз).

3.4. Прикладний аналіз системних спроможностей та правові орієнтири забезпечення кіберстійкості інформаційної інфраструктури

Логіка побудови сучасної системи національної кіберстійкості вимагає концептуального переходу від пасивної моделі фіксації недоліків до активної моделі нарощування ресурсів. У науковому дискурсі терміни «вразливість» та «спроможність» виступають як взаємопротилежні явища за своїм сутнісним змістом та вектором спрямованості. Вразливість за своєю природою є статичною та реактивною категорією; вона позначає слабкі місця або недоліки в програмному забезпеченні, процесах чи людському факторі, які створюють потенційну можливість для нанесення шкоди. Орієнтація виключно на вразливості фокусує увагу суб'єктів кібербезпеки на минулому досвіді та вже існуючих помилках, що часто виявляється недостатнім у ситуації з непередбачуваними загрозами «нульового дня».

На противагу цьому, спроможність є динамічним та проактивним явищем, що характеризує здатність системи не просто уникати впливу, а активно протидіяти йому, адаптуватися до змінних умов і швидко відновлювати працездатність. Якщо вразливість – це «прогалина» в обороні, то спроможність – це «інструмент» та «сила», що дозволяють цій обороні бути живою та ефективною. Перехід від аналізу вразливостей до аналізу інституційної спроможності системи кібербезпеки означає зміну фокусу з того, «що в нас не працює», на те, «що ми можемо зробити», щоб система залишалася функціональною під час та після атаки.

Концепція інституційної спроможності у науковому дискурсі характеризується поліаспектністю тлумачень. Окремі дослідники розглядають її як динамічний процес або системний внесок; інші ж акцентують увагу на детермінації результату (П. Морган), визначають як інституційну якість (Ф. Фукуяма), фундаментальну властивість управління (Е. Гріндел) або специфічну організаційну характеристику (А. Толобем). Крім того, даний феномен інтерпретується як фактор, що розкриває потенціал індивідуальності (А. Сен). У науковій літературі термін «інституційна спроможність» часто корелює із поняттями належного врядування, системної організованості та управлінської ефективності [87, с. 380].

У широкому контексті інституційна спроможність суб'єктів кібербезпеки передбачає здатність державних структур результативно реалізовувати ключові функції із захисту національного цифрового простору та здійснювати наскрізний контроль за їх виконанням на всіх ієрархічних рівнях – від загальнодержавного центрального до місцевого регіонального. Йдеться, насамперед, про фундаментальні функції держави: забезпечення кіберпорядку, захист цифрових свобод, дотримання справедливості та надання безпечних соціальних благ у кіберпросторі [87, с. 380].

Незважаючи на значний доробок вітчизняних і зарубіжних вчених (Ю. Битяка, Л. Гонюкової, А. Кабанця, М. Кармазіної, Т. Мотренка, В. Мельниченка, Ю. Сурміна, О. Сушинського, О. Оболенського, Н. Нижник, В. Олуйка, Т. Пахомової, Л. Пашко, А. Сіцінського, С. Серьогіна та інших), присвячений теоретико-методологічним аспектам категорій «інститут» та «спроможність», питання обґрунтування інституційної спроможності саме в системі державного управління кібербезпекою України потребує більш ґрунтовної галузевої детермінації [62]. На сьогодні залишається недостатньо вивченою проблематика безпосереднього аналізу та стратегічного розвитку інституційної спроможності у сфері забезпечення кібербезпеки та кіберстійкості України.

Згідно з тлумачними джерелами, поняття «спроможність» визначається як здатність до реалізації певної діяльності або наявність сукупності сприятливих умов для досягнення мети [124, с. 605]. Професор Колісніченко Н. інтерпретує спроможність як інтегральну сукупність організаційних, технологічних можливостей, соціальних взаємовідносин та ціннісних орієнтирів, що дозволяють державі, організаціям та окремим громадянам на будь-якому суспільно-політичному рівні ефективно виконувати функції та досягати цілей сталого розвитку протягом визначеного часу [61, с. 299].

У розвиток зазначеного, імперативною умовою формування спроможностей у сфері кібербезпеки є наявність необхідного ресурсного забезпечення (матеріальних та нематеріальних активів, інтелектуального капіталу, злагоджених алгоритмів організаційних процесів, актуальної інформації та верифікованих знань), що контролюються відповідною інституцією. Це дозволяє впроваджувати стратегії, спрямовані на підвищення раціональності та ефективності протидії кіберзагрозам [51, с. 11].

Водночас, інституційна спроможність у кіберсфері базується на колективній здатності організації реалізовувати специфічні види активності (прогнозування, запобігання, реагування) та властивості суб'єкта ефективно оперувати наявними ресурсами [3, с. 363]. У сучасних умовах така колективна здатність є деривативом стабільного функціонування установи чи підприємства, через яке системно генеруються стратегічні та операційні завдання, спрямовані на підвищення загальної управлінської ефективності в умовах динамічного кіберпростору [423, с. 340].

В межах даного дослідження перехід до стратегічного виміру стійкості було реалізовано на методологічній основі ризик-орієнтованого підходу. Ми дослідили розгалужену систему індикаторів спроможностей суб'єктів кібербезпеки в Україні, де кожен показник розглядається не як ізольована технічна одиниця, а як компонент загальної витривалості держави. Такий підхід дозволив трансформувати розуміння ризику: він більше не

сприймається лише як імовірність експлуатації вразливості, а оцінюється через призму спроможності системи мінімізувати вплив цього ризику та забезпечити безперервність бізнес-процесів.

Використання ризик-орієнтованого підходу забезпечило можливість інтегрувати технічні вимірники з управлінськими рішеннями, що дозволило перейти від «латання дірок» до системного управління життєздатністю національної інформаційної інфраструктури. Таким чином, аналіз спроможностей стає фундаментом для побудови прогнозової моделі, де стійкість виступає як результат свідомого інвестування в активи, навички та координаційні механізми, здатні поглинати зовнішні стреси.

Аналіз усієї сукупності даних демонструє неоднорідний ландшафт спроможностей, де середні значення коливаються в діапазоні від 44.46% до 66.33% (рис. 3.3). Така варіативність свідчить про те, що національна система кібербезпеки перебуває у стані активної трансформації: окремі функціональні сегменти вже досягли рівня впевненої стабільності, тоді як інші залишаються на етапі первинного формування. Загальна тенденція вказує на зміщення акцентів у бік високої централізації спроможностей на загальнодержавному рівні, що створює певну «захисну парасольку», проте супроводжується значним розпорошенням показників на нижчих рівнях управління та в окремих специфічних доменах.

Виходячи з нашого алгоритму (де значення $>50\%$ трактується як позитивна спроможність), переважна більшість досліджених індикаторів знаходиться у позитивній зоні. Це говорить про формованість базису. Система загалом вийшла за межі критичної вразливості та демонструє життєздатність. Більшість середніх показників концентруються в межах 52–59%, що свідчить про наявність дієвого інструментарію та нормативної бази для протидії загрозам. Водночас, знаходження показників у діапазоні 50–65% вказує на значний «коридор росту». Система має сформований «скелет» спроможностей, але потребує нарощування «м'язової маси» – поглиблення

експертизи, автоматизації процесів та масштабування успішних практик на всю вертикаль управління.

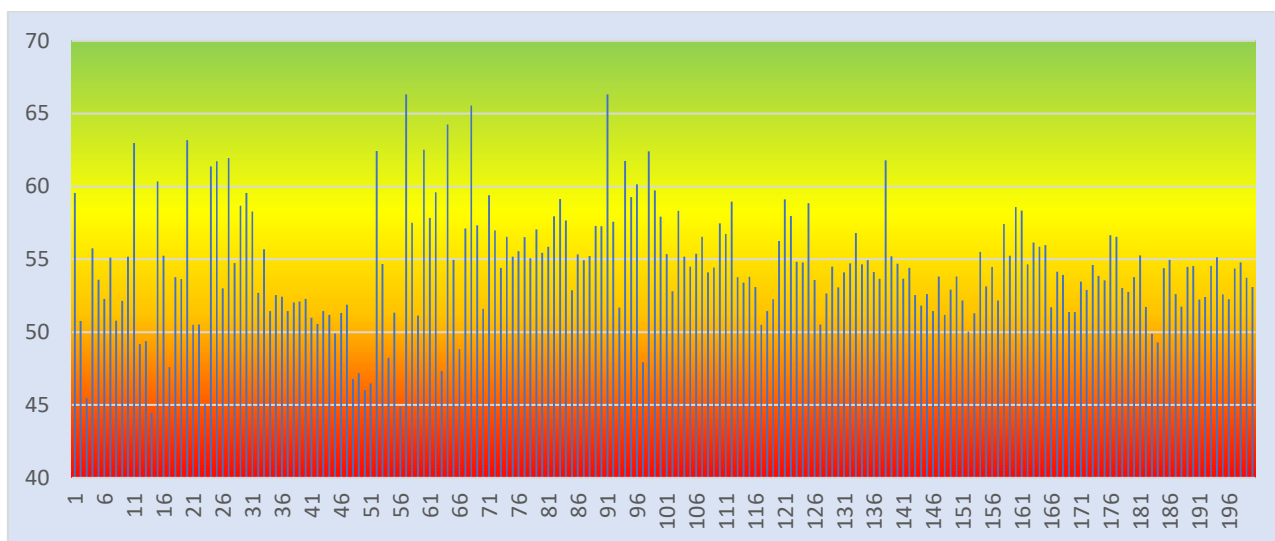


Рис. 3.3 Діаграма спроможностей суб'єктів системи кібербезпеки в Україні

Сукупність індикаторів, значення яких опустилося нижче позначки 50%, чітко окреслює зони системної вразливості. Наявність таких показників (мінімальне значення – 44.46%) свідчить про існування напрямів, де система захисту є номінальною або недостатньою для протидії сучасним викликам. А також про те, що ці зони вимагають не просто косметичних поліпшень, а впровадження фундаментальних змін. Це ті ланки, які у разі масштабної кіберкризи можуть стати «точками входу» для деструктивного впливу або призвести до колапсу окремих сервісів на локальних рівнях.

Загальна картина свідчить про переважно позитивний вектор розвитку спроможностей (більшість $> 50\%$), що підтверджує перехід України до побудови системи кіберстійкості. Однак суттєва варіативність та наявність зон із показниками нижче 50% вказують на те, що система є незбалансованою. Ми маємо міцний «центр», але вразливу «периферію» та недофінансовані або організаційно слабкі специфічні напрями, які потребують першочергового втручання.

Аналіз результатів оцінювання ефективності формування та реалізації державної політики у сфері кібербезпеки дозволяє виявити чітку ієрархічну залежність та секторальну диференціацію спроможностей національної системи (табл. 3.19). На загальнодержавному рівні інтегральний показник ефективності становить 59,55%, що згідно з визначеним алгоритмом свідчить про наявність позитивної спроможності та сталого потенціалу для подальшого зростання. Найвищу ефективність реалізації політики зафіксовано в фінансовому та банківському секторах (73,91%), що вказує на пріоритетність захисту критичних логістичних вузлів у стратегічному плануванні держави. Також високі рівні спроможності демонструють державне управління (61,99%) та сфера інфраструктури та транспорту (60,87%), що підтверджує успішність впровадження державних стандартів у базових галузях життєзабезпечення.

Таблиця 3.19

Рівень ризику ефективності формування та реалізації державної політики у сфері кібербезпеки (%)

Ефективність формування/реалізації державної політики у сфері кібербезпеки на рівні:	Оцінка ризику, %	державне управління	енергетичний комплекс	фінанси/ банки/ страхування	інфраструктура/ транспортна система	телекомунікаційні послуги	цифрові послуги	оборонно-промисловий комплекс
загальнодержавному	59,55	61,99	53,91	73,91	60,87	60,04	54,63	57,00
регіональному	50,77	52,31	42,61	47,82	41,30	52,17	44,78	48,31
місцевому	45,48	46,28	46,08	47,82	34,78	47,55	42,17	42,02
діяльності Уряду	55,75	59,40	39,13	63,04	47,82	58,59	51,88	45,41
діяльності ЦОВВ	53,59	57,99	36,52	54,34	47,82	54,65	47,83	45,89

На рівні діяльності Уряду та центральних органів виконавчої влади (ЦОВВ) показники ефективності залишаються в позитивній зоні – 55,75% та 53,59% відповідно. Це свідчить про функціональність вертикалі управління, проте аналіз окремих секторів виявляє суттєві вразливості. Зокрема, ефективність політики в сегменті енергетичного комплексу на рівні Уряду оцінюється лише у 39,13%, а на рівні ЦОВВ – у 36,52%. Оскільки ці значення суттєво нижчі за критичний поріг у 50%, енергетичний сектор у розрізі

виконавчої влади ідентифікується як зона високого ризику, що потребує негайного перегляду регуляторних підходів та механізмів впровадження політики.

Регіональний рівень демонструє граничний стан спроможності з показником 50,77%, що формально відносить його до позитивної зони, проте свідчить про високу нестабільність системи. Секторальна деталізація на цьому рівні виявляє глибокі вразливості: у сферах енергетичного комплексу (42,61%), інфраструктури та транспорту (41,30%), а також цифрових послуг (44,78%) рівень ризику перевищує допустиму межу. Це говорить про значну деградацію спроможностей при переході від стратегічного планування в центрі до операційної реалізації в регіонах, де державна політика часто втрачає свою ефективність через брак ресурсів або недосконалість координаційних каналів.

Найбільш критична ситуація спостерігається на місцевому рівні, де середній рівень спроможності становить лише 45,48%, що вказує на системну вразливість муніципальної ланки управління кібербезпекою. Всі без винятку сектори на місцевому рівні знаходяться в «червоній зоні» ризику (нижче 50%), а найнижче значення зафіксовано у сфері інфраструктури і транспорту – 34,78%. Така депресивність показників свідчить про відсутність дієвих механізмів імплементації національної кіберстратегії на місцях.

Узагальнюючи дані, можна стверджувати, що вітчизняна система кібербезпеки характеризується моделлю «сильного центру та слабкої периферії». Якщо на загальнодержавному рівні сформовано дієву політику з високим рівнем спроможностей, то на місцевому та частково регіональному рівнях система перебуває у стані вразливості. Стратегічний розрив між центральними органами та місцевим самоврядуванням, а також специфічні провали в управлінні енергетичним комплексом на рівні ЦОВВ є головними бар'єрами для перетворення окремих державних спроможностей на цілісну та стійку національну екосистему кіберстійкості.

Аналіз наступного блоку показників, що стосуються рівня захисту цифрового середовища (мереж), дозволяє розширити розуміння архітектури національної кіберстійкості через призму регіональної диференціації та ієрархічної структури захисту (табл. 3.20). Застосування алгоритму оцінки ризиків (де поріг 50% розмежовує вразливість та спроможність) демонструє виразну тенденцію: чим ближче об'єкт захисту до індивідуального рівня або приватного сектору, тим вищим стає рівень системного ризику.

Таблиця 3.20

Рівень ризику щодо захисту цифрового середовища (мереж) (%)

Рівень захисту цифрового середовища (мереж)	ризик, %	РЕГІОНИ																								
		Вінницька	Волинська	Донецька	Дніпропетровська	Житомирська	Закарпатська	Запорізька	Івано-Франківська	м.Київ	Київська	Кіровоградська	Луганська	Львівська	Миколаївська	Одеська	Полтавська	Рівненська	Сумська	Тернопільська	Харківська	Херсонська	Хмельницька	Черкаська	Чернівецька	Чернігівська
на національному рівні	62,99	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
на місцевому рівні	49,17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
на рівні окремих підприємств	49,39	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
на індивідуальному рівні	44,46	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
щодо запобігання кібератакам	60,35	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
щодо створення базової безпеки в продуктах і послугах	55,25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
щодо допомоги приватним особам, малим підприємствам та організаціям з базовими заходами для покращення кібербезпеки	47,61	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
щодо подолання державними установами системних кібер-ризиків	53,78	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
щодо формування державними установами системної підтримки через рекомендації, інструменти, розвиток навичок та акредитацію на ринку	53,64	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

На верхньому щаблі ієрархії рівень захисту на національному рівні оцінюється у 62,99%, що свідчить про стійке позитивне значення спроможності та наявності стратегічного ресурсу для подальшого розвитку. Однак при переході до місцевого рівня (49,17%) та рівня окремих підприємств (49,39%) система перетинає критичну межу, потрапляючи в зону вразливості. Найбільш критичним є індивідуальний рівень (44,46%), який ідентифікується як зона високого ризику. Це вказує на те, що державні заходи захисту поки не

трансформуються у персональну захищеність громадян, створюючи «безпековий вакуум» на рівні кінцевого користувача.

У функціональному розрізі спостерігається позитивна динаміка в частині запобігання кібератакам (60,35%) та створення базової безпеки в продуктах і послугах (55,25%), що підтверджує наявність технічних спроможностей. Водночас сфера допомоги приватним особам та малому бізнесу (47,61%) залишається вразливою. Хоча державні установи демонструють спроможність щодо подолання системних ризиків (53,78%) та надання системної підтримки (53,64%), ефективність цих заходів наразі обмежена переважно державним сектором.

Детальний аналіз регіонального зрізу виявляє глибоку нерівномірність та специфічні локальні ризики. Миколаївська область демонструє аномально високий рівень довіри до національного захисту та високу спроможність у запобіганні атакам. На противагу цьому, Полтавська область фіксує критичну вразливість на індивідуальному рівні та найнижчий рівень захисту підприємств.

У Житомирській області спостерігається найбільший розрив між оцінкою національного рівня та рівня окремих підприємств. Це свідчить про критичну ізолюваність приватного сектору регіону від загальнодержавних систем кіберзахисту. Сумська область є одним із лідерів за рівнем захисту на місцевому рівні, що вказує на ефективну імплементацію заходів безпеки на рівні громад, попри прикордонний статус та постійні загрози. А Черкаська область є єдиним регіоном, де індивідуальний рівень захисту перетнув поріг спроможності, тоді як у решті областей цей показник стабільно перебуває в зоні ризику (нижче 50%). Водночас, столичний регіон демонструє збалансовані, але помірні показники, що, попри концентрацію ресурсів, вказує на високу вразливість через складність та масштабність міської цифрової інфраструктури.

Таким чином, регіональний аналіз підтверджує, що кіберстійкість України має «острівний» характер. Державна спроможність (ризик >50%) є

виразною на національному рівні та в частині стратегічного запобігання атакам. Проте «глибина» захисту залишається недостатньою: регіони з високим рівнем державного захисту можуть мати катастрофічні вразливості на рівні бізнесу та громадян. Це вимагає переходу від універсальних загальнодержавних рішень до диференційованої регіональної політики, спрямованої на ліквідацію локальних «зон мовчання» та підсилення індивідуальної захищеності.

Блок аналізу «Ефективність досягнення кіберстійкості: суб'єктно-рівневий зріз» дозволяє глибше зануритися в суб'єктивну архітектуру національної кіберстійкості, де оцінка ризиків та спроможностей безпосередньо залежить від відомчого профілю експертів (табл. 3.21). Використання алгоритму (де межа у 50% відділяє зону спроможності від зони вразливості) виявляє значну диференціацію у сприйнятті ефективності системи різними суб'єктами.

Таблиця 3.21

Рівень ризику щодо ефективності досягнення кіберстійкості суб'єктами (%)

Ефективність щодо досягнення кіберстійкості (прогнозування, запобігання, адекватного реагування та швидкого відновлення) в Україні:	Оцінка ризику, %	Експертне залучення за суб'єктом							
		ЦОВВ	ДСТЗІ	ОВА	РВА	П/О	Розвід. орган	ОКІ	Освіта / Наука
загальнодержавному	62,43	63,59	61,74	71,25	61,38	57,49	65,22	63,42	65,94
регіональному (область)	54,68	55,07	51,96	59,47	53,71	49,15	34,78	52,77	57,25
місцевому	48,25	43,12	45,22	49,79	48,08	46,38	34,78	49,18	53,62
окремих підприємств	51,35	54,17	47,17	48,81	47,57	54,59	65,22	54,72	53,14
індивідуальному	44,88	42,75	42,61	39,97	39,90	47,83	34,78	46,48	49,28
Здатність суб'єктів вітчизняної системи кібербезпеки:									
розбудовувати національну систему кіберстійкості	61,39	60,14	60,22	67,04	61,64	56,76	65,22	63,27	63,04
розробляти нові методи кіберзахисту	55,68	47,28	52,61	61,29	56,78	50,36	34,78	57,12	67,63

Аналіз ефективності прогнозування, запобігання та реагування на кібератаки підтверджує раніше виявлену тенденцію до високої централізації успішних практик. На загальнодержавному рівні середній показник спроможності становить 62,43%, що свідчить про стійку впевненість усіх груп експертів у дієвості національного контуру захисту. Проте деталізація за

суб'єктами виявляє цікавий феномен: найбільш оптимістично національну стійкість оцінюють представники обласних військових адміністрацій (РВА) – 71,25%, тоді як найбільш стриманими є представники правоохоронних органів – 57,49%. Це вказує на те, що оперативні підрозділи, які безпосередньо стикаються з прихованими загрозами, бачать більше прихованих ризиків у загальній системі, ніж адміністративні ланки.

При переході до місцевого рівня (48,25%) та індивідуального рівня (44,88%), система масово зміщується в зону системної вразливості. Єдиною експертною групою, яка оцінює місцевий рівень як спроможний, є представники освіти та науки (53,62%), що може свідчити про певну відірваність наукового дискурсу від реального операційного стану справ у громадах. На противагу їм, представники розвідувальних органів (34,78%) та ЦОВВ (43,12%) фіксують у цих сегментах критичний рівень ризику, що вимагає негайної трансформації політики підтримки кінцевих споживачів та дрібних суб'єктів.

Оцінка цільових спроможностей щодо розвитку системи виявляє стратегічний розрив між процесом побудови інфраструктури та процесом інтелектуального оновлення методів захисту. Всі групи експертів оцінюють здатність розбудови національної системи кіберстійкості (61,39%) як позитивну спроможність. Найвищий рівень довіри до цього процесу демонструють представники ОВА (67,04%) та оператори критичної інфраструктури (63,27%), що вказує на високу залученість реального сектору та регіонального менеджменту до стратегічного будівництва системи. Індикатор щодо розробки нових методів кіберзахисту (55,68%) демонструє значно вищу варіативність ризиків. Якщо представники освіти та науки бачать тут потужний потенціал (67,63%), то розвідувальні органи ідентифікують цей напрям як критичну вразливість (34,78%). Такий радикальний розрив в оцінках свідчить про те, що академічні напрацювання в Україні наразі недостатньо імплементуються в реальну розвідувальну та контррозвідувальну діяльність, створюючи ризик технологічного відставання від агресора.

Підсумовуючи дані за цим блоком, можна стверджувати, що вітчизняна система кібербезпеки тримається на «оптимізмі адміністраторів» та «скептицизмі оперативників». Рівень ризику, який фіксують спецслужби та правоохоронці у нижніх ланках системи (місцевий та індивідуальний рівні), значно перевищує оцінки, що надаються державними управліннями.

Це говорить про наявність у системі «інформаційних бульбашок»: вище керівництво та регіональні адміністрації можуть мати деформоване уявлення про реальну захищеність на місцях, сприймаючи високу ефективність центру як загальнодержавну тенденцію. Зокрема, критичний рівень ризику в інноваційному секторі (34,78% за оцінкою розвідки) є сигналом про те, що без інтеграції науки в практику та реальної підтримки індивідуальної безпеки громадян, загальнодержавні успіхи можуть бути знівельовані через вразливість «периферійних» вузлів системи.

Аналіз блоку індикаторів, що характеризують ефективність реагування на кіберінциденти (табл. 3.22), дозволяє оцінити не лише технічну готовність системи, а й професійну рефлексію різних фахових груп щодо результативності чинних механізмів захисту. Загальний показник спроможності на загальнодержавному рівні становить 66,33%, що є одним із найвищих значень у дослідженні та свідчить про сформовану та дієву систему оперативного реагування на макрорівні.

Аналіз оцінювання за фаховими групами виявляє суттєвий розрив у сприйнятті реальності. Аналітики демонструють найбільш високий рівень довіри до системи реагування, оцінюючи її на загальнодержавному рівні у 70,43%, а на рівні об'єктів критичної інфраструктури – у 68,70%. Це може бути пов'язано з їхнім безпосереднім залученням до обробки великих масивів даних та баченням загальної позитивної динаміки нейтралізації загроз.

Науковці, на противагу, виступають найбільш консервативною групою, надаючи стабільно нижчі оцінки. Їхній показник на загальнодержавному рівні становить лише 57,31%, а на місцевому рівні він опускається до 48,62%, що згідно з нашим алгоритмом переводить муніципальну ланку в зону системної

вразливості. Такий скептицизм вчених свідчить про глибше розуміння ними теоретичних прогалин та потенційних ризиків, які можуть бути непомітними в поточному оперативному процесі.

Таблиця 3.22

Рівень ризику щодо ефективності реагування на кіберінциденти (%)

Ефективність реагування на кіберінциденти на рівні:	Оцінка ризику, %	Менеджер	Фахівець, інспектор	Аналітик	Науковець
загальнодержавному	66,33	66,39	68,27	70,43	57,31
регіональному (область)	57,52	55,18	58,72	66,96	52,17
місцевому	51,13	50,06	50,45	61,74	48,62
правоохоронних, розвідувальних органів та безпеки	62,52	59,75	63,88	64,35	56,92
окремих підприємств-постачальників ІКТ послуг	57,84	56,80	58,63	68,70	52,17
окремих об'єктів критичної інфраструктури	59,59	57,97	61,21	68,70	54,94
індивідуальному	47,35	43,09	47,74	53,91	47,43

Менеджери та фахівці (інспектори) займають проміжну позицію, де практичне бачення інспекторів щодо реагування на рівні правоохоронних органів (63,88%) є вищим за оцінки менеджерів (59,75%). Це говорить про те, що на виконавчому рівні інструментарій реагування сприймається як більш ефективний, ніж на рівні стратегічного управління.

Трансформація спроможностей від центру до периферії підтверджує тенденцію поступової деградації ефективності. Сфера правоохоронних та розвідувальних органів (62,52%), а також об'єктів критичної інфраструктури (59,59%) демонструє стабільно позитивну спроможність. Це вказує на те, що державний ресурс сфокусований на захисті найбільш чутливих вузлів системи.

Водночас, показник у 51,13% формально залишає місцевий рівень у зоні спроможності, проте фактично він знаходиться на межі ризику. Враховуючи, що наукова спільнота вже оцінює цей сегмент як вразливий (48,62%), муніципальне реагування на кіберінциденти ідентифікується як «слабка ланка», що тримається на мінімально допустимому рівні.

Важливо зазначити, що з середнім показником 47,35% індивідуальний сегмент офіційно визнається зоною вразливості. Примітно, що навіть за умови оптимізму аналітиків (53,91%), оцінки менеджерів (43,09%) та науковців (47,43%) чітко вказують на неспроможність системи забезпечити адекватне реагування на інциденти, що стосуються приватних осіб та індивідуальних користувачів.

Таким чином, система реагування на кіберінциденти в Україні має виражений «професійно-орієнтований» характер. Вона ефективна там, де працюють спеціалізовані структури (аналітики, розвідка, КІІ), але практично нівелюється на рівні громадянина. Розрив в оцінках між аналітиками та науковцями вказує на відсутність єдиного бачення ефективності: поки практика (аналітика) звітує про успіхи, наука попереджає про глибокі системні ризики на нижчих рівнях. Це вимагає впровадження заходів щодо «горизонтальної» стабілізації системи, підтягування індивідуальної та місцевої спроможностей до рівня національних стандартів.

Аналіз блоку показників, що стосуються співпраці з приватним сектором та захисту інтернет-користувачів (табл. 3.23), дозволяє оцінити стан «колективного імунітету» цифрового простору України. Даний сегмент фокусується на найбільш динамічних аспектах кіберстійкості: від адаптації до нових методів атак і до формування цифрових навичок населення. Загальний профіль цього блоку демонструє гранично позитивні значення (50,04% – 56,81%), що свідчить про перехідний стан системи від пасивного захисту до активної розбудови екосистеми стійкості.

Аналіз оцінювання за експертним досвідом виявляє глибоку диференціацію сприйняття ризиків, що безпосередньо залежить від тривалості фахової діяльності. Група з досвідом 1–3 роки виступає найбільш оптимістичним сегментом, надаючи найвищі оцінки стійкості до нових методів атак (58,19%) та розумінню суб'єктами потреби в розбудові системи (58,00%). Це може свідчити про високу адаптивність молодого покоління

фахівців до сучасних технологічних трендів та їхню віру в ефективність нових інструментів.

Таблиця 3.23

Рівень ризику щодо співпраці з приватним сектором та захисту інтернет-користувачів (%)

Рівень співпраці з провайдерами онлайн-послуг, телекомунікаційних технологій, банківським сектором і роздрібною торгівлею щодо кращого захисту українських інтернет-користувачів	Оцінка ризику, %	До 1-го року	1-3 роки	3-10 років	10-20 років	більше 20 років
Рівень стійкості до поширених нових методів кібератак	56,81	56,75	58,19	56,01	56,52	50,59
Рівень цільового законодавчого забезпечення секторів, де потенційний вплив кібератак є найбільшим, включаючи постачальників певних основних та цифрових послуг, захист даних в економіці в цілому, та для великого бізнесу	53,81	54,16	53,75	53,13	53,16	55,73
Розробленість та доступність стимулів, технічних порад, інструментів самопомоги, а також гарантованих продуктів та послуг, для підвищення кіберстійкості громадян, фізичних осіб-підприємців та малих підприємств.	52,17	51,14	53,75	51,51	50,79	55,73
Організаційне, фінансове забезпечення та доступність формування цифрових навичок громадянами усіх вікових груп	50,04	49,50	51,99	48,56	47,04	52,96
Рівень допомоги підприємствам та організаціям в орієнтуванні на складному ринку кібербезпеки, розширюючи рамки гарантованих продуктів і послуг та полегшуючи малим підприємствам доступ до базових консультацій	51,30	51,03	52,91	51,07	46,44	51,38
Рівень розуміння суб'єктами системи кібербезпеки необхідності розбудови національної системи кіберстійкості	55,52	53,59	58,00	54,90	57,91	52,96

Експерти зі стажем 10–20 років демонструють найбільш виражений критицизм, ідентифікуючи ключові системні провали. Саме ця група оцінює організаційне та фінансове забезпечення цифрових навичок (47,04%) та рівень допомоги бізнесу в орієнтуванні на ринку (46,44%) як зони прямої вразливості (ризик нижче 50%). Такий скептицизм досвідчених фахівців вказує на виявлення ними глибоких структурних недоліків, які не завжди помітні на рівні оперативної діяльності. Водночас, ветерани галузі (стаж понад 20 років) проявляють «зважений скептицизм». Їхня оцінка стійкості до нових методів атак (50,59%) знаходиться на межі вразливості, що підкреслює їхнє розуміння циклічності загроз та постійної гонитви озброєнь у кіберпросторі. При цьому

вони вище за інших оцінюють потенціал цільового законодавства (55,73%) та доступність інструментів самодопомоги (55,73%), вбачаючи в системності та регуляції головну опору стійкості.

Незважаючи на варіативність оцінок, система демонструє стійкі позитивні індикатори в стратегічних напрямках. Стійкість до нових методів кібератак (56,81%) є найбільш зрілою спроможністю в цьому блоці. Це підтверджує високу адаптивність вітчизняного ринку та фахівців до поширених загроз, що постійно еволюціонують. Розуміння необхідності розбудови національної системи кіберстійкості (55,52%) свідчить про сформований консенсус серед суб'єктів щодо стратегічного вектора розвитку. Це критично важливий показник, оскільки спільне бачення мети є передумовою успішної координації. Цільове законодавче забезпечення (53,81%) також перебуває в зоні спроможності, що вказує на функціональність нормативно-правової бази для основних секторів економіки.

Найбільш тривожним сигналом є стан організаційного та фінансового забезпечення формування цифрових навичок громадян (50,04%). Це значення знаходиться на самій межі вразливості. Враховуючи, що експерти з досвідом 3–10 та 10–20 років вже оцінюють цей напрям нижче 50% (48,56% та 47,04% відповідно), можна констатувати наявність системної кризи в освітньо-фінансовій підтримці населення. Без дієвих заходів у цій сфері «людський фактор» залишатиметься головним джерелом ризику для всієї національної системи.

Також у зоні підвищеного ризику знаходиться допомога підприємствам в орієнтуванні на ринку кібербезпеки (51,30%). Низька оцінка цього показника експертами середньої та вищої ланки свідчить про відсутність прозорих механізмів підтримки малого та середнього бізнесу, що робить його легкою мішенню для фінансово-мотивованих атак.

Таким чином, співпраця з провайдерами та захист користувачів в Україні наразі базуються на високій адаптивності фахівців та стратегічному розумінні проблем. Проте система має критично слабку «гуманітарну»

складову: фінансування навчання громадян та підтримка бізнесу на ринку є недостатніми. Розрив в оцінках між поколіннями експертів вказує на потребу в «інституційній пам'яті» та врахуванні досвіду ветеранів для посилення вразливих ділянок, які молоді фахівці можуть недооцінювати.

Аналіз блоку показників, присвячених посиленню стійкості на національному та організаційному рівнях (табл. 3.24), дозволяє оцінити якість «командної гри» суб'єктів кібербезпеки та рівень їхньої готовності до скоординованих дій у кризових ситуаціях. Цей сегмент дослідження охоплює аспекти стратегічного управління, прозорості інформування та професійної підготовки через призму практичних навчань. Загальний профіль показників (від 51,39% до 58,35%) свідчить про наявність сформованої інституційної бази, проте експертне залучення за суб'єктами виявляє глибокі розбіжності в оцінці функціональності цих механізмів.

Рівень ефективності стратегічного управління та координації (58,35%) оцінюється експертами як стійка позитивна спроможність. Найбільшу впевненість у дієвості державного менеджменту висловлюють розвідоргани – 65,22% та представники обласних військових адміністрацій (РВА) – 61,71%. Водночас правоохоронні органи демонструють більш стриману позицію (54,95%), що може вказувати на наявність процедурних бар'єрів у процесах оперативної взаємодії між цивільними та силовими структурами.

Високу оцінку отримала компетентність фахівців державних органів (56,54%). Примітно, що представники розвідувальних органів (65,22%) та ЦОВВ (61,23%) оцінюють потенціал кадрів значно вище за середній рівень. Проте оцінка з боку РВА (51,15%) знаходиться на межі вразливості, що вказує на кадровий дефіцит або недостатній рівень фахової підготовки управлінців саме на низових ланках державної служби.

Сфера інформаційної прозорості демонструє наявність «критичних точок» у сприйнятті суб'єктами. Доступність повідомлень про кіберінциденти (55,99%) сприймається як спроможність більшістю груп, особливо ЦОВВ (61,78%) та ОВА (61,15%). Однак розвідувальні органи (47,83%)

ідентифікують цей напрям як зону вразливості. Це говорить про те, що фахівці, які працюють із закритими даними, вважають існуючі канали публічного або міжвідомчого інформування недостатньо ефективними або безпечними.

Таблиця 3.24

Рівень ризику щодо посилення стійкості на національному та організаційному рівнях (%)

Посилення стійкості на національному та організаційному рівнях, реагування на кібератаки та відновлення після них	Оцінка ризику, %	Експертне залучення за суб'єктом							
		ЦОВВ	ДСТЗІ	ОВА	РВА	П/О	Розвід. орган	ОКІ	Освіта / Наука
Рівень ефективності стратегічного управління в державі та координації реагування на національно значущі кіберінциденти	58,35	59,42	60,00	61,71	60,87	54,95	65,22	56,52	57,00
Доступність повідомлень про кіберінциденти	55,99	61,78	54,57	61,15	54,99	53,02	47,83	53,22	60,14
Рівень мотивації розвитку оповіщення нетрадиційними способами про кіберінциденти	51,39	48,19	45,87	48,95	49,10	52,42	34,78	56,07	57,97
Рівень планування та проведення регулярних навчань щодо реагування на випадок інцидентів та відновлення після них	53,46	49,46	50,65	52,73	53,71	53,62	47,83	54,87	56,76
Рівень включення кібер-аспектів у національні навчання з врегулювання кризових ситуацій	52,90	51,27	52,17	52,59	53,71	53,14	47,83	51,42	60,87
Рівень проведення національних командно-штабних навчань із включенням різних відомств, відповідальних за надання критично важливих послуг, представників приватного сектору і ключовий персонал органів державного управління	54,61	55,80	53,48	57,50	57,03	54,83	65,22	51,87	59,66
Рівень компетентності фахівців державних органів щодо управління кіберінцидентами, наявності відповідного потенціалу та можливостей реагування ними на весь спектр кіберінцидентів, із врахуванням майбутніх змін	56,54	61,23	59,35	58,91	51,15	54,83	65,22	54,27	60,87

Мотивація до нетрадиційного оповіщення (51,39%) є найбільш проблемним індикатором. Оцінки представників розвідувальних органів (34,78%), а також ДСТЗІ (45,87%), ОВА (48,95%) та ЦОВВ (48,19%) одноставно свідчать про глибоку вразливість. Це вказує на консервативність системи: державні органи не готові до впровадження альтернативних чи гнучких способів обміну даними, що в умовах гібридної війни може призводити до інформаційного запізнення. Позитивний баланс тут тримають

лише освіта/наука (57,97%) та ОКІ (56,07%), які більше орієнтовані на інноваційні підходи.

Показники щодо проведення навчань (53,46%) та включення кібер-аспектів у національні тренінги (52,90%) перебувають у позитивній зоні, але мають потенціал до зростання. Високий рівень довіри до командно-штабних навчань (54,61%) з боку розвідувальних органів (65,22%) та ОВА (57,50%) підтверджує, що цей формат є найбільш ефективним інструментом відпрацювання взаємодії. Наукова спільнота також високо оцінює інтеграцію кібер-аспектів у загальнонаціональні навчання (60,87%), що вказує на якісну теоретичну проробку сценаріїв кризових ситуацій.

Таким чином, стратегічна стійкість України наразі базується на високій компетентності центру та перевірених форматах штабної роботи. Проте в системі спостерігається «страх інновацій»: поки традиційні методи управління та навчання працюють добре (ризик > 50%), будь-які спроби впровадження нетрадиційних способів оповіщення сприймаються спецслужбами та регуляторами як небезпечна вразливість (ризик < 35-46%). Це створює парадокс: система є «стійкою, але застиглою», що у довгостроковій перспективі може стати ризиком при зустрічі з принципово новими, динамічними методами агресії.

Аналіз фінального блоку показників, що стосуються сфери науки та освіти (табл. 3.25), виявляє найбільш критичну зону в системі національної кіберстійкості. Цей сектор є фундаментом для підготовки кадрів та розробки інноваційних методів захисту, проте результати оцінювання свідчать про стан системної крихкості. Загальний профіль показників коливається від 46,03% до 51,45%, що вказує на те, що більшість індикаторів або знаходяться на межі ризику, або вже перетнули поріг вразливості.

Аналіз оцінювання різними фаховими групами демонструє найвищий рівень полярності думок у всьому дослідженні. Аналітики залишаються незмінними оптимістами, оцінюючи всі без винятку показники науково-освітнього блоку в межах 53,04% – 60,87%.

Рівень ризику за науковим та освітнім сегментом кіберстійкості (%)

НАУКА / ОСВІТА	Оцінка ризику, %	Менеджер	Фахівець, інспектор	Аналітик	Науковець
Рівень науково-методичного забезпечення у сфері кібербезпеки	51,45	51,11	52,00	60,87	45,45
Рівень взаємозв'язку науки і практики у сфері кібербезпеки	51,19	51,39	50,67	53,04	47,43
Рівень фахової освіти за спеціальністю «Кібербезпека» у закладах вищої освіти	51,32	49,83	52,04	58,26	46,64
Рівень фінансового забезпечення наукової та дослідницької діяльності у сфері кібербезпеки	46,80	45,26	46,45	53,04	43,08
Рівень пріоритетності фінансування прикладних і теоретичних досліджень в галузі інформатики	46,03	44,76	45,93	53,04	45,45
Рівень заохочення міждисциплінарних кібердосліджень для підготовки покоління осіб, які приймають рішення, аналітиків	46,48	46,54	45,20	53,04	43,08

Таке бачення свідчить про те, що з погляду зовнішнього спостерігача (аналітика) система виглядає спроможною та забезпеченою. Науковці, які є безпосередніми суб'єктами цієї сфери, демонструють радикально протилежну думку. Всі їхні оцінки знаходяться в зоні вразливості (нижче 50%). Найнижчі бали вони виставляють фінансовому забезпеченню та міждисциплінарним дослідженням (43,08%). Це свідчить про глибоку внутрішню кризу, яку фахівці зсередини відчувають значно гостріше, ніж зовнішні експерти. Водночас, менеджери та фахівці займають граничну позицію, де рівень фахової освіти у ЗВО оцінюється ними на межі (49,83% – 52,04%), що підтверджує нестабільність якості підготовки нових кадрів.

У функціональному розрізі блок «Наука / Освіта» чітко розпадається на дві зони:

зона граничної спроможності (51,19% – 51,45%). Сюди відносяться рівень науково-методичного забезпечення та фахової освіти. Хоча середні значення формально перебувають у позитивній зоні, оцінки науковців (нижче 47%) вказують на те, що цей успіх є скоріше декларативним, ніж фактичним.

зона відкритої вразливості (46,03% – 46,80%). Всі індикатори, пов'язані з фінансуванням та пріоритетністю досліджень, впали нижче критичної позначки в 50%. Це означає, що система кібербезпеки України має «порожній бак» у частині майбутніх розробок. Низький рівень заохочення міждисциплінарних досліджень (46,48%) говорить про те, що підготовка майбутніх лідерів, здатних приймати складні рішення, наразі не є пріоритетом.

Особливу тривогу викликає найнижчий показник у всьому блоці – пріоритетність фінансування прикладних і теоретичних досліджень (46,03%). Це свідчить про те, що держава та приватний сектор сфокусовані на «гасінні пожеж» (реагуванні), ігноруючи потребу в створенні власного інтелектуального продукту. Без теоретичної бази система приречена на постійне наздоганяння технологій агресора.

Таким чином, сфера науки та освіти в контексті кіберстійкості є «ахіллесовою п'ятою» національної безпеки. Ми спостерігаємо парадоксальну ситуацію: аналітики вірять у світле майбутнє науки, тоді як самі науковці констатують фінансове та організаційне виснаження. Згідно з нашим алгоритмом, цей блок потребує негайного впровадження «дієвих заходів поліпшення», оскільки рівень ризику тут є системним. Без радикального перегляду фінансової політики та об'єднання зусиль науки і практики, Україна ризикує залишитися з високою оперативною спроможністю (реагування), але без стратегічної глибини (інновації).

Результати проведеного прикладного дослідження (цього та попереднього підрозділів), що зафіксували реальний стан та динаміку показників кіберстійкості, створюють необхідне підґрунтя для переходу від діагностичного етапу до етапу стратегічного нормопроєктування. У сучасному правознавстві такий підхід базується на методологічній концепції Evidence-based Lawmaking (нормотворення на основі фактичних даних), яка передбачає, що розробка правових норм має спиратися на верифіковані емпіричні докази та кількісний аналіз реальних суспільних відносин.

Відповідно до поглядів прибічників цієї концепції, правова норма не може бути продуктом виключно умоглядної дедукції, а має виступати інструментом вирішення об'єктивно зафіксованих проблем. Теоретичне коріння цього підходу простежується ще у працях Р. Паунда, який розглядав право як інструмент «соціальної інженерії», покликаний вирішувати конкретні суспільні проблеми на основі наукового вивчення соціальних фактів [370]. У сучасному контексті ця ідея розвивається у межах парадигми *Evidence-Based Policy*, де Н. Картрайт (Nancy Cartwright) наголошує на необхідності прогнозування ефективності політики через детальний аналіз локальних умов та фактичних спроможностей [191].

Застосування принципів *Evidence-based Lawmaking* дозволяє подолати суб'єктивізм у законотворчості та забезпечити функціональну результативність нормативних приписів. Виявлені «зони вразливості» (ризик < 50%) ідентифікуються як прогалини в правовому регулюванні, що потребують оперативного заповнення. Таким чином, отримані аналітичні висновки трансформуються у нормативний імператив: кожна точка системного ризику отримує відповідний правовий «рецепт» у формі конкретних пропозицій щодо вдосконалення інституційної структури, перерозподілу повноважень суб'єктів кібербезпеки та впровадження нових режимів відповідальності.

Визначена методологічна база і формує підстави для подальшого вироблення пропозицій щодо удосконалення правового регулювання у сфері кіберстійкості. Перш за все, необхідно вказати на необхідність юридичної детермінації переходу до моделі спроможностей. Концептуальна зміна вектору національної безпеки з реактивного захисту на проактивну стійкість потребує насамперед чіткої юридичної детермінації основних категорій. Чинне законодавство України здебільшого оперує терміном «кібербезпека», що за своєю суттю фокусується на стані захищеності та мінімізації вразливостей. Однак емпіричні дані підтверджують, що в умовах гібридної війни

ефективність системи визначається не відсутністю інцидентів, а спроможністю до поглинання удару та адаптації.

Першочерговим кроком є внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України» в частині розширення термінологічного апарату. Пропонується дефініція «кіберстійкості» як динамічної здатності національної кіберсистеми передбачати, витримувати, відновлювати функціональність та адаптуватися до деструктивних впливів у цифровому просторі. Юридичне виокремлення стійкості від безпеки дозволить сформулювати нові об'єкти правового регулювання: не лише технічні засоби захисту, а й процеси життєздатності критичних функцій держави. Це створить правове підґрунтя для переходу від оцінювання «наявності засобів захисту» до оцінювання «ефективності реагування та відновлення».

Важливим є запровадження обов'язковості ризик-орієнтованого матричного підходу. На основі апробованої у розділі 3.3 матриці кіберстійкості (фізичний, інформаційний, когнітивний та соціальний домени), необхідно нормативно закріпити обов'язковість проведення періодичного стрес-тестування для суб'єктів критичної інформаційної інфраструктури (КІІ). На відміну від класичного аудиту інформаційної безпеки, такий аудит стійкості повинен мати статус юридично значущої перевірки здатності суб'єкта до функціонування в умовах часткової компрометації мереж.

Юридична імплементація цього підходу має включати:

встановлення критеріїв «прийнятного рівня деградації сервісу» для об'єктів КІІ під час атаки;

правове визначення обов'язкових резервних спроможностей, що корелює з нашим висновком про необхідність підсилення фізичного домену стійкості;

перегляд стандартів звітності, де акцент зміщується з факту виявлення вразливості на швидкість відновлення бізнес-процесу.

Юридична детермінація спроможностей вимагає визнання «інформаційних потоків» та «координаційних зв'язків» (соціальний домен)

об'єктами пріоритетної правової охорони. Оскільки дослідження виявило, що координація на етапі планування є слабкою ланкою, правове регулювання повинно вийти за межі охорони «даних у спокої» до охорони «безперервності процесів». Це потребує розробки підзаконних актів, які б регламентували юридичну відповідальність не за факт витоку даних, а за неспроможність забезпечити функціонування сервісу у визначений регламентом час.

Таким чином, юридична детермінація переходу до моделі спроможностей створює умови, за яких право не просто фіксує статичний стан безпеки, а стимулює динамічну живучість системи. Це дозволяє легалізувати адаптивні механізми захисту, що є критично важливим для подолання виявленого нами розриву між технічною готовністю центру та організаційною вразливістю регіональних структур.

Важливим є питання адміністративно-правового подолання «безпекового розриву». Емпіричне дослідження спроможностей продемонструвало критичну деградацію стійкості при переході від загальнодержавного до місцевого рівня. Юридична природа цього «безпекового розриву» полягає у відсутності чіткої вертикалі відповідальності та правової невизначеності ролі органів місцевого самоврядування у національній системі кібербезпеки. Поточна модель, де основний тягар відповідальності покладено на центральні органи (ЦОВВ), не враховує децентралізацію цифрових послуг, що робить громади найбільш вразливими точками входу для системних кібератак.

На основі виявленого успішного досвіду «полюсів стійкості», пропонується законодавчо закріпити створення регіональних центрів кіберстійкості при Обласних військових адміністраціях (ОВА). Необхідно внести зміни до положень про НКЦК при РНБО України щодо делегування частини координаційних повноважень на рівень областей. Це дозволить легалізувати горизонтальні зв'язки між регіональними підрозділами СБУ, Держспецзв'язку та місцевою владою, перетворюючи їх із пасивних виконавців на суб'єктів формування локальної політики стійкості.

Оскільки аналіз зафіксував вразливість муніципальної ланки, правове регулювання має зміститися у площину стандартизації. Пропонується:

розробити та затвердити на рівні Кабінету Міністрів України Типове положення про цифрову безпеку територіальної громади, яке б визначало обов'язковий перелік заходів із захисту реєстрів та комунальних сервісів;

запровадити правовий інститут «муніципального офіцера з кібербезпеки» або делегування цих функцій спеціалізованим сервісним центрам на умовах аутсорсингу, що дозволить вирішити проблему кадрового дефіциту в регіонах;

юридично закріпити механізм «субвенцій на кіберстійкість» – цільового фінансування з державного бюджету для технічного переоснащення найбільш вразливих громад.

Необхідно забезпечувати регламентацію міжвідомчої взаємодії в кризових умовах. Виявлений у дослідженні скептицизм оперативних підрозділів вказує на правовий вакуум у питаннях обміну інформацією між «центром» та «місцями». Необхідно нормативно визначити протоколи передачі повноважень від місцевого рівня до національних центрів реагування (CERT-UA) у разі перевищення певного порогу деградації системи. Це дозволить юридично зняти з місцевих управлінців відповідальність за інциденти, що мають загальнодержавне значення, та забезпечити швидке залучення ресурсів національного рівня.

Потребує уваги і процес легалізації регіональних планів безперервності. На основі матричного аналізу соціального домену, необхідно зобов'язати органи місцевого самоврядування розробляти та погоджувати з Держспецзв'язку локальні плани безперервності критичних сервісів (водопостачання, тепломережа, транспорт). Юридичне визнання таких планів обов'язковими компонентами цивільного захисту дозволить інтегрувати кібербезпеку в загальну систему безпеки життєдіяльності регіону.

Таким чином, адміністративно-правова реформа повинна перетворити регіони з «об'єктів захисту» на «суб'єктів стійкості». Це дозволить подолати

ідентифікований «острівний» характер кібербезпеки України, забезпечивши рівномірний розподіл спроможностей по всій вертикалі державного управління та гарантуючи захищеність кожного громадянина незалежно від місця проживання.

Одним з ключових напрямів є спрямування правових інструментів на зміцнення гуманітарного домену та підтримки цифрової екосистеми. Аналіз соціального та когнітивного доменів у підрозділі 3.3 виявив критичну інертність системи щодо впровадження інноваційних методів комунікації та підтримки приватного сектору. Показник мотивації до нетрадиційного оповіщення свідчить про те, що чинне правове поле є занадто ригідним, що стримує гнучкість системи в умовах динамічних кіберзагроз.

Для подолання виявленої вразливості щодо нетрадиційних та децентралізованих способів оповіщення необхідно нормативно розширити перелік допустимих каналів обміну інформацією про кіберінциденти. З цією метою пропонується внести зміни до профільних постанов Кабінету Міністрів України, які б дозволили суб'єктам КІІ використовувати верифіковані децентралізовані платформи та захищені месенджери як допоміжні канали оперативного інформування. Також, важливим аспектом є впровадження правового режиму «Safe Harbor» (безпечна гавань) для суб'єктів, які добровільно та оперативно повідомляють про виявлені аномалії через неформальні канали, звільняючи їх від адміністративної відповідальності у разі, якщо таке повідомлення допомогло локалізувати атаку на національному рівні.

Оскільки рівень допомоги індивідуальним користувачам та малим формам бізнесу перебуває у зоні ризику, правове регулювання повинно стимулювати державне-приватне партнерство. Необхідно розробити нормативну базу для функціонування «Кібер-волонтерства» та «Кібер-резерву», надавши таким об'єднанням правовий статус помічників суб'єктів забезпечення кібербезпеки. Пропонується також запровадження механізму «Кібер-ваучерів» – державної субсидії для малих підприємств на отримання

базових консультацій або аудитів від акредитованих приватних компаній. Це дозволить подолати ідентифікований у дослідженні бар'єр складності ринку для малого бізнесу.

Важливим є нормативне забезпечення цифрових навичок як елемента національної безпеки. Зважаючи на межовий стан показника фінансового забезпечення цифрових навичок, пропонується юридично закріпити статус «цифрової грамотності» як компонента цивільного захисту. Це передбачає внесення змін до освітніх стандартів та трудового законодавства щодо обов'язкового періодичного тестування («кібер-чекап») працівників державного сектору та критичної інфраструктури. Правове регулювання має змістити акцент з формального навчання на ігрове та симуляційне тренування (Cyber Range), що за результатами нашого аналізу значно вище оцінюється фахівцями (домени відновлення та адаптації).

Надзвичайно ефективним є використання потенціалу «етичних хакерів», які водночас, потребують правового захисту. Для підвищення рівня стійкості інформаційного домену, необхідно декриміналізувати та нормативно врегулювати діяльність із пошуку вразливостей у державних інформаційних системах. Створення правового поля для етичного тестування дозволить використовувати зовнішній інтелектуальний ресурс для зміцнення національної інфраструктури, що особливо актуально на фоні низьких показників внутрішнього фінансування науки.

Таким чином, удосконалення правового регулювання у гуманітарній сфері має на меті перетворити «пасивного користувача» на «активного учасника» системи кіберстійкості. Це дозволить заповнити прогалини у соціальному домені та створити адаптивне середовище, де швидкість обміну інформацією та рівень навичок громадян стануть надійним бар'єром проти гібридних впливів.

Емпіричне дослідження виявило критичну депресивність показників фінансового та організаційного забезпечення наукової діяльності. Скептицизм самих науковців щодо фінансування на фоні відірваності академічних

розробок від практичних потреб правоохоронних органів свідчить про системний розрив у ланцюгу *«ідея – розробка – впровадження»*. Без правової реанімації науково-інноваційного циклу та стимулювання кібердосліджень, національна система кіберстійкості втратить свою стратегічну глибину та здатність до випереджальної адаптації.

Для подолання виявленої вразливості пропонується запровадження моделі цільового фінансування прикладних досліджень, для чого необхідно розробити та прийняти Закон України «Про стимулювання інновацій у сфері кібербезпеки та кіберстійкості». Юридичний механізм має передбачати створення Державного фонду кіберінновацій, наповнення якого здійснюватиметься шляхом фіксованих відрахувань від ліцензійних зборів у сфері телекомунікацій та штрафів за порушення законодавства про захист персональних даних. Крім того, доцільним є законодавче закріплення частки (не менше 1%) бюджетних призначень сектору безпеки та оборони на проведення НДДКР (науково-дослідних та дослідно-конструкторських робіт) виключно за напрямом кіберстійкості. Це дозволить перетворити фінансування з «залишкового» на «пріоритетне».

Важливою залишається правова інтеграція науки та оперативної практики. З огляду на низький рівень взаємозв'язку науки і практики, необхідно нормативно легалізувати формати прямої взаємодії. Пропонується внести зміни до КПК України та законів про розвідувальну діяльність, які б дозволили залучати наукові установи як офіційних експертних контрб'юторів до аналізу складних кіберінцидентів. Також, необхідно на рівні Кабінету Міністрів України затвердити Порядок функціонування національних наукових кібер-полігонів, що забезпечить науковцям правовий доступ до знеособлених масивів даних про реальні атаки для розробки прогностичних моделей, що є відповіддю на потребу в когнітивній адаптації.

Стимулювання міждисциплінарних кібердосліджень передбачатиме зміну логіки підготовки кадрів. Пропонується запровадження юридичного статусу «міждисциплінарних освітньо-наукових центрів кіберстійкості»

(Cyber Resilience Hubs) на базі провідних ЗВО. Важливо також нормативно забезпечити створення спільних магістерських програм на стику права, психології (когнітивний домен), соціології та комп'ютерних наук. Це дозволить готувати «покоління осіб, які приймають рішення», здатних розуміти соціально-правові наслідки технічних рішень.

Сучасним викликом для України є захист інтелектуальної власності у сфері оборонних кібертехнологій. Створення правового режиму «військової інтелектуальної власності» для розробок у сфері кіберзахисту дозволить збалансувати секретність державних розробок із можливістю їх комерціалізації приватними розробниками після демілітаризації технологій. Це стимулюватиме приплив приватного капіталу в наукові дослідження, що наразі ідентифікується як критична прогалина.

Таким чином, правове регулювання наукового циклу має на меті перетворити науку з «теоретичного додатка» на «інтелектуальний двигун» стійкості. Юридична консолідація фінансових ресурсів та оперативних даних дозволить Україні перейти від закупівлі іноземних рішень до генерації власних адаптивних технологій, що є єдиним шляхом подолання технологічної залежності в умовах довготривалої війни.

Водночас, емпіричні дані чітко вказують на те, що індивідуальна захищеність є найслабшою ланкою національної архітектури безпеки. Низький рівень спроможності на індивідуальному рівні та незадовільна оцінка захисту приватних осіб свідчать про те, що чинне законодавство сприймає громадянина переважно як «об'єкт» захисту, а не як повноправного «суб'єкта» з власними правами та обов'язками у кіберпросторі.

На законодавчому рівні пропонується закріпити «Права на кіберзахист» як базового цифрового права та запровадити концепцію «мінімального гарантованого рівня цифрової безпеки». Це передбачає внесення змін до Закону України «Про захист прав споживачів» у частині обов'язкової відповідності цифрових продуктів і послуг стандартам кіберстійкості. А також юридичне визнання того, що неспроможність державного органу або

провайдера забезпечити базовий захист персональних даних громадянина є порушенням його конституційного права на приватність, що тягне за собою спрощену процедуру відшкодування шкоди.

Враховуючи вразливість базової безпеки в продуктах, необхідно нормативно закріпити відповідальність розробників та постачальників програмного забезпечення, що використовується в державному секторі та КІІ. Запровадження обов'язкової сертифікації для розробників ПЗ, що підтверджує використання принципів безпечного проектування та юридичне визначення терміну «цифрова недбалість» для компаній, які свідомо ігнорують виправлення критичних вразливостей у продуктах, що призвело до масових інцидентів на індивідуальному рівні.

Удосконалення правового регулювання передбачає і індивідуальну відповідальність та «кібер-гігієну». Трансформація громадянина у суб'єкта права передбачає не лише захист, а й підвищення рівня правової культури. Пропонується розробка правових механізмів, які б заохочували громадян до підвищення власної кіберстійкості (наприклад, пільгові умови страхування або отримання певних цифрових послуг за умови проходження сертифікованого курсу з кібергігієни). Важливим є захист цифрової ідентичності на основі посилення кримінальної та адміністративної відповідальності за крадіжку цифрової особистості, що наразі ідентифікується як один із найбільш зростаючих ризиків для індивідуального рівня.

І на завершення, емпіричні дані та висновки чітко вказують на необхідність юридичного захисту малого та середнього бізнесу. Оскільки малі підприємства часто потрапляють у «правову лагуну» між великим бізнесом та фізичними особами, необхідно створити спеціальний правовий режим їх підтримки. Це передбачатиме запровадження спрощених протоколів звітування про кіберінциденти для малого бізнесу та створення правових підстав для безкоштовного надання державними центрами реагування (CERT-UA) базових інструментів захисту та відновлення для суб'єктів малого підприємництва у разі масових атак.

Таким чином, проведені дослідження інституційної спроможності та аналіз емпіричних даних дозволяють сформулювати цілісну концепцію поточної моделі кіберстійкості України та визначити стратегічні орієнтири її подальшого розвитку.

1. *Трансформація парадигми.* Обґрунтовано необхідність концептуального переходу від реактивної моделі «кібербезпеки» (усунення вразливостей) до проактивної моделі «кіберстійкості» (нарощування спроможностей). Доведено, що в умовах гібридної агресії спроможність системи поглинати удари та швидко відновлюватися є більш критичною характеристикою, ніж абсолютна захищеність периметра.

2. *Диспропорція «Центр – Периферія».* Аналіз ефективності державної політики виявив модель «сильного центру» (ризик > 59%) та «вразливої периферії». Якщо на загальнодержавному рівні сформовано дієву систему управління, то на місцевому та індивідуальному рівнях показники спроможності стабільно перебувають у зоні ризику (нижче 50%). Це свідчить про наявність «безпекового розриву», де пересічний громадянин та малий бізнес залишаються найбільш незахищеними ланками національної екосистеми.

3. *Технологічне випередження над гуманітарним фактором.* Емпіричне оцінювання за матричною моделлю показало, що інформаційний та фізичний домени (технічна база) розвиваються швидше, ніж когнітивний та соціальний (процеси ухвалення рішень та координація). Найвищий показник здатності до відновлення зафіксовано в інформаційній сфері, тоді як соціальна координація на етапі планування є найбільш вразливою.

4. *Суб'єктний дисонанс.* Виявлено суттєву різницю у сприйнятті ризиків різними групами експертів. «Оптимізм адміністраторів» (високі оцінки від ОВА/РВА) контрастує зі «скептицизмом оперативників та науковців» (низькі оцінки від розвідувальних органів та вчених). Зокрема, критичний рівень вразливості в інноваційному секторі та міждисциплінарних дослідженнях

(ризик < 46%) вказує на загрозу «теоретичного голодування» системи в майбутньому.

5. Регіональна децентралізація ризиків. Регіональний зріз підтвердив неоднорідність кіберпростору України. Наявність локальних «полюсів стійкості» (наприклад, Сумська область у місцевому захисті) та «зон глибокої вразливості» (Закарпатська область у захисті підприємств) вимагає переходу від уніфікованих рішень до диференційованої регіональної політики кібербезпеки.

Таким чином, побудова прогностичної моделі кіберстійкості України потребує негайного зміщення фокусу з технічного зміцнення центру на інституційну підтримку периферії: фінансування прикладних наукових досліджень, підвищення індивідуальної захищеності громадян та вдосконалення соціальної координації. Тільки через подолання «внутрішнього цифрового розриву» та інтеграцію науки в оперативну практику Україна зможе трансформувати свою поточну витривалість у сталу стратегічну перевагу.

Удосконалення правового регулювання, запропоноване у даному розділі, базується на принципі «стійкість через право». Замість декларативних закликів до безпеки, ми пропонуємо жорстку юридичну фіксацію спроможностей:

на макрорівні – легалізація ризик-орієнтованого підходу та адаптивних методів управління ризиками;

на рівні вертикалі – подолання розриву між центром та регіонами через нормативну децентралізацію;

на рівні інновацій – правове стимулювання науки та залучення етичних дослідників;

на рівні громадянина – перехід до активної суб'єктності та відповідальності виробників ПЗ.

Запропоновані зміни дозволять перетворити виявлені під час аналізу «вразливості» на нормативно закріплені «спроможності», що забезпечить

довгострокову витривалість національної кіберсистеми в умовах постійної трансформації загроз.

Висновки до розділу 3

У ході проведення аналітичної розвідки стратегічних напрямів національної кіберстійкості було встановлено, що сучасна методологія дослідження має базуватися на міждисциплінарному підході, який інтегрує соціологічні теорії «суспільства ризику» з інженерними принципами надійності систем. Доведено, що процес розвідки не може обмежуватися лише технічним аудитом вразливостей, а повинен включати глибокий аналіз соціально-економічних та інституційних чинників, що впливають на здатність держави адаптуватися до непередбачуваних шоків. Сформована автором методологічна база дозволяє розглядати кіберстійкість як динамічний процес, де ключову роль відіграє зважене прийняття управлінських рішень на основі прогнозних моделей. Встановлено, що ефективність стратегічного планування в Україні безпосередньо залежить від впровадження інструментів «foresight»-аналізу, які дають змогу не лише реагувати на поточні інциденти, а й превентивно готувати критичну інфраструктуру до майбутніх викликів. Аналіз підтвердив, що методологічне розмежування між реактивною безпекою та проактивною стійкістю є фундаментом для побудови нової системи національної стійкості, де безпека розглядається як інвестиція в сталий розвиток.

Глибокий аналіз сучасного стану та викликів кіберстійкості України в умовах глобальних та локальних загроз виявив критичну вразливість існуючих ієрархічних структур управління. Дослідження засвідчило, що традиційні моделі захисту, орієнтовані на централізацію ресурсів, виявляються малоефективними проти децентралізованих та гібридних атак. Особливу увагу приділено феномену «цифрового розриву» між центральними органами влади

та регіональними суб'єктами, що створює зони слабкості в загальнонаціональному периметрі захисту. Виявлено, що низький рівень інституційної підтримки наукових досліджень та недостатнє залучення експертного середовища до оперативної практики стримують трансформацію поточної витривалості країни у сталу стратегічну перевагу. На основі проведеного аудиту встановлено, що ключовим викликом є не лише брак технологічного оновлення, а й відсутність сталої культури кібергігієни на рівні пересічного громадянина, який у сучасних умовах стає активним суб'єктом (або об'єктом) кібервійни. Авторське бачення ситуації підкреслює, що подолання цих розривів потребує переходу до мережевої моделі координації, де кожен елемент системи володіє автономною здатністю до самовідновлення.

Обґрунтування пріоритетних напрямів удосконалення механізмів управління кіберстійкістю базується на необхідності впровадження ризик-орієнтованого підходу як обов'язкового стандарту для всіх секторів економіки. Пропоновані стратегічні вектори включають нормативну децентралізацію, що передбачає передачу частини повноважень та ресурсів на регіональний рівень для оперативного реагування на місцях. Важливим напрямом визначено стимулювання наукоємних інновацій через створення правових та фінансових преференцій для вітчизняних розробників засобів кіберзахисту. Встановлено, що розвиток національної екосистеми кіберстійкості неможливий без інтеграції освіти, науки та бізнесу у форматі «технологічних кластерів», які б забезпечували безперервне навчання та обмін досвідом. Особливий акцент зроблено на переході до «активної суб'єктності» виробників програмного забезпечення, що передбачає їхню пряму юридичну та репутаційну відповідальність за вбудовану безпеку продуктів. Такі заходи дозволять перетворити управління стійкістю з суто адміністративної функції на дієвий механізм забезпечення технологічного суверенітету держави.

Завершальним етапом дослідження став розвиток концепції «стійкість через право», що передбачає глибоку трансформацію нормативно-правового поля України. Пропонується відмовитися від декларативних закликів на

користь жорсткої юридичної фіксації необхідних спроможностей суб'єктів кіберпростору. Удосконалення законодавства має відбуватися за чотирма рівнями: легалізація адаптивних методів управління ризиками на макрорівні; нормативне подолання розриву між центром та периферією; правове залучення «етичних дослідників» (white hats) до пошуку вразливостей; та встановлення стандартів персональної відповідальності за цифрову безпеку. Доведено, що правовий механізм має стати не обмежувачем, а стимулом для розвитку інновацій, забезпечуючи баланс між необхідним контролем та свободою наукового пошуку. Сформовані рекомендації щодо гармонізації українського законодавства із європейськими директивами (зокрема NIS2) закладають основу для створення передбачуваного та безпечного цифрового середовища. Реалізація цих підходів дозволить Україні не лише ефективно протидіяти поточним загрозам, а й виступати активним суб'єктом формування глобальних стандартів кіберстійкості.

РОЗДІЛ 4

ПРІОРИТЕТИ СТРАТЕГІЧНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

4.1. Сучасні методологічні засади виявлення та аналізу кіберзлочинності

Розглядаючи питання пов'язані з протидією кіберзлочинності, фахівцями та представниками різних фахових груп використовуються різні та взаємопов'язані терміни у зазначеному контексті діяльності, зокрема: «комп'ютерна злочинність», «інтернет-злочинність», «онлайн-злочинність», «високотехнологічні злочини», «злочини у сфері інформаційних технологій» та «кіберзлочини». У загальному значенні кіберзлочин – це будь-яка незаконна діяльність, пов'язана з одним або кількома компонентами Інтернету, такими як веб-сайти, чати або електронна пошта [264, с. 613], і зазвичай визначається як «кримінальне правопорушення, вчинене з використанням Інтернету або іншої комп'ютерної мережі як компонента злочину» [142, с. 595]. У 2007 році Європейська комісія (ЄК) визначила три різні типи кіберзлочинності: традиційні форми злочинів з використанням кіберпростору, пов'язані, наприклад, з підробкою документів, шахрайством в інтернет-магазинах і на електронних ринках, незаконним контентом, таким як дитяча порнографія, і «злочинами, характерними для електронних мереж» (наприклад, хакерство і атаки типу «відмова в обслуговуванні»). Автори публікації [180, с. 224] розрізняють «справжню» кіберзлочинність (тобто нечесні або зловмисні дії, які не існували б поза межами онлайн-ового середовища) від злочинів, які є просто «електронними». Вони представили «справжні» кіберзлочини як хакерство, розповсюдження вірусів, кібервандалізм, викрадення доменних імен, DoS/DDoS атаки, на відміну від «електронних» злочинів, таких як зловживання кредитними картками, крадіжка інформації, наклеп, чорна

розсилка, кіберпорнографія, сайти ненависті, відмивання коштів, порушення авторських прав, кібертероризм і шифрування. Водночас, фахівцями сьогодні зазначається, що злочинність проникла у Веб 2.0 «разом з усіма іншими видами людської діяльності» [23, с. 39].

Кібератаки все частіше розглядаються як надзвичайна загроза національній безпеці. Такі атаки порушують легітимну роботу мережі і включають навмисне нанесення шкоди мережевим пристроям, перевантаження мережі та відмову в наданні послуг легітимним користувачам. Зловмисник також може використовувати зацикленість, помилки та неправильні конфігурації в програмному забезпеченні, щоб порушити нормальну роботу мережі [23, с. 39].

Мета зловмисника – провести розвідку, обмеживши можливості вільно доступної інформації, отриманої за допомогою різних способів збору розвідувальних даних, перед тим, як здійснити цільову атаку [383]. Тим часом, «секретність» є ключовою частиною будь-якої організованої кібератаки. Дії можуть бути приховані за маскою анонімності, починаючи від використання всюдисущих кібер-кафе і закінчуючи витонченими зусиллями з приховування інтернет-маршрутизації [264, с. 612]. Кіберзлочинці використовують можливості анонімності та маскування під час спілкування в Інтернеті для здійснення шкідливих дій, таких як фішинг, спам, шантаж, крадіжка особистих даних і торгівля наркотиками [263; 287]. Інструменти мережевої безпеки допомагають розпізнавати вразливості мережі та збирати статистику сайтів. Мережеві зловмисники намагаються виявити проломи в безпеці на основі загальних служб, відкритих на хості, збираючи відповідну інформацію для запуску успішної атаки [23, с. 39].

Фахівці класифікують кібератаки на два типи: цілеспрямовані та ситуаційні [315]. При цілеспрямованих атаках застосовуються специфічні інструменти проти конкретних кібер-цілей, що робить цей тип більш небезпечним, ніж інший. Ситуаційні атаки спричиняють розповсюдження хробаків і вірусів, які розгортаються в Інтернеті без розбору [23; 283].

Для протидії здатності організованої кіберзлочинності діяти віддалено через облікові записи, які неможливо відстежити, а також для боротьби з онлайн-злочинними угрупованнями важливо забезпечити правоохоронні органи та суб'єктів національної безпеки інструментами для виявлення, класифікації та захисту від різних типів атак [381]. Збільшення кількості і типів викликів для сучасних фахівців з національної безпеки, розвідки, правоохоронних органів і служб безпеки прискорило використання відкритих джерел в Інтернеті, щоб допомогти скласти більш цілісну картину про людей, організації та діяльність [23; 53].

Методи використання відкритих джерел включають низку спеціальних дисциплін, зокрема статистику, data mining, машинне навчання, нейронні мережі, аналіз соціальних мереж, обробку сигналів, розпізнавання шаблонів (моделей), методи оптимізації та підходи до візуалізації [23; 143; 198].

Готтшальк та ін. [263] представили чотирьохетапну модель «Пошуку знань» для підтримки розслідувань і запобігання білокомірцевим злочинам в бізнесі [262]. Виділено чотири етапи [23, с. 40]:

- від слідчого до технології;
- від слідчого до слідчого;
- від слідчого до інформації;
- від слідчого до заяви.

Завдяки належному застосуванню знань такі процеси можуть допомогти у вирішенні проблем. Ця система, що складається з чотирьох частин, намагається зосереджувати увагу на підтримці пошуку доказів. У правоохоронних органах це важлива функція системи, оскільки докази визначають, чи буде особа звинувачена у вчиненні злочину [263], і наскільки успішним буде судовий розгляд [23, с. 40].

Лінделауф та ін. [321] досліджували структурну побудову таємних злочинних мереж, використовуючи характеристику компромісу між секретністю та інформаційними можливостями для виявлення топологій злочинних мереж. Вони застосували цю методику до доказів у розслідуванні

вибуху на Балі, здійсненого Джемаа Ісламією, а також до мереж розповсюдження героїну в Нью-Йорку. Дановські [216, с. 225–230] розробив методологію, що поєднує аналіз текстів і аналіз соціальних мереж, для пошуку осіб на дискусійних форумах, які мають дуже схожі семантичні мережі на основі змісту повідомлень, що спостерігаються членами списку спостереження, або на основі інших стандартів, таких як радикальний зміст, витягнутий з повідомлень, які вони поширюють в Інтернеті. У сфері протидії кібертероризму та підбурюванню до насильства Дановські використовували пакистанський дискусійний форум з різноманітним контентом для отримання розвідувальної інформації про протиправну поведінку. Ігбал та ін. [286, с. 102–104] представили уніфіковане рішення з data mining для вирішення проблеми аналізу авторства в анонімних текстових повідомленнях, таких як спам і поширення шкідливого програмного забезпечення, а також для моделювання стилю письма підозрюваних в контексті кіберзлочинної поведінки [23, с. 40].

Брантінгем [176] запропонував комплексну обчислювальну систему для мережевого аналізу даних про спільні злочини, яка поєднує формальне моделювання даних з аналізом великих масивів даних про злочинність і тероризм, спрямований на виявлення спільних та актуальних шаблонів. Петерсен та ін. [357, с. 362–364] запропонували алгоритм видалення вузлів в контексті кібертероризму для видалення ключових вузлів терористичної мережі. Фаллах [241, с. 8–10] запропонував стратегію на основі теорії ігор з використанням концепції рівноваги Неша (Nash Equilibrium) для обробки складних сценаріїв DoS-атак. Чонка та ін. [199, с. 1101] запропонували рішення за допомогою Cloud TraceBack (СТВ) для пошуку джерела DoS-атак і запровадили використання мережі з нейтральним зворотним поширенням, яка отримала назву «Cloud Protector», яка була навчена виявляти та фільтрувати трафік таких атак. Інші автори [334] запропонували використовувати систему байєсівського переконання для оцінювання ризиків та кількісного визначення кібер-ризиків та кібер-вразливостей (CVA) [23, с. 40].

Наявні на сьогоднішній день методи можна класифікувати за схемою, як показано на рисунку 4.1. Перший рівень загальних напрямів формується на основі напрямів: аналіз соціальних мереж, Data Mining та статистичного аналізу. Аналіз соціальних мереж передбачає використання таких методів: видалення вузла, вилучення мережі та семантичний аналіз мережі. У свою чергу Data Mining формується чотирма напрямками: текс-майнінг, оптимізаційний метод, веб-майнінг та машинне навчання. Ключовим же напрямом статистичного аналізу залишається регресійний метод [23, с. 40].

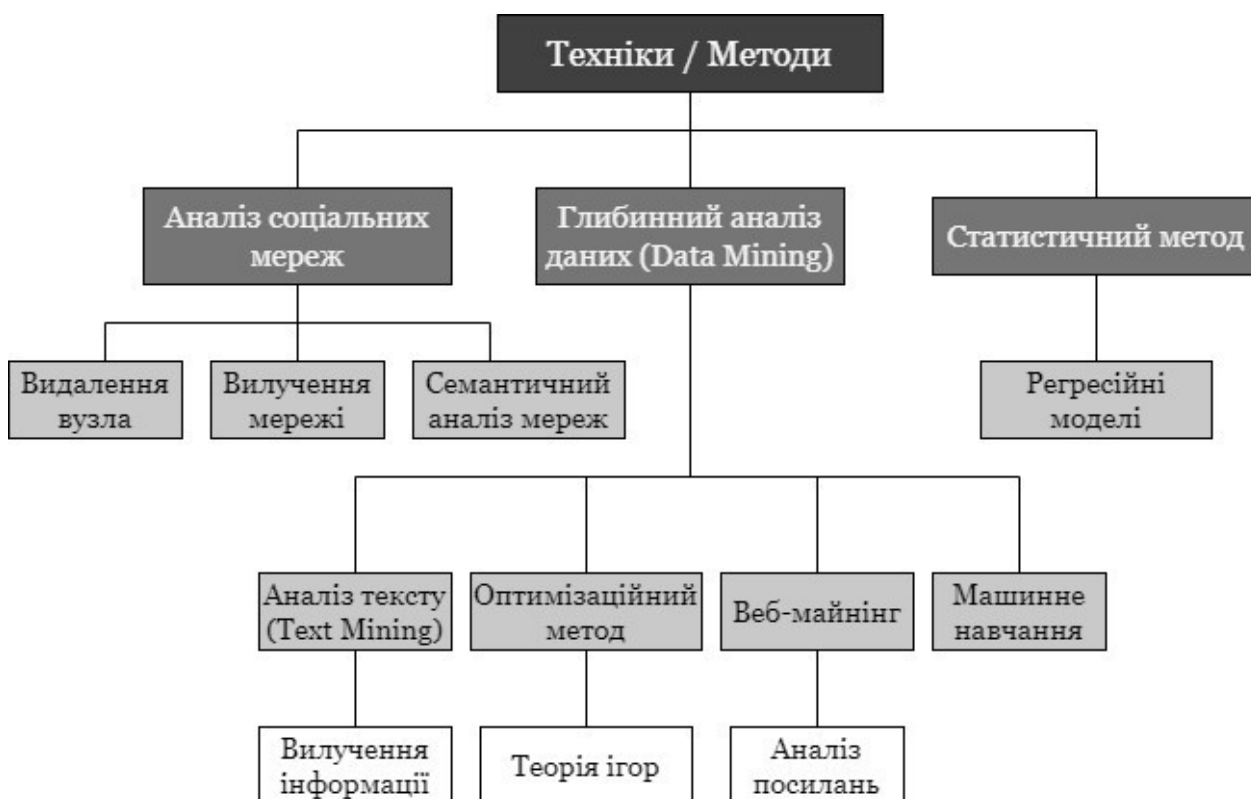


Рис. 4.1 Класифікація методів та моделей розслідування кіберзлочинів [23, с. 39]

Таким чином, сфера комп'ютерної кримінології включає в себе широкий спектр обчислювальних методів для ідентифікації:

- шаблонів і появи трендів;
- причини та умови злочинності;
- соціальних та просторових мереж тероризму, організованої злочинності та банд;

- мереж співучасників злочинів [23, с. 40].

Хоча багато підходів здаються корисними для розслідування кіберзлочинів, існуюча література свідчить про те, що аналіз соціальних мереж, інтелектуальний аналіз даних, аналіз текстів, кореляційні дослідження та методи оптимізації, особливо з акцентом на аналізі великих обсягів даних з відкритих джерел, є найбільш практичними методами, які допоможуть практикам, службам безпеки та судово-експертним установам [23, с. 41].

Прикладні наукові аспекти аналізу кіберзлочинності в Україні вирішувались також на основі наукової методології, що базується на оцінці ризиків [64, с. 54]. Такий підхід формує можливості комплексного аналізу ризиків з наступним виділенням ключових напрямів:

- ідентифікація загроз та оцінювання ризиків поширення кіберзлочинності в Україні;
- оцінювання спроможностей протидії кіберзлочинам та визначення вразливостей;
- аналіз тенденцій у сфері кіберзлочинності в Україні;
- побудова прогнозних моделей управління ризиками у сфері протидії кіберзлочинності [23-24; 26].

Для вирішення зазначених завдань, з метою забезпечення комплексного дослідження, використано сучасні підходи щодо аналізу великих даних, із врахуванням методології ІОСТА Європолу, а також міжнародних стандартів з оцінювання ризиків.

ІОСТА (*оцінка загроз організованої злочинності в Інтернеті*) є флагманським стратегічним продуктом Європолу, якому виповнилося понад 10 років з моменту випуску першого звіту, і який надає правоохоронним органам оцінку загроз, тенденцій та ключових подій у сфері кіберзлочинності.

У 2023-2025 роках найбільш загрозливими проявами кіберзлочинності в Європейському Союзі (ЄС) залишалися атаки з вимогами викупу, сексуальна експлуатація дітей (СЕД) та шахрайство в Інтернеті. Ландшафт кіберзлочинності залишається різноманітним і включає в себе як поодиноких

виконавців, так і злочинні мережі, що пропонують широкий спектр знань і можливостей. Деякі кіберзлочинці, націлені на ЄС, базуються в ЄС, тоді як інші вважають за краще діяти з-за кордону, приховуючи свої незаконні операції та кошти в третіх країнах. На основі аналізу даних сформовано основні рекомендації щодо реагування на явище кіберзлочинності та висвітлено декілька пріоритетних тем для визначення оперативних дій правоохоронних органів ЄС у межах циклу формування політики ЄС.

Загалом дослідження включало певні етапи, про які важливо зазначити, так як саме їх комплексність і забезпечує репрезентативність кримінологічного аналізу кіберзлочинності:

- розробка опитувальника та інструментарію для подальшого аналізу;
- проведення опитування в експертному середовищі;
- очищення даних, введення та перевірку даних на логічні помилки;
- підготовку остаточного (надійного) масиву даних;
- розробку експертної вибірки;
- аналітичне опрацювання даних на основі методології оцінювання ризиків;
- інтерпретація статистичних даних;
- розроблення та формування ключових висновків й рекомендацій;
- підготовка аналітичного звіту.

Опитування проводилося в режимі ON-LINE шляхом заповнення опитувальника з дотриманням режиму конфіденційності та без розкриття індивідуальних даних опитуваних.

Генеральна сукупність даних представлена експертним середовищем Департаменту кіберполіції (далі ДКП) Національної поліції України та сформована шляхом суцільного опитування, яким охоплено керівний склад ДКП, оперативних працівників та інспекторів (аналітиків). Кожен опитувальник заповнювався експертами у відповідності до кількості матеріалів (кримінальні провадження, оперативно-розшукові та аналітичні дані), що були у провадженні експерта за період 2021-2023 року.

За регіональною ознакою генеральна сукупність даних представлена за виключенням тимчасово окупованих територій (АР Крим, Донецька та Луганська області) (рис. 4.2).

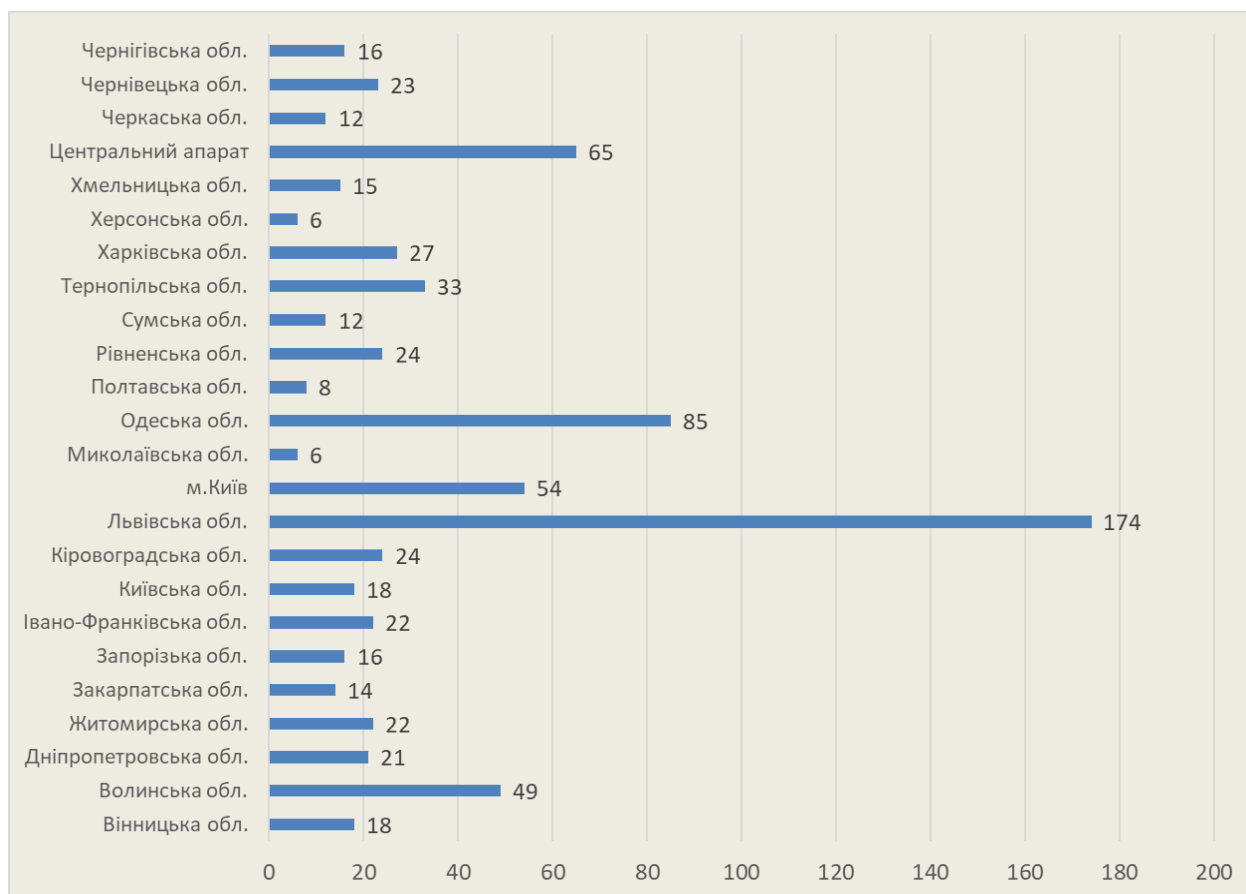


Рис. 4.2 Генеральна сукупність даних за регіональною ознакою

Експертні вибірки сформовані у відповідності з наступними ознаками: стать, посада, досвід роботи та освіта.

За статтю експертні групи представлені наступним розподілом (рис. 4.3): чоловіча стать – 95%, жіноча – 5%.

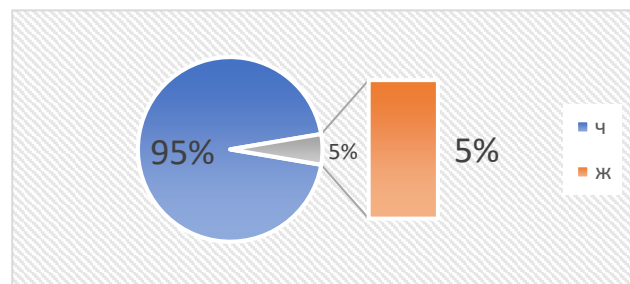
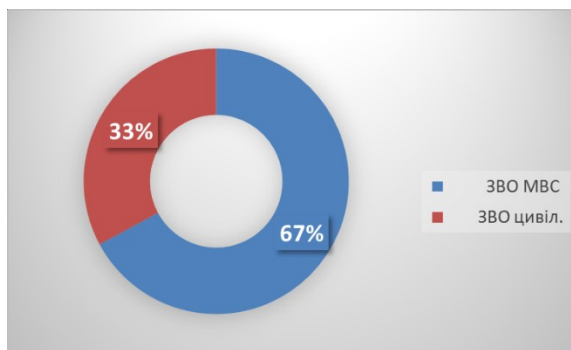


Рис. 4.3 Генеральна сукупність даних за ознакою статі

За категорією посад експертів, які взяли участь в опитуванні, дані наступні (табл. 4.1) [26, с. 20]:

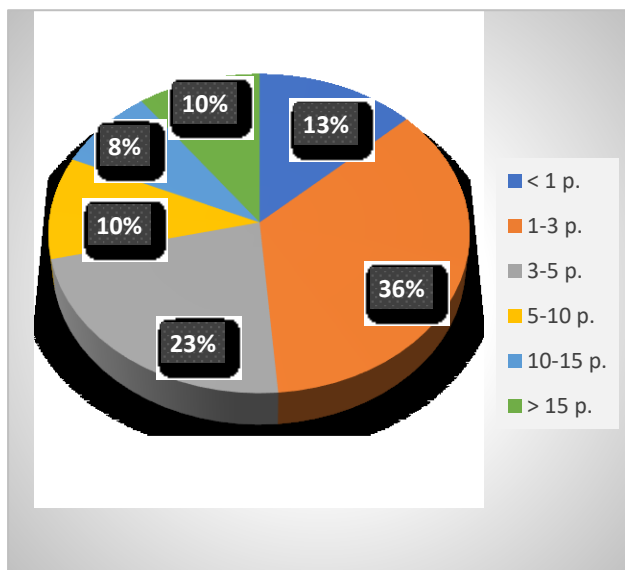
Категорії посад респондентів

КАТЕГОРІЯ ПОСАДИ	Відсоток у загальній кількості
оперативний працівник	17.7
керівник оперативного підрозділу	4.6
аналітик	1.4
керівник аналітичного підрозділу	0.3
інспектор (старший інспектор)	76.0



За освітою експертні групи представлені наступним розподілом (рис. 4.4): заклади вищої освіти системи МВС України – 67%, цивільні заклади вищої освіти – 33%.

Рис. 4.4 Генеральна сукупність даних за ознакою освіти



За досвідом роботи генеральна експертна сукупність представлена відповідними групами (рис. 4.5). Більше третини складають працівники, що працюють в ДКП від 1 до 3 років. Ще чверть – від 3 до 5 років. З досвідом більше 10 років сукупно складають 18% працівників. І лише 13% – працівники з досвідом менше 1 року.

Рис. 4.5 Генеральна сукупність даних за ознакою досвіду роботи

Водночас, розподіл за освітньою спеціальністю (рис. 4.6) з перевагою юридичної освіти (69%) та менше чверті (22%) технічною спеціальністю за освітою.

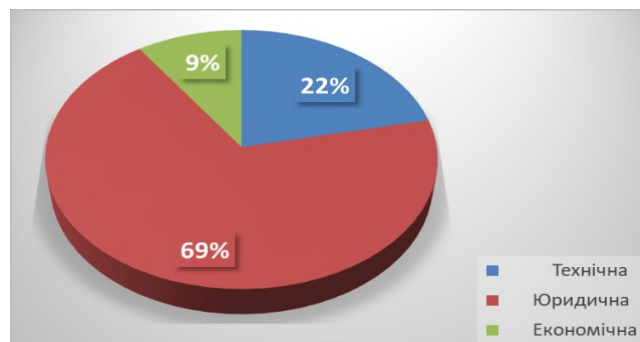


Рис. 4.6 Генеральна сукупність даних за ознакою освітньої спеціальності

Важливо зазначити, що ІОСТА та СОСТА використовують широкий спектр інформаційних джерел, серед яких важливе місце займає саме експертна думка, а не лише матеріали кримінальних проваджень, які потенційно обмежують перспективи аналітичних висновків [64]. А тому сформований масив даних забезпечено використанням наступних джерел (рис. 4.7): кримінальні провадження – 80 %; оперативно-розшукові справи – 5%; довідково-аналітичні матеріали – 15 %.

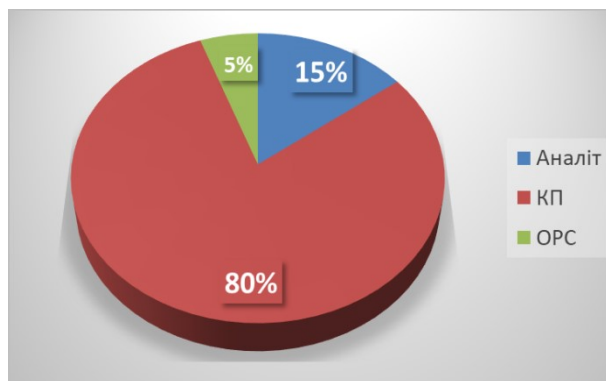


Рис. 4.7 Джерела інформації за генеральною сукупністю даних

Використання зазначених експертних вибірок є важливим інструментом оцінювання низки показників, порівняння їх за різними групами та формування більш зваженої думки та висновків.

Для виокремлення найбільш надійної інформації з отриманих даних було здійснено відбір анкет лише тих експертів, які надавали логічно узгоджені відповіді. Статистичні обґрунтування процедури обмеження

вибірки базуються на тому, що через значний обсяг анкети експерти могли припускати помилки у відповідях, оскільки складність питань і короткий час їх осмислення призводить до нестійкості уваги [26; 64; 67]. З цією метою при розробленні опитувальника у різні розділи були внесені відповідні запитання, з попередньо логічно обґрунтованою відповіддю.

Незважаючи на те, що після фільтрування даних залишилося 45,81 % початкової вибірки, якість результатів суттєво зросла. Це можна бачити на прикладі оцінювання індикаторів за експертними вибірками щодо надійності (табл. 4.2) [64].

Таблиця 4.2

Аналіз за фільтром логічної помилки

НАЗВА ІНДИКАТОРА	ОЦІНКА	Вибірка		Статистична значущість	Pearson Chi-Square	Cramer's V
		Ненадійна частина	Надійна частина			
11.7. Активність в Darknet: відмивання коштів	<i>так</i>	60,3%	38,9%	0,000	29.314	.214
	<i>ні</i>	39,7%	61,1%	0,000		
1.1. Технологічна відсталість в Україні щодо сучасних ІКТ (рівень)	<i>нульовий</i>	7.3%	3.4%	0,000	30.118	.217
	<i>низький</i>	10.4%	15.5%	0,000		
	<i>середній</i>	43.1%	58.7%	0,000		
	<i>високий</i>	25.0%	14.0%	0,000		
	<i>дуже високий</i>	14.2%	8.3%	0,000		

Порівнюючи розподіл оцінювання за групами експертів, що були відібрані за фільтром відсутності логічних помилок, у порівнянні з тими, хто цей фільтр не пройшов, можна бачити, різниця в розподілах є значною, зокрема [64]:

щодо активності в Darknet по відмиванню коштів – 60,3 % ненадійних експертів вказали на таку ймовірність, в той час як надійні обрали цей варіант лише у 38,9% випадків. Ця різниця є не тільки статистично значущою

(критерій $\chi^2 = 29.314$, $p < 0.000$), але й величина ефекту є значною (V Крамера $= 0.214$, $p < 0.000$), а результати, за своєю сутністю, були прямо протилежні;

щодо технологічної відсталості України в сучасних ІКТ – 10,4 % ненадійних експертів вказали на низький рівень, в той час як надійні обрали цей варіант у 15,5 % випадків. Варіант «дуже високий» був обраний ними лише у 8,3 % випадків. Ця різниця є не тільки статистично значущою (критерій $\chi^2 = 30.118$, $p < 0.000$), але й величина ефекту є значною (V Крамера $= 0.217$, $p < 0.000$). Аналогічні тенденції спостерігаються і по інших важливих індикаторах.

Таким чином, обмеження вибірки на основі перевірки на логічну помилку є статистично значущим та забезпечує надійність експертної вибірки для подальшого репрезентативного аналізу [26; 64; 67].

Для проведення дослідження обрано ризик-орієнтований підхід у якості базового, який став основою для дослідження за обраним напрямом. Базовими засадами для реалізації визначених завдань оцінювання ризиків є міжнародний стандарт, імplementований у 2018 році до вітчизняного законодавства як національний стандарт – ДСТУ ISO 31000:2018 [48].

Реальності нашого часу диктують необхідність нового рівня мислення в правоохоронній діяльності, що передбачає адекватне сприйняття ризику і його використання, оскільки він є істотним компонентом аналізу майбутнього. Ризик необхідно розглядати як особливий метод пізнання та управління правоохоронною діяльністю, що виступає як набір способів прийняття рішень.

ISO 31000 як національний стандарт прийняли більш ніж 50 національних органів по стандартизації, охопивши понад 70 % населення світу. А також деякі організації ООН і національні урядові організації як основу для розробки власних стандартів і методик.

Науковці в Україні вже не один рік використовують ризик-орієнтований підхід щодо аналізу проблем у сфері безпеки [26; 29; 64-67; 308; 312]. Водночас, у 2021 році у складі експертної групи РНБО України реалізовано проєкт, предметом якого був стратегічний аналіз у сфері кібербезпеки в

Україні [65]. Науковий інтерес завжди викликають зарубіжні новації, упровадження яких в Україні є не лише можливим, а й необхідним процесом. Зокрема, фахівці з кібербезпеки, особливо у сфері правоохоронної діяльності, неодноразово висказувалися щодо методології Європолу ІОСТА, яка є головним стратегічним продуктом Європолу, що забезпечує орієнтовану на правоохоронні органи оцінку нових загроз і ключових подій у сфері кіберзлочинності. В аналітичних висновках, окрім загальних характеристик кіберзлочинців, висвітлюються тенденції щодо її поширення, нові форми та напрями, про що свідчать кібератаки. Також зазначається про зростаюче зближення кіберпростору та організованої злочинності тощо [64-65].

Таким чином, використовуючи методологію Європолу ІОСТА та застосовуючи ризик-орієнтований підхід, реалізовано сучасний підхід стратегічного аналізу у сфері протидії кіберзлочинності. Достатньо показовими є використані у дослідженні матеріали опитування експертів, а також проведена вибірка на основі логічної помилки, що дозволило підійти до наступного усвідомлення сучасних трендів та реального пізнання ключових кіберзагроз, оцінювання ризиків їх поширення, оцінювання спроможностей та вразливостей щодо протидії кіберзагрозам [26].

4.2. Виклики та пріоритетні напрями стратегічного забезпечення протидії кіберзлочинності в Україні

Для подальшого аналізу кіберзлочинності було виділено 4 групи кримінальних правопорушень (далі к/п), які поєднуються та сукупно виділяються певною специфічною сферою діяльності у суспільстві, але які також характеризуються використанням злочинцями сучасних інформаційних та телекомунікаційних технологій:

1) у сфері використання комп'ютерів, систем та комп'ютерних мереж;

- 2) у сфері протидії обігу протиправного контенту і телекомунікацій;
- 3) у сфері протидії злочинам у банківській сфері;
- 4) у сфері протидії різновидам шахрайства з платежами.

Перша група кримінальних правопорушень відноситься до кіберзалежних злочинів, так як такі діяння можуть бути вчинені лише з використанням комп'ютерів, комп'ютерних мереж або інших форм інформаційно-комунікаційних технологій (ІКТ).

Водночас, переважна більшість зазначених к/п є предметом виявлення та розслідування різних підрозділів та правоохоронних органів, що унеможливорює достатньо глибоке статистичне відображення їх у ЄРДР за ознакою «кіберзлочин».

Подальший аналіз поширеності зазначених кримінальних правопорушень здійснено на основі виділення зазначених окремих груп злочинної діяльності.

Кримінальні правопорушення у сфері використання комп'ютерів, систем та комп'ютерних мереж є найбільш поширеними і безпосереднім віддзеркаленням змісту та рівня кіберзлочинності. До цього переліку відносяться кримінальні правопорушення передбачені такими статтями ККУ [22, с. 158]:

Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Стаття 361¹. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Стаття 361². Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

Стаття 363¹. Перешкодження роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [22, с. 158].

Найбільш поширеними у зазначеному переліку є к/п, передбачені статтею 361 ККУ (53,02 %) (табл. 4.3). Така тенденція корелюється і з даними ЄРДР (червона зона). Водночас, на відміну від опитування (6,67 % – жовта зона), за даними ЄРДР значною поширеністю додатково характеризується і злочин передбачений ст. 362 ККУ (червона зона 35-48 % за відповідними роками), що пояснюється врахуванням діяльності і інших правоохоронних органів.

Таблиця 4.3

Співвідношення кількості злочинів за даними опитування та ЄРДР

Стаття ККУ	361	361-1	361-2	362	363	363-1
За даними опитування, %	53,02	6,35	4,76	6,67	2,86	1,11
ЄРДР 2021, %	50,73	1,06	4,26	43,50	0,36	0,09
ЄРДР 2022, %	41,08	8,20	1,76	48,73	0,09	0,15
ЄРДР 2023, %	59,18	0,91	4,30	35,28	0,29	0,05

Таким чином, за даними експертного опитування найбільшими збитками матеріального та нематеріального характеру характеризується також к/п передбачене ст.361 ККУ (табл. 4.4). І хоча питома вага збитків до 5 млн. грн. у кожному конкретному випадку є переважаючою, лише ці к/п вказують і

на великі збитки, що значно перевищують зазначену суму, а в окремих випадках більше 1 млрд. грн [22, с. 158].

Таблиця 4.4

Співвідношення злочинів за наслідками їх вчинення та сумою збитків

	Менше 100 тис.	100 тис - 500 тис	500 тис - 1 млн	1 млн - 5 млн	5 млн - 50 млн	50 млн - 500 млн	500 млн - 1 млрд	більше 1 млрд	Нематеріал ьні збитки
361									
361-1									
361-2									
362									
363									

Водночас, інші к/п цієї групи характеризуються як у сукупному врахуванні, так і у кожному конкретному випадку, меншими сумами матеріальних збитків, переважно до 5 млн. грн. Хоча за ст. 362 ККУ наслідки вчинення к/п в окремих випадках характеризуються збитками і до 1 млрд. грн [22, с. 159].

Крім того, за даними експертного опитування, при розгляді наслідків вчинення к/п цієї групи, із врахуванням суб'єкта посягання (табл. 4.5), найбільшими збитками характеризується також протиправна діяльність, передбачена статтями ККУ 361 та 362, а серед суб'єктів переважно їх зазнають фізичні особи та держава [22, с. 159].

Таблиця 4.5

Співвідношення злочинів за наслідками їх вчинення та за суб'єктом

посягання

	361	361-1	361-2	362	363
Державі					
Державному органу					
Державному підприємству (установі)					
Комерційному підприємству					
Фізичній особі					

При вчиненні цієї групи злочинів, злочинці використовують різноманітні специфічні інструменти (послуги).

Серед операційних систем найчастіше використовується злочинцями Kali Linux – 33%, що значно частіше у порівнянні з BlackArch Linux (11%), BackBox Linux (10%) та Parrot Security OS (9%) (табл. 4.6, рис. 4.8) [22, с. 159].

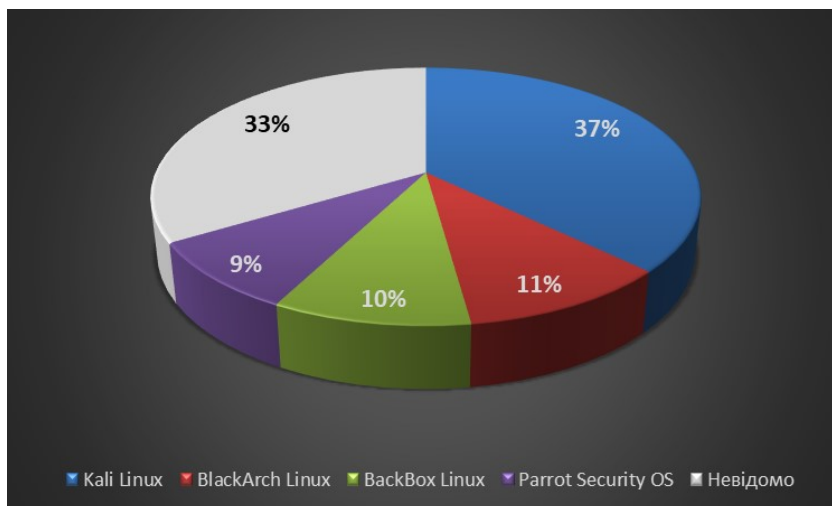


Рис. 4.8 Питома вага видів операційних систем, що використовуються злочинцями

Таблиця 4.6

Види операційних систем, що використовуються злочинцями

Операційні системи	361 ККУ	361-1 ККУ	362 ККУ
Kali Linux			
BlackArch Linux			
BackBox Linux			
Parrot Security OS			
Невідомо			

Водночас, з метою несанкціонованого втручання в роботу інформаційно-комунікаційних систем, електронних комунікаційних мереж, значно зростає питома вага використання злочинцями операційної системи Kali Linux – 41% (рис. 4.9) [22, с. 159].

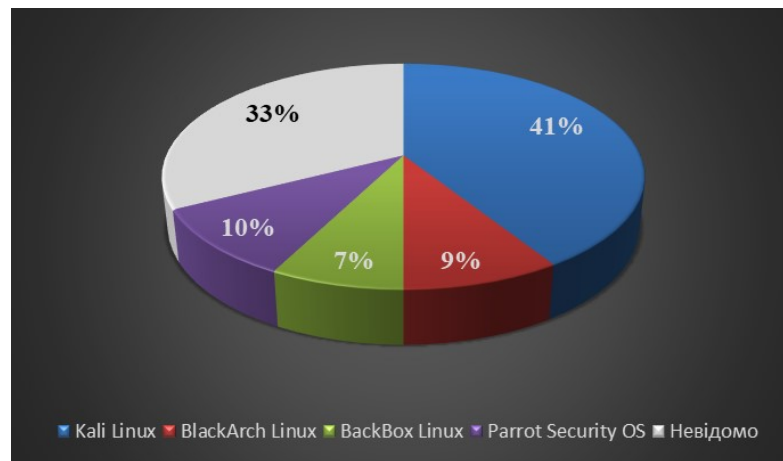


Рисунок 4.9 Питома вага видів операційних систем, що використовуються при вчинення к/п, передбаченого ст. 361 ККУ

Серед спеціального програмного забезпечення експерти виділяють DoS-атаки (22%), спамінг (21%), брутфорс (24%) та пентестинг (9%) (табл. 4.7, рис. 4.10) [22, с. 160].



Рисунок 4.10 Питома вага видів операційних систем, що використовуються злочинцями

Таблиця 4.7

Використання злочинцями спеціального програмного забезпечення

Використання спеціального програмного забезпечення	361 ККУ	361-1 ККУ	362 ККУ
DoS-атака			
Спамінг			
Брутфорс			
Пентестинг			
Невідомо			

Водночас, з метою несанкціонованого втручання в роботу інформаційно-комунікаційних систем, електронних комунікаційних мереж,

значно зростає питома вага використання злочинцями спеціального програмного забезпечення Брутфорс та DoS-атак, а спамінг є більш характерним для розповсюдження шкідливих програмних чи технічних засобів та несанкціонованих дій з інформацією.

Такого роду спеціальне програмне забезпечення злочинці можуть рівнозначно отримувати, використовуючи ресурси соціальних мереж, форумів та Darknety (табл. 4.8) [22, с. 161].

Таблиця 4.8

Джерела отримання злочинцями спеціального програмного забезпечення

Джерело отримання програмного забезпечення злочинцями	361 ККУ	361-1 ККУ	362 ККУ
Даркнет			
Форуми			
Соціальні мережі			
Невідомо			

Досліджуючи зазначену групу злочинів, важливо також з'ясувати основні способи їх вчинення.

Експертною групою кіберполіції було виділено чотири ключові групи, що об'єднували основні способи вчинення таких злочинів (табл. 4.9) [22, с. 161].

За способом отримання доступу до телекомунікаційних каналів та комп'ютерних мереж найчастіше злочинці використовують перехоплення інформації при її передачі, а також відкритий доступ до ПК. Значно рідше використовується проникнення до приміщень. При цьому, перехоплення трафіку переважно здійснюється за допомогою шкідливого ПЗ, яке отримує авторизаційні дані з браузера (Stiller). Хоча значною питоною вагою серед способів перехоплення трафіку залишається фактор «людина посередині», а також «паралельна сесія» та «отруйний DNS» [22, с. 161].

За способом віддаленого отримання доступу, рівнозначним є використання злочинцями реальних паролів користувачів, як отриманих в мережі, так і шляхом перебору за допомогою спеціальних програм.

Таблиця 4.9

Способи вчинення злочинів

	361 ККУ	361-1 ККУ	362 ККУ
За способом отримання доступу:			
Шляхом перехоплення інформ при її передачі телекомунікацій каналами і комп'ютерними мережами			
Шляхом проникнення до приміщення, в якому знаходиться ПК			
Шляхом відкритого доступу до ПК			
Невідомо			
За способом віддаленого отримання доступу:			
Використання зловмисниками реальних паролів користувачів, отриман в мережі			
Отримання паролів, ключів шляхом перебору за допомогою спеціальних програм			
Невідомо			
За способом отримання потерпілими посилання на шкідливе програмне забезпечення			
Месенджери			
Соціальні мережі			
Електронна пошта			
Sms-повідомлення			
Сайт			
Невідомо			
За способом перехоплення трафіку			
Людина посередині (man in the middle)			
Отруйний DNS (poison DNS)			
Паралельна сесія			
За допомогою шкідливого ПЗ, яке отримує авторизаційні дані з браузера (Stiller)			
Невідомо			

Шкідливе програмне забезпечення злочинці розповсюджують, використовуючи широкий перелік засобів: месенджери, соціальні мережі, електронну пошту, sms-повідомлення та різноманітні сайти [22, с. 161].

Водночас месенджери та соціальні мережі є найбільш поширеним засобом отримання потерпілими посилання на шкідливе програмне забезпечення.

Мотивація злочинців, перш за все, пов'язана з їх матеріальним збагаченням, на що вказує більше 60% експертів за матеріалами проваджень (табл. 4.10). Поряд з цим, важливим є зазначити, що в межах 10% оцінюється можливість вчинення цієї групи злочинів як складової гібридної війни проти України. Водночас, трохи більший відсоток злочинів (до 13%) характеризується співпрацею з російським агресором [22, с. 161].

Мотивація злочинців

Мотивація злочинців	361 ККУ %	361-1 ККУ %	362 ККУ %
матеріальне збагачення	61	67	66
складова гібридної війни	10	11	9
співпраця з агресором	13	5	9
хуліганські дії	10	17	9
соціальний протест	2	0	5
невідомо	4	0	2

Експертним середовищем акцентовано увагу на вчиненні певної частини злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж організованими злочинними угрупованнями (далі – ОЗУ) (табл. 4.11) [22, с. 162].

Таблиця 4.11

Питома вага вчинених злочинів ОЗУ

Стаття ККУ	361 ККУ	361-1 ККУ	362 ККУ
ОЗУ, %	51,20	35,00	73,81
ОЗУ укр, %	14,70	17,50	35,70

За наявними ознаками кваліфікації злочинів, передбачених ст. 361 ККУ більше 50 відсотків вчиняється у складі ОЗУ і майже три чверті – за ст. 362 ККУ. Водночас, експерти зазначають щодо загрози діяльності ОЗУ безпосередньо на території України: за ст. 361 ККУ – 14,7 %; за ст. 361¹ ККУ – 17,5 %; за ст. 362 ККУ – 35,7 % [22, с. 162-163].

Зазначений сегмент к/п характеризується значним переліком протиправної діяльності і також у переважній більшості є безпосереднім об'єктом протидії підрозділами кіберполіції НПУ. Зазначені к/п передбачені відповідними статтями, зокрема: 120 ККУ, 149 ККУ, 156 ККУ, 156-1 ККУ, 176 ККУ, 203-1 ККУ, 229 ККУ, ч.3, 4, 5 301 ККУ, 301-1 ККУ, 301-2 ККУ, 307 ККУ, 321 ККУ, 321-1 ККУ.

Водночас, за даними експертного опитування найбільш поширеними у зазначеному переліку є к/п, передбачені ККУ (табл. 4.12):

Стаття 301¹. Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження – 33,81 %;

Стаття 229. Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару – 17,86 %;

Стаття 301. Ввезення, виготовлення, збут і розповсюдження порнографічних предметів – 16,19 %;

Стаття 176. Порушення авторського права і суміжних прав – 12,14 %;

Стаття 307. Незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів – 7,38 %.

Таблиця 4.12

Співвідношення кількості злочинів за даними опитування та ЄРДР

	120 ККУ	149 ККУ	156 ККУ	156-1 ККУ	176 ККУ	203-1 ККУ	229 ККУ	ч.3, 4, 5 301 ККУ	301-1 ККУ	301-2 ККУ	307* ККУ	321 ККУ	321-1 ККУ
За даними експертів %	1,90	0,48	3,10	0,71	12,14	0,71	17,86	16,19	33,81	2,38	7,38	1,43	1,67
2021 % за ЄРДР	4,05	8,31	9,31	0,00	2,94	0,07	3,40	53,46	0,00	0,00		17,72	0,75
2022 % за ЄРДР	2,43	5,12	7,01	0,35	1,19	0,00	1,04	30,23	42,16	0,00		9,82	0,65
2023 % за ЄРДР	1,32	4,12	7,29	0,36	0,92	0,00	3,34	25,31	45,43	0,00		11,18	0,73

**Прим.: Для уникнення спотворення статистичного відображення відповідного рівня поширення зазначеної групи к/п, з таблиці було видалено відносні показники поширення к/п за ст.307 ККУ, так як пов'язані з незаконним обігом наркотичних засобів і є об'єктом активного контролю широкого спектру п/о підрозділів та характеризуються надзвичайно великою кількістю.*

Результати експертного опитування переважно корелюються з даними щодо к/п зареєстрованих в ЄРДР. Водночас, нехарактерними для кіберполіції є к/п передбачені ст.ст. ККУ 321, 156 та 149, але які мають певне поширення за дами реєстрації в ЄРДР.

Певним чином це пояснюється оцінюванням експертами кіберполіції наслідків вчинення к/п цієї групи, у якому найзначніші матеріальні збитки

мають місце при вчинення к/п за ст.ст. 301¹; 301 ч. 3, 4, 5; 229 та 176 ККУ (табл. 4.13). І хоча питома вага збитків до 5 млн. грн. у кожному конкретному випадку є переважаючою, в окремих випадках мають місце великі збитки, що значно перевищують суму 500 млн. грн., а то й 1 млрд. грн.

Водночас, інші к/п цієї групи характеризуються як у сукупному врахуванні, так і у кожному конкретному випадку, меншими сумами матеріальних збитків, переважно до 50 млн. грн. (ст.ст. 156, 301² та 307 ККУ).

Таблиця 4.13

Співвідношення злочинів за наслідками їх вчинення та сумою збитків

	120 ККУ	149 ККУ	156 ККУ	156-1 ККУ	176 ККУ	203-1 ККУ	229 ККУ	ч.3, 4, 5 301 ККУ	301-1 ККУ	301-2 ККУ	307 ККУ	321 ККУ	321-1 ККУ
Менше 100 тис													
100 тис - 500 тис													
500 тис - 1 млн													
1 млн - 5 млн													
5 млн - 50 млн													
50 млн - 500 млн													
500 млн - 1 млрд													
більше 1 млрд													

Крім того, за даними експертного опитування, при розгляді наслідків вчинення к/п цієї групи, серед суб'єктів переважно найбільших збитків зазнають фізичні особи та держава. Водночас, значні збитки несуть державні та комерційні підприємства від протиправної діяльності, передбаченої ст.ст. 176, 229, 301 та 301¹ ККУ (табл. 4.14).

Таблиця 4.14

Співвідношення злочинів за наслідками їх вчинення та за суб'єктом посягання

	120 ККУ	149 ККУ	156 ККУ	156-1 ККУ	176 ККУ	203-1 ККУ	229 ККУ	ч.3, 4, 5 301 ККУ	301-1 ККУ	301-2 ККУ	307 ККУ	321 ККУ	321-1 ККУ
Державі													
Державному органу													
Державному підприємству (установі)													
Комерційному підприємству													
Фізичній особі													

Мотивація злочинців, перш за все, пов'язана з їх матеріальним збагаченням, що характеризується вибіркою 60-66 % в межах генеральної сукупності (табл. 4.15). Водночас, вибіркою в межах 8-10 % ця група злочинів характеризується як складова гібридної війни проти України. Має місце і

співпраця з російським агресором у вчиненні цієї групи злочинів, яка оцінюється на рівні дещо вищому: 301¹ ККУ – 17 %; 176 ККУ – 14 %; 229 ККУ – 11 %.

Таблиця 4.15

Мотивація злочинців

Мотивація злочинців	176 ККУ %	229 ККУ %	301 ККУ %	301-1 ККУ %	307 ККУ %
матеріальне збагачення	61	66	61	60	65
складова гібридної війни	9	8	8	10	10
співпраця з агресором	14	11	8	17	3
хуліганські дії	12	7	17	10	13
соціальний протест	2	5	3	0	3
невідомо	2	3	3	3	6



Ключовою загрозою цієї групи є вчинення злочину, передбаченого ч. 3, 4, 5 ст. 301 ККУ. За оцінкою експертів розповсюдження дитячої порнографії здійснюється з території рф у 36,5% випадків, а України – 24,3% (рис. 4.11).

Рис. 4.11 Країна походження головної загрози (ч. 3, 4, 5 ст. 301 ККУ)



Водночас, наявність ознаки діяльності ОЗУ щодо поширення дитячої порнографії вбачається в 70% випадків (рис. 4.12).

Рис. 4.12 Наявні ознаки кваліфікації ОГ або ЗО (ч. 3, 4, 5 ст. 301 ККУ)

До переліку кримінальних правопорушень в банківській сфері відносяться такі:

Стаття 185. Крадіжка

Стаття 200. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення

Стаття 209. Легалізація (відмивання) майна, одержаного злочинним шляхом

Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Характеризувати зазначені кримінальні правопорушення, порівнюючи думку експертів з даними реєстрації в ЄРДР не є доречним, так як кожен з цих злочинів характеризується специфічною об'єктивною стороною, що не коректно відображатиме будь-яке співставлення. Але усі к/п мають достатньо високий рівень поширення із використанням ІТ технологій і потребують більш глибокого аналізу.

Найбільш поширеними, за даними опитування, у зазначеному переліку є к/п, передбачені статтею 200 ККУ (66 %) (рис. 4.14). Водночас крадіжка (185 ККУ) та відмивання коштів (209 ККУ) на думку експертів кіберполіції також мають значне поширення [65, с. 157].

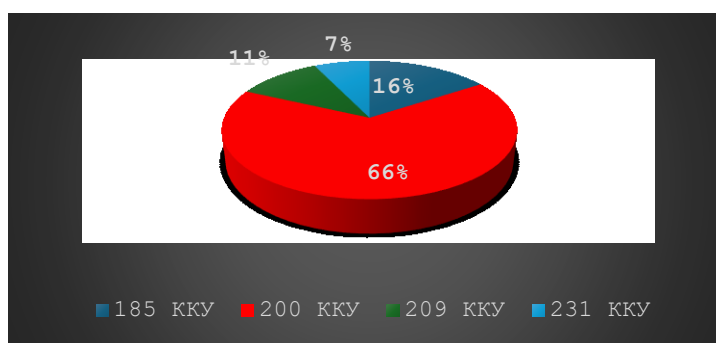


Рис. 4.13 Питома вага кіберзлочинів, що вчиняються в банківській сфері

Загальне співвідношення к/п цієї групи за наслідками їх вчинення переважно зберігається. Найзначнішими наслідками характеризується к/п за ст. 200 ККУ. Водночас, серед інших виділяються к/п передбачені ст. 209 ККУ, які характеризуються в усьому спектрі сум матеріальними збитками, у тому

числі і щодо сум в окремих випадках більше 500 млн. грн. та 1 млрд. грн. (табл. 4.16) [65, с. 157].

Таблиця 4.16

Співвідношення злочинів за наслідками їх вчинення та сумою збитків

	185 ККУ	200 ККУ	209 ККУ	231 ККУ
Менше 100 тис				
100 тис - 500 тис				
500 тис - 1 млн				
1 млн - 5 млн				
5 млн - 50 млн				
50 млн - 500 млн				
500 млн - 1 млрд				
більше 1 млрд				

Крім того, за даними експертного опитування, при розгляді наслідків вчинення к/п цієї групи, серед суб'єктів переважно найбільших збитків зазнають фізичні особи та держава. Водночас, значні збитки несуть державні та комерційні підприємства від протиправної діяльності, передбаченої ст. 200 ККУ (табл. 4.17) [65, с. 157].

Таблиця 4.17

Співвідношення злочинів за наслідками їх вчинення та за суб'єктом посягання

	185 ККУ	200 ККУ	209 ККУ	231 ККУ
Державі				
Державному органу				
Державному підприємству (установі)				
Комерційному підприємству				
Фізичній особі				

Мотивація злочинців, перш за все, пов'язана з їх матеріальним збагаченням, що характеризується вибіркою 55-59 % в межах генеральної сукупності (табл. 4.18). Водночас, вибіркою в межах 10-17 % ця група злочинів характеризується як складова гібридної війни проти України. Має місце і співпраця з російським агресором у вчиненні цієї групи злочинів, яка

оцінюється на рівні: 185 ККУ – 7 %; 200 ККУ – 16 %; 209 ККУ – 14 % [65, с. 158].

Таблиця 4.18

Мотивація злочинців

Мотивація злочинців	185 ККУ %	200 ККУ %	209 ККУ %
матеріальне збагачення	55	55	59
складова гібридної війни	17	11	10
співпраця з агресором	7	16	14
хуліганські дії	8	13	14
соціальний протест	3	2	3
невідомо	10	3	0

Експертним середовищем акцентовано увагу на вчиненні певної частини злочинів у банківській сфері організованими злочинними угрупованнями (табл. 4.19) [65, с. 158].

Таблиця 4.19

Питома вага вчинених злочинів ОЗУ

Стаття ККУ	185 ККУ	200 ККУ	209 ККУ
ОЗУ, %	14,70	35,79	29,79
ОЗУ укр, %	5,88	7,72	17,02

За наявними ознаками кваліфікації злочинів, передбачених ст. 200 ККУ більше 35 відсотків вчиняється у складі ОЗУ і майже третина – за ст. 209 ККУ. Водночас, експерти зазначають щодо загрози діяльності ОЗУ безпосередньо на території України: за ст. 185 ККУ – 5,88 %; за ст. 200 ККУ – 7,72 %; за ст. 209 ККУ – 17,02 % [65, с. 159].

Шахрайство з платежами (On-line шахрайства) є сучасним різновидом шахрайства (ст. 190 ККУ) і у переважній більшості є безпосереднім об'єктом протидії підрозділами кіберполіції НПУ (ч. 4 ст. 190 ККУ – *шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки*) [33].

Виділення цього виду кримінального правопорушення обґрунтовується значним зростанням використання телекомунікаційних технологій при їх вчиненні, що і визначає специфіку об'єктивної сторони цього злочину.

On-line шахрайства є найбільш поширеним видом кіберзлочину (рис. 4.14). Питома вага його у загальній сукупності кримінальних правопорушень, при вчиненні яких використовуються сучасні інформаційні та телекомунікаційні технології, складає 36 %. Несанкціоноване втручання в роботу інформаційно-комунікаційних систем, електронних комунікаційних мереж складає 26 %, а незаконні дії з платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення – 22 %, у загальній сукупності злочинів, протидія яким є пріоритетом кіберполіції [33, с. 144].

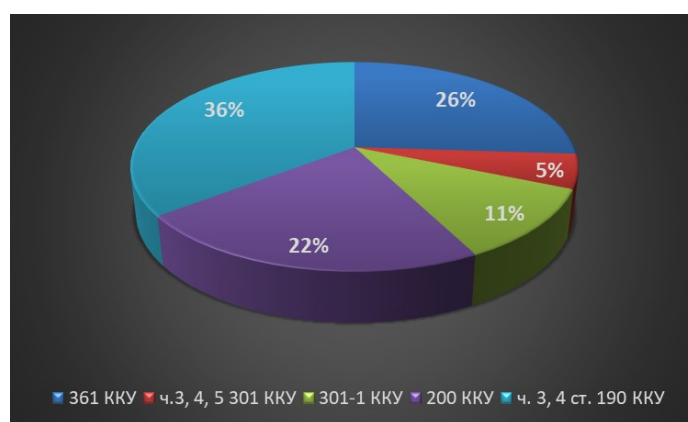


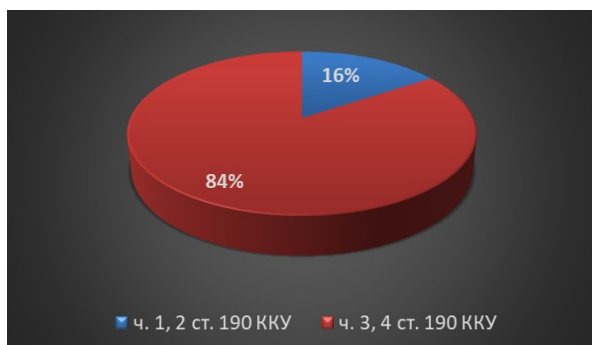
Рис. 4.14 Питома вага кіберзлочинів

Враховуючи латентність шахрайства, а також те що цей вид злочину загалом є об'єктом протидії не лише кіберполіції (за об'єктивною стороною складу злочину), важливим є зазначити на характері джерела за експертним опитуванням (рис. 4.15). Лише у 59,8% це матеріали кримінальних проваджень [33, с. 145].



Близько 30% експертів були зорієнтовані на основі аналітичних матеріалів, що суттєво доповнює загальну характеристику поширення on-line шахрайства в Україні [33, с. 145].

Рис. 4.15 Характер джерела інформації про злочини



Таким чином, 84% шахрайств вчиняються саме у формі діяльності передбаченої частинами 3 та 4 ст.190 ККУ (рис. 4.16), що ще раз підкреслює надзвичайну поширеність on-line шахрайства в Україні [33, с. 145].

Рис. 4.16 Питома вага злочинів, передбачених ч. 3, 4 ст.190 ККУ

Водночас, за даними експертного опитування, діяння передбачені частинами 3 та 4 ст.190 ККУ, також характеризуються найбільшими збитками (табл. 4.20). І хоча питома вага збитків до 5 млн. грн. у кожному конкретному випадку є переважаючою, все ж мають місце значні збитки, що значно перевищують зазначену суму, а в окремих випадках більше 1 млрд. грн [33, с. 146].

Таблиця 4.20

Співвідношення злочинів за наслідками їх вчинення та сумою збитків

	ч. 1, 2 ст. 190 ККУ	ч. 3, 4 ст. 190 ККУ
Менше 100 тис		
100 тис - 500 тис		
500 тис - 1 млн		
1 млн - 5 млн		
5 млн - 50 млн		
50 млн - 500 млн		
500 млн - 1 млрд		
більше 1 млрд		

Крім того, при розгляді наслідків вчинення к/п цієї групи, серед суб'єктів переважно найбільших збитків зазнають фізичні особи та держава. Водночас, значні збитки несуть також і державні та комерційні підприємства від протиправної діяльності, передбаченої саме частинами 3 та 4 ст. 190 ККУ (табл. 4.21) [33, с. 146].

Співвідношення злочинів за наслідками їх вчинення та за суб'єктом
посягання

	ч. 1, 2 ст. 190 ККУ	ч. 3, 4 ст. 190 ККУ
Державі		
Державному органу		
Державному підприємству (установі)		
Комерційному підприємству		
Фізичній особі		

Мотивація злочинців, перш за все, пов'язана з їх матеріальним збагаченням, що характеризується вибіркою 62 % в межах генеральної сукупності (рис. 4.17). Водночас, вибіркою в межах 10 % ця група злочинів



характеризується як складова гібридної війни проти України. Має місце і співпраця з російським агресором у вчиненні цієї групи злочинів, яка оцінюється на рівні 12 % [33, с. 147].

Рис. 4.17 Мотивація злочинців, що вчиняють злочини передбачені ч.3, 4 ст.190 ККУ

За методологією Європол ІОСТА, із врахуванням значної різноманітності способів та засобів, що використовуються при здійсненні платежів, розрізняється два види шахрайства з платежами: з використанням картки та без такої [33, с. 147].

Експертною групою було ідентифіковано 17 загроз поширення шахрайства з платежами без використання банківської картки (табл. 4.22). За сучасного стану найбільшим поширенням характеризуються загрози шахрайства з платежами, пов'язані з: роздрібною торгівлею фізичними (51,4 %) та віртуальними товарами (40,6 %); конвертацією валют (криптовалют та електронних грошей) (46,6 %); а також позикою (46,6 %) [33, с. 147].

Загрози шахрайства з платежами, без використання банківської картки

ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ БЕЗ ВИКОРИСТАННЯ БАНКІВСЬКОЇ КАРТКИ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
2.1. пов'язане з транспортом – авіаквитки		23,3	-	-	-	33,91
2.2. пов'язане з транспортом – квитки на поїзд або автобус		30	-	-	-	34,00
2.3. пов'язане з транспортом – оренда автомобілів		22,6	-	-	-	31,83
2.4. пов'язане з позикою (послугою, орендою приміщення тощо)		46,6	-	-	-	37,43
2.5. пов'язане з веб-сайтами азартних ігор		37,1	-	-	-	33,67
2.6. пов'язане з роздрібною торгівлею – фізичні товари		51,4	-	-	-	39,52
2.7. пов'язане з роздр торг– віртуальні товари		40,6	-	-	-	36,66
2.8. пов'язане з конвертацією валют (криптовалют та електр грошей)		46,6	-	-	-	38,95
2.9. з використанням паливних карток		37,4	-	-	-	34,62
2.10. з використанням карток у роздрібній торгівлі продуктам		28,3	-	-	-	32,53
2.11. з використанням клубних карток		16,3	-	-	-	28,33
2.12. з використанням подарункових карток		18,3	-	-	-	28,60
2.13. з використанням ігрових карток		19,7	-	-	-	29,01
2.14. на ринку мобільного зв'язку		30,6	-	-	-	32,23
2.15. в сфері комп'ютерних ігор (внутрішньоігрові перекази)		29,7	-	-	-	30,02
2.16. пов'язане з букмекірськими послугами		28,3	-	-	-	31,29
2.17. пов'язане з «move to»		21,1	-	-	-	29,89

Експертами зазначається про певне загальне зниження масштабів поширення цієї групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення, хоча окремі з них характеризуються меншим трендом до зниження масштабів, зокрема, пов'язані з: позикою, роздрібною торгівлею фізичними товарами, конвертацією валют (криптовалют та електронних грошей) та використанням паливних карток [33, с. 148].

Зазначені види загроз шахрайства з платежами, без використання банківської картки, характеризуються і найвищим ризиком поширення у післявоєнний період, зокрема, пов'язані з: роздрібною торгівлею фізичними товарами (39,52%), конвертацією валют (криптовалют та електронних грошей) (38,95%), позикою (37,43%) та роздрібною торгівлею віртуальними товарами (36,66%) [33, с. 148].

Водночас, експертною групою було ідентифіковано 13 загроз, у якості різновиду поширення шахрайства з платежами, з використанням банківської картки (табл. 4.23). За сучасного стану, враховуючи і перші роки повномасштабного вторгнення, найбільшим поширенням серед таких загроз характеризуються: зняття готівки з банківських карт UA в межах UA (63,70%); шахрайство з платіжними картками (фішинг) (52,3%); зняття готівки з банківських карт UA за межами UA (46,0%); PoS-покупки з використанням

скомпрометованої платіжної карти (45,1%), а також шахрайство з телефоном та інтернетом (вішинг) (44,9 %) [33, с. 148].

Переважною частиною експертів зазначається про незмінність масштабів поширення зазначеної групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення. Водночас, окремі загрози, характеризувалися певним трендом підвищення масштабів поширення (табл. 4.23, рис. 4.18): шахрайство з платіжними картками (фішинг); зняття готівки з банківських карт UA в межах UA; зняття готівки з банківських карт UA за межами UA [33, с. 148].

Таблиця 4.23

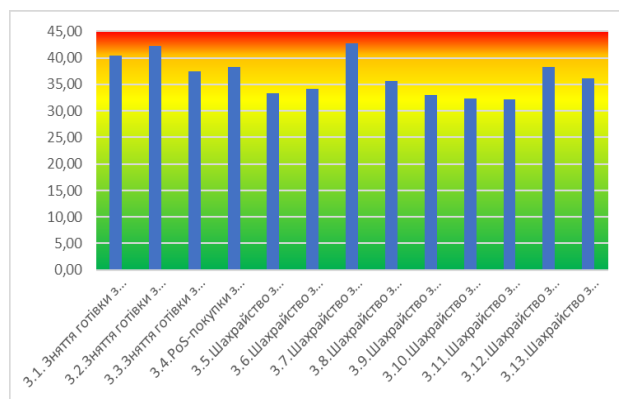
Загрози шахрайства з платежами, з використанням банківської картки

ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ З ВИКОРИСТАННЯМ БАНКІВСЬКОЇ КАРТКИ	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
3.1. Зняття готівки з банківських карт UA за межами UA	-	46,00	-	-	-	40,45
3.2. Зняття готівки з банківських карт UA в межах UA	-	63,70	-	-	-	42,23
3.3. Зняття готівки з іноземних банківських карток у межах UA	-	38,60	-	-	-	37,40
3.4. PoS-покупки з використанням скомпрометованої платіж карти	-	45,10	-	-	-	38,35
3.5. Шахрайство з платіжними картками: трешінг	-	30,90	-	-	-	33,40
3.6. Шахрайство з платіжними картками: фармінг	-	32,00	-	-	-	34,23
3.7. Шахрайство з платіжними картками: фішинг	-	52,30	-	-	-	42,80
3.8. Шахрайство з банкоматом: скімінг	-	37,40	-	-	-	35,67
3.9. Шахрайство з банкоматом: траппінг	-	29,10	-	-	-	33,04
3.10. Шахрайство з банкоматом: фантом	-	27,40	-	-	-	32,36
3.11. Шахрайство з банкоматом: jackpotting	-	26,90	-	-	-	32,17
3.12. Шахрайство з телефоном та інтернетом: вішинг	-	44,90	-	-	-	38,26
3.13. Шахрайство з телефоном та інтернетом: смішинг	-	38,60	-	-	-	36,06



Рис. 4.18 Сучасний тренд окремих загроз шахрайства з платежами

Оцінюючи ризики поширення групи загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період, такий же різновид шахрайства характеризуються найвищим ризиком (рис. 4.19): шахрайство з



платіжними картками (фішинг) (42,8%); зняття готівки з банківських карт UA в межах UA (42,23%); та зняття готівки з банківських карт UA за межами UA (40,45%) [33, с. 149].

Рис. 4.19 Оцінка ризиків поширення

загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період

4.3. Ризики поширення кримінальних загроз у кіберпросторі

Значна частина кіберзлочинів вчиняється фінансово мотивованими злочинцями. Таким злочинцям, які займаються торгівлею на кримінальних ринках або вимаганням грошей від своїх жертв, потрібні певні кошти чи інші фінансові інструменти для здійснення та отримання прибутку від своєї діяльності. У «реальних» злочинах це, швидше за все, була б готівка в місцевій або вільно конвертованій валюті, але кіберзлочинцям, які працюють у цифровому світі, потрібне цифрове рішення [65].

Дані попереднього аналізу щодо мотивації злочинців при вчиненні кіберзлочинів прямо вказують на перевагу їх матеріального збагачення (50-60%). Тобто фінансова активність, перш за все, пов'язується з отриманням швидкого прибутку і мінімізацією ризиків для самих кіберзлочинців, та набуває самих різних форм [64; 65]:

- фінансові шахрайства: використання фішингу, скімінгу, та інших методів для отримання доступу до банківських рахунків та кредитних карток;

- фінансові транзакції від жертв до злочинців та між злочинцями: використання новітніх банківських послуг та сучасних фінансових інструментів.

Водночас важливими аспектами фінансової активності кіберзлочинців є відмивання коштів та фінансування тероризму, що певним чином пов'язується не лише з матеріальним збагаченням, а й з формуванням ринку кримінальних послуг у кіберпросторі.

Експертним середовищем кіберполіції було оцінено окремі індикатори як загрози, що характеризують фінансову активність кіберзлочинців (табл. 4.24) [64; 65].

Таблиця 4.24

Фінансова активність кіберзлочинців

ВИДИ ФІНАНСОВОЇ АКТИВНОСТІ КІБЕРЗЛОЧИНЦІВ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
Шахрайство з платежами	-	67,10	-	-	-	45,37
Фінансова активність пов'язана з платежами між злочинцями	-	47,10	-	-	-	40,78
Фінансова активність пов'язана з платежами від жертв до злочинців	-	60,90	-	-	-	44,42
Відмивання коштів	-	48,00	-	-	-	41,61
Фінансування тероризму	-	32,30	-	-	-	36,45

За сучасного стану найбільшим поширенням характеризуються загрози шахрайства з платежами (67,10%), що корелюється з висновками у розділі 2, водночас є значною фінансова активність, пов'язана з платежами від жертв до злочинців (60,90%). Такий тренд зберігався упродовж останніх років та є характерним також у післявоєнний період, зокрема: значним рівнем ризику у майбутньому характеризуються шахрайство з платежами (45,37%) та

фінансова активність, пов'язана з платежами від жертв до злочинців (44,42%) [64; 65].

Серед фінансових інструментів, що використовують жертви шахрайства, найбільшим поширенням характеризуються традиційні – банківські перекази (66,0%) та використання платіжних карток – 64,3%), тренд високого рівня за якими, зберігається упродовж останніх років та характеризується найвищим рівнем ризику у післявоєнний період (табл. 4.25) [64; 65].

Таблиця 4.25

Рівень ризиків фінансової активності за платежами від жертв до злочинців

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
5.1.Банківські перекази		66,00				43,70
5.2.Платіжна картка		64,30				43,91
5.3.Шляхом поповнення мобільного рахунку		43,70				38,18
5.4.Шляхом покупки якогось предмету, речі		50,90				40,54
5.5.Системи оплати ваучерами (наприклад, paysafecard)		27,40				33,38
5.6.Використання електронних грошей		42,60				39,74
5.7.Використання криптовалют		48,60				41,35

Водночас, високим рівнем використання також визначаються платежі від жертв злочинів, що здійснюються шляхом купівлі предметів та речей (50,9%) та з використанням криптовалют (48,6%). При цьому, значним поширенням характеризується шахрайське поповнення мобільного рахунку (43,7%) та використання електронних грошей (42,6%) [64; 65].

Співвідношення активності використання різних фінансових інструментів жертвами шахрайства, залишається сталим як упродовж останніх років, так і відповідно таким самим чином характеризується тренд у післявоєнний період.

Використовуючи криптовалюту у якості платежів від жертв злочинів, найбільша активність стосується: Bitcoin (53,7%), USDT (46,9%) та Ethereum (40,6%) (табл. 4.26) [64; 65].

Таблиця 4.26

Рівень ризиків платежів від жертв до злочинців за видами криптовалют

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: криптовалюта	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
7.1.Bitcoin		53,70				40,05
7.2.Ethereum		40,60				37,44
7.3.Ripple		26,00				32,63
7.4.Monero		28,00				33,38
7.5.BNB		29,40				32,09
7.6.USDT		46,90				38,12
7.7.USDC		32,00				33,50
7.8.Zcash		23,40				31,76
7.9.Dash		25,10				31,89
7.10.Litecoin		30,60				32,59

Bitcoin найпопулярніша валюта для здійснення розрахунків між злочинцями, наприклад, під час придбання або оренди інструментів або послуг для вчинення кіберзлочинів у цифровому підпіллі. Це єдина валюта, яку приймають в більшості магазинів у Darknet та автоматизованих магазинів карток, і валюта, яку вимагають як викуп у майже у всіх сьогодишніх атаках з використанням програм-вимагачів або DoS-атаках [64; 65].

Незважаючи на те, що використання Bitcoin у злочинних цілях залишається ключовим фактором, що сприяє злочинній поведінці в мережі Інтернет, у цифровому підпіллі зростає активність інших криптовалют [64, с.57-59].

Monero – з'явилася у 2014 році. Більша частина зростаючої популярності Monero пов'язана з додатковими функціями безпеки та конфіденційності, які вона пропонує; транзакції не можуть бути віднесені до конкретного користувача/адреси, всі монети, що використовуються в транзакції, «приховані» за замовчуванням, а історії транзакцій є приватними. Monero зараз приймають у низці ринків в Darknet, а в 2017 році з'явилася перша програма вимагач – Kirk, в якій викуп потрібно було сплатити у криптовалюті Monero [64, с.57-59].

Ethereum – «smart-контракти» Ethereum можуть стати інструментом для бізнес-моделі «злочин як послуга». Поки що цього не сталося, але принаймні певні ринки в Darknet приймають Ethereum для здійснення платежів і покупок.

Zcash – це ще одна криптовалюта, яка забезпечує підвищений рівень конфіденційності для своїх користувачів, приховуючи як одержувача транзакції, так і суму транзакції.

Інші види криптовалют також використовуються для здійснення платежів від жертв злочинів до злочинців, але відносно зазначених вище видів цей рівень є дещо нижчим (23,4%-29,4%).

Упродовж останніх років тренд за видами криптовалют, що використовуються для здійснення платежів від жертв злочинів до злочинців, залишається без особливих змін.

У післявоєнний період залишається переважно без змін співвідношення щодо використання найбільш поширених видів криптовалют для здійснення платежів від жертв злочинів до злочинців, а найвищий рівень ризику передбачається щодо Bitcoin (40,05%), USDT (38,12%) та Ethereum (37,44%).

При використанні електронних грошей, у якості платежів від жертв злочинів до злочинців, найчастіше використовуються системи: EasyPay (47,1%), PayPal (42,0%), а також Webmoney (35,4%) та Qiwi (32,6%) (табл. 4.27).

У післявоєнний період залишається переважно без змін співвідношення щодо використання найбільш поширених систем електронних грошей для здійснення платежів від жертв злочинів до злочинців, а найвищий рівень ризику передбачається щодо: EasyPay (37,88%), PayPal (35,73%), Webmoney (34,27%) [64, с.57-59].

Інші системи електронних грошей також використовуються для платежів від жертв злочинів до злочинців, але відносно зазначених вище систем цей рівень є дещо нижчим (25,4%-28,6%).

Таблиця 4.27

Платежі від жертв до злочинців за видами електронних грошей

ПЛАТЕЖІ ВІД ЖЕРТВ ДО ЗЛОЧИНЦІВ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
6.1.Webmoney		35,40				34,27
6.2.PerfectMoney		28,60				33,46
6.3.Yomoney		25,40				32,06
6.4.Qiwi		32,60				33,34
6.5.PayPal		42,00				35,73
6.6.Advanced Cash		26,60				32,47
6.7.Payeer		27,70				33,16
6.8.Skrill		26,30				32,44
6.9.EasyPay		47,10				37,88

Значною у кіберпросторі є фінансова активність, що пов'язана з платежами між злочинцями.

Серед фінансових інструментів, що використовуються для здійснення платежів між злочинцями, найбільшим поширенням характеризуються – грошові мули (60,9%), використання банківських карток (60,9%) та банківські перекази (56,9%). Водночас, упродовж останніх років тренд високого рівня зберігався більше за грошовими мулами та характеризується найвищим рівнем ризику у післявоєнний період (табл. 4.28) [65, с. 158].

Таблиця 4.28

Рівень ризиків фінансової активності за платежами між злочинцями

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
4.1. Грошові мули (дропи)		60,9				45,62
4.2. Банківські перекази		56,9				42,14
4.3. Банківська картка		60,6				43,08
4.4. Системи оплати ваучерами (наприклад, paysafecard)		31,4				34,92

Багато кіберзалежних злочинів в певний момент породжують фіатну валюту з регульованим фінансовим сектором, незалежно від того, чи вона отримана із скомпрометованого банківського рахунка жертви чи з банкомату,

зараженого шкідливим програмним забезпеченням. Доступ до цих коштів часто становить значно більший ризик, ніж дії, спрямовані на те, щоб перевести їх під контроль злочинців. Саме тут з'являється потреба в послугах третьої сторони – «грошових мулів» [65, с. 158].

«Грошові мули» – це найняті, або в деяких випадках введені в оману особи, які приймають або забирають кошти від імені злочинців. Наприклад, «грошові мули» можуть відкривати нові банківські рахунки або використовувати існуючі для отримання коштів з рахунків, скомпрометованих банківськими троянськими програмами. Потім кошти перераховуються на інші рахунки, можливо, ті, що безпосередньо контролюються злочинцями, або забираються і передаються злочинцям в інший спосіб, наприклад, через бюро, що надають грошові послуги, за невелику частину коштів у вигляді оплати за такі послуги [65, с. 159].

Для вербування нічого не підозрюючих «грошових мулів» використовуються різні шахрайські схеми. Більшість з них, принаймні спочатку, вважають, їх найняли на оплачувану роботу в легальній компанії. Інші «грошові мули» повністю усвідомлюють свою діяльність і є її співучасником. Таких «грошових мулів» часто можна знайти на кримінальних форумах. Вони пропонують свої послуги в обмін на частину прибутку. Професійні «грошові мули» часто є добре організованими і працюють в координуваних групах [65, с. 159].

Найчастіше «грошовими мулами» стають люди з невеликим доходом або які взагалі не мають регулярного доходу, наприклад студенти або безробітні і люди, які вперше приїхали до певної країни. У деяких європейських країнах існує значний фінансовий стимул займатися такою діяльністю.

Такій діяльності частково сприяє легкість відкриття нових рахунків, особливо в деяких європейських країнах, де є багато банків, що дозволяють клієнтам відкривати рахунок в режимі онлайн без потреби фізично відвідувати відділення або подавати документи, що посвідчують особу [64; 65].

Тренд у майбутньому щодо традиційних банківських фінансових послуг хоча і є відносно меншим за рівнем ризику, у порівнянні з використанням грошових мулів, все ж у перспективі оцінюється експертним середовищем на рівні вищому 40% і зниження рівня ризику є лише відносним, у порівнянні з використанням грошових мулів.

Використовуючи криптовалюти у якості платежів між злочинцями найбільш поширеними також є Bitcoin (54,9%), USDT (45,4%) та Ethereum (43,4%) (табл. 4.29) [65, с. 159].

Таблиця 4.29

Рівень ризиків платежів між злочинцями за видами криптовалют

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: криптовалюти	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінювалися	Масштаби зменшилися	Ризик після війни, %
4.14. Bitcoin		54,90				41,35
4.15. Ethereum		43,40				38,12
4.16. Ripple		29,70				33,52
4.17. Monero		30,90				34,59
4.18. BNB		33,40				33,26
4.19. USDT		45,40				39,14
4.20. USDC		34,60				34,86
4.21. Zcash		28,00				32,72
4.22. Dash		27,70				32,62
4.23. Litecoin		32,00				33,46

Інші види криптовалют також використовуються для платежів між злочинцями, але відносно зазначених вище видів цей рівень є дещо нижчим (27,7%-34,6%).

Такий же тренд за видами криптовалют, що використовуються для здійснення платежів між злочинцями, зберігався упродовж останніх років. Більше того, відзначається певне збільшення масштабів використання Bitcoin, USDT та Ethereum навіть у період воєнного стану [65, с. 159].

Рівень ризиків у післявоєнний період характеризується збереженням співвідношення між активністю використання різних видів криптовалют та підвищенням у платежах між злочинцями USDC (33,5%) та Monero (33,38%).

При використанні електронних грошей, у якості платежів між злочинцями, найчастіше використовуються системи: EasyPay (46,6%), PayPal (42,6%), а також Webmoney (34,0%), Qiwi (32,0%) та PerfectMoney (31,4%) (табл. 4.30). Інші системи електронних грошей також використовуються для платежів між злочинцями, але відносно зазначених вище систем цей рівень є дещо нижчим (26,3%-30,3%) [65, с. 159].

Такий же тренд за видами систем електронних грошей, що використовуються для здійснення платежів між злочинцями, з перевагою EasyPay та PayPal, зберігався упродовж останніх років.

Водночас, у післявоєнний період щодо використання окремих найбільш поширених систем електронних грошей для здійснення платежів між злочинцями, експертним середовищем передбачається зниження рівня ризику їх використання, у порівнянні з іншими системами, хоча все ще відносно більшим рівнем ризику: EasyPay (37,94%), PayPal (36,99%) (табл. 4.30) [64, с. 160].

Таблиця 4.30

Рівень ризиків платежів між злочинцями за видами електронних грошей

ПЛАТЕЖІ МІЖ ЗЛОЧИНЦЯМИ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінювались	Масштаби зменшились	Ризик після війни, %
4.5. Webmoney		34,00				35,14
4.6. PerfectMoney		31,40				34,32
4.7. Юmoney		28,90				33,08
4.8. Qiwi		32,00				34,81
4.9. PayPal		42,60				36,99
4.10. Advanced Cash		26,30				33,05
4.11. Payeer		30,30				33,62
4.12. Skrill		26,60				32,33
4.13. EasyPay		46,60				37,94

Високим рівнем також характеризується загроза використання злочинцями механізмів відмивання коштів, із застосуванням ІТ технологій та використанням кіберпростору [117].

Загалом, відмивання коштів використовується для розподілу великих сум грошей на менші транзакції, щоб уникнути підозри; для анонімізації транзакцій та приховування слідів грошей при здійсненні операцій з криптовалютами; для перетворення незаконно отриманих коштів у фізичні активи, такі як нерухомість, автомобілі, коштовності тощо.

Тренд, використання злочинцями у кіберпросторі та застосування при цьому інформаційно-телекомунікаційних технологій з метою відмивання коштів, за останні роки (зокрема у період воєнного стану) є стабільним без зменшення, а в окремих випадках характеризується підвищенням [117].

Серед фінансових інструментів, що використовуються для відмивання коштів, найбільшим поширенням характеризуються як традиційні – банківські перекази (63,1%) та використання платіжних карток – 62,0%), тренд високого рівня за якими, зберігається упродовж останніх років та характеризується найвищим рівнем ризику у післявоєнний період (табл. 4.31), так і більш сучасні – криптовалюти (50,3%), купівля якогось предмету, речі, послуги (48,9%) та електронні гроші (44,6%) [117, с. 168-169].

Таблиця 4.31

Використання злочинцями механізмів відмивання коштів у кіберпросторі

ВІДМИВАННЯ КОШТІВ	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
8.1. Банківські перекази		63,10				42,33
8.2. Платіжні картки		62,00				42,59
8.3. Рахунки мобільних телефонів		40,86				37,31
8.4. Шляхом купівлі якогось предмету, речі, послуги		48,90				39,50
8.5. Система оплати ваучерами		26,60				32,95
8.6. Електронні гроші		44,60				39,34
8.7. Криптовалюти		50,30				41,07

Інші фінансові інструменти також використовуються для відмивання коштів, але відносно зазначених вище видів, активність є дещо нижчою: система оплати ваучерами (26,6%) та рахунки мобільних телефонів (40,86%).

Такий же тренд за видами фінансових інструментів, що використовуються для відмивання коштів, зберігався упродовж останніх років. Водночас, співвідношення рівнів ризиків, використання різних фінансових інструментів для відмивання коштів, залишається сталим і у післявоєнний період.

Здійснюючи платежі з метою відмивання коштів злочинці переважно використовують грошових мулів (84,50%) та традиційні банківські послуги – банківські карти (83,9%) та банківські перекази (79,8%). Оплата ваучерами використовується порівняно рідше, але все ж достатньо активно (54,8%) (табл. 4.32) [117, с. 168-169].

Таблиця 4.32

Використання в платежах між злочинцями фінансових механізмів для відмивання коштів

ВІДМИВАННЯ КОШТІВ: платежі між злочинцями	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
Банківські перекази		79,80				50,06
Банківська картка		83,90				51,50
Грошові мули (дропи)		84,50				54,54
Система оплати ваучерами		54,80				42,57

Такий же тренд зберігався упродовж останніх років. Водночас, співвідношення рівнів ризиків, використання різних фінансових інструментів при розрахунках між злочинцями з метою відмивання коштів, залишається сталим і у післявоєнний період. Експертами передбачається що найвищим рівнем ризику характеризуватиметься використання грошових мулів (дропів) (54,54%). Високим ризиком у майбутньому також оцінюється використання традиційних банківських інструментів: банківських карт (51,5%) та банківських переказів (50,06%) [117, с. 168-169].

У характеристиці платежів між злочинцями, з метою відмивання коштів, експерти зазначають про високу фінансову активність використання електронних грошей. Усі системи активно використовуються злочинцями,

водночас, найчастіше використовуються: EasyPay (84,0%), PayPal (80,1%), а також Webmoney (65,4%), PerfectMoney (64,1%) та Qiwi (62,8%) (табл. 4.33).

Інші системи електронних грошей також використовуються для платежів між злочинцями, але відносно зазначених вище систем цей рівень є дещо нижчим (52,6%-58,3%) [117, с. 168-169].

Такий же тренд за видами систем електронних грошей, що використовуються для здійснення платежів між злочинцями з метою відмивання коштів, з перевагою EasyPay, PayPal та PerfectMoney зберігався упродовж останніх років. Водночас, характерним є певне збільшення масштабів використання електронних грошей з метою відмивання коштів навіть у період воєнного стану.

У післявоєнний період щодо використання електронних грошей для здійснення платежів між злочинцями з метою відмивання коштів, експертним середовищем також передбачається висока фінансова активність з перевагою використання: EasyPay (48,92%), PayPal (46,56%) (табл. 4.33) [117, с.169].

Таблиця 4.33

Використання електронних грошей у розрахунках між злочинцями з метою відмивання коштів

ВІДМИВАННЯ КОШТІВ: електронні гроші	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінювалися	Масштаби зменшилися	Ризик після війни, %
4.5. Webmoney		65,40				43,62
4.6. PerfectMoney		64,10				43,12
4.7. Юmoney		58,30				40,55
4.8. Qiwi		62,80				43,79
4.9. PayPal		80,10				46,56
4.10. Advanced Cash		52,60				40,96
4.11. Payeer		56,90				42,14
4.12. Skrill		53,20				40,42
4.13. EasyPay		84,00				48,92

Значною активність у схемах по відмиванню коштів характеризується також використання криптовалюти у якості платежів між злочинцями.

Найчастіше використовуються: Bitcoin (91,5%), USDT (82,4%) та Ethereum (76,10%) (табл. 4.34) [117, с. 169].

Таблиця 4.34

Використання криптовалют у розрахунках між злочинцями з метою
відмивання коштів

ВІДМИВАННЯ КОШТІВ: криптовалюти	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
4.14. Bitcoin		91,50				51,29
4.15. Ethereum		76,10				47,31
4.16. Ripple		54,50				40,67
4.17. Monero		57,40				42,76
4.18. BNB		60,80				40,70
4.19. USDT		82,40				49,46
4.20. USDC		62,50				42,64
4.21. Zcash		52,80				39,80
4.22. Dash		50,60				39,35
4.23. Litecoin		59,10				40,61

Інші види криптовалют також використовуються, але відносно зазначених вище видів цей рівень є дещо нижчим (50,6%-62,5%).

Такий же тренд за видами криптовалют, що використовуються для здійснення платежів між злочинцями у схемах з відмивання коштів, зберігався упродовж останніх років. Водночас, характерним є певне збільшення масштабів використання криптовалют з метою відмивання коштів навіть у період воєнного стану.

У післявоєнний період щодо використання криптовалют для здійснення платежів між злочинцями з метою відмивання коштів, експертним середовищем також передбачається високий рівень ризику з перевагою використання Bitcoin (51,29%), USDT (49,46%) та Ethereum (47,31%) [117, с. 169].

Відмивання коштів залишається однією з основних злочинних активностей у Darknet. Злочинці активно використовують Darknet для приховування джерел незаконно здобутих коштів, а також для інтеграції цих

коштів у легальну економіку. Широке використання криптовалют, анонімних платіжних систем і складних схем транзакцій у Darknet сприяє підтриманню високого рівня активності у цій сфері.

За останні роки відбулися значні зміни у масштабах відмивання коштів через Darknet. Експерти відзначають збільшення активності у цій сфері. Це зростання може бути пов'язане з більшою кількістю злочинів, які генерують незаконні прибутки, такими як кіберзлочини, продаж наркотиків і контрабанда. Багато злочинців шукають нові способи легалізації доходів, використовуючи для цього можливості Darknet. Значна частина експертів вважають, що масштаби залишилися незмінними, що свідчить про вже існуючу високу базу для таких операцій.

Очікується, що ризик відмивання коштів залишиться значним і після завершення війни, оцінюється він на рівні 37,52%. Відновлення економіки, відкриття нових фінансових каналів та послаблення контролю у період після війни можуть створити додаткові можливості для відмивання коштів. Злочинні групи будуть шукати способи легалізації своїх прибутків через менше захищені фінансові системи та нові економічні можливості, які з'являться під час післявоєнної відбудови.

Готівка продовжує відігравати важливу роль, коли справа стосується злочинців, які прагнуть матеріалізувати свій прибуток, отриманий злочинним шляхом. Для неї існують вже усталені методи відмивання, її легко обміняти, вона відносно невідстежувана і псевдоанонімна – подібно до криптовалют, що використовуються у цифровому підпіллі. Як наслідок, віртуальні валюти ще не використовуються значною мірою особами, які давно займаються відмиванням грошей, і які, ймовірно, віддаватимуть перевагу давно випробуваним методам.

Однак криптовалюти продовжуватимуть набувати популярності, як в Інтернеті, так і в реальному світі, з огляду на декілька нових валют, які вже закріплюються на кримінальних ринках. Хоча поки невідомо, чи зможе якась інша криптовалюта похитнути Bitcoin з точки зору використання в злочинних

цілях, але такі криптовалюти, як Monero або Zcash, як видається, пропонують більше злочинцям, які хочуть працювати з більшою анонімністю.

Незважаючи на те, що знання та досвід щодо розслідування, відстеження та конфіскації віртуальних валют продовжують зростати у правоохоронній спільноті, за підтримки різних інструментів для ідентифікації від приватного сектору, вони часто обмежуються лише Bitcoin, і не включають інші криптовалюти, що з'являються на кримінальних ринках. Успішна правоохоронна діяльність, пов'язана з кіберзлочинцями, що використовують Bitcoin, може спонукати її користувачів до використання альтернативних криптовалют.

4.3.1. Кримінальні on-line ринки та комунікації

Хоча значна частина торгівлі незаконними товарами відбувається у відкритому Інтернеті, будь-які відкриті продажі, що не обмежуються закритими кримінальними ринками, часто включають викрадені, шахрайські або підроблені товари, які можуть видаватися за легальні. Правоохоронні органи, реєстратори доменів та постачальники хостинг-послуг можуть швидко реагувати на продаж явно незаконних товарів на веб-сайтах, що використовують звичайний хостинг.

Саме тому злочинці використовують шифрування своєї діяльності у кіберпросторі, використовуючи сучасні технології, передові методи шифрування для приховування своїх незаконних дій. Це робить виявлення та припинення таких дій надзвичайно складним для правоохоронних органів. Злочинці можуть шифрувати комунікації, файли та транзакції, забезпечуючи таким чином конфіденційність своїх операцій, таких як продаж наркотиків, кіберзлом, торгівля людьми, відмивання коштів тощо. Використання шифрування також ускладнює ідентифікацію злочинців та збір доказів проти них, що ускладнює боротьбу з кіберзлочинністю.

Водночас шифрування використовується як для захисту даних та інформації від протиправного використання, вторгнення та зловживання злочинцями, так і з метою приховування діяльності від правоохоронних органів. Спектр інструментів такого характеру є значним (рис. 4.20).

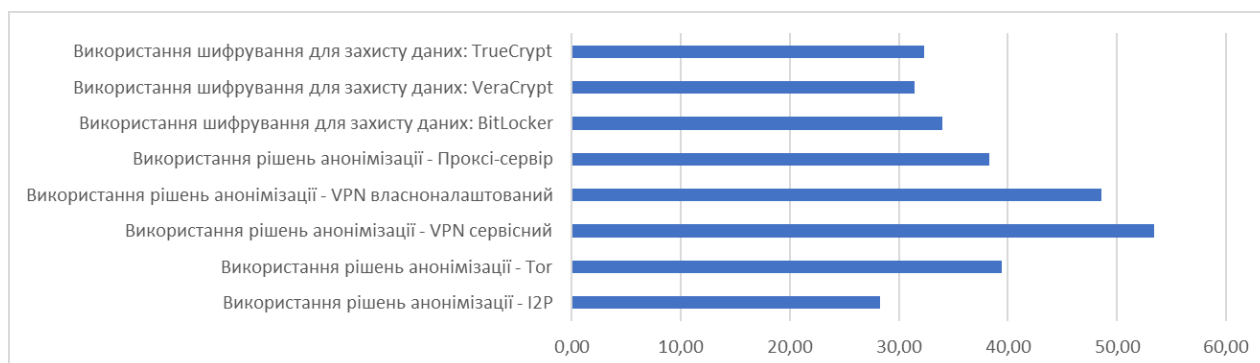


Рис. 4.20 Способи шифрування та анонімізації

На основі наведених даних (табл. 4.35) можна зробити висновок, що VPN-сервіси та власноналаштовані VPN демонструють найвищий рівень популярності серед інструментів анонімізації, з показниками 53,40% і 48,60% відповідно. Це свідчить про те, що користувачі вважають ці інструменти більш надійними та простими у використанні для захисту своєї приватності та даних. Хоча VPN (Virtual Private Network) головним чином використовується для захисту особистих даних і конфіденційності в інтернеті, злочинці також застосовують VPN для шифрування трафіку та приховування своєї реальної IP-адреси, що ускладнює їх виявлення.

Таблиця 4.35

Способи шифрування та анонімізації діяльності в кіберпросторі

СПОСОБИ ШИФРУВАННЯ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
Використання рішень анонімізації - I2P		28,30	Збільшились	Не змінилися	Зменшились	34,36
Використання рішень анонімізації - Tor		39,40	Збільшились	Не змінилися	Зменшились	36,44
Використання рішень анонімізації - VPN сервісний		53,40	Збільшились	Не змінилися	Зменшились	39,28
Використання рішень анонімізації - VPN власноналаштований		48,60	Збільшились	Не змінилися	Зменшились	37,73
Використання рішень анонімізації - Проксі-сервір		38,30	Збільшились	Не змінилися	Зменшились	35,13
Використання шифрування для захисту даних: BitLocker		34,00	Збільшились	Не змінилися	Зменшились	34,27
Використання шифрування для захисту даних: VeraCrypt		31,40	Збільшились	Не змінилися	Зменшились	33,73
Використання шифрування для захисту даних: TrueCrypt		32,30	Збільшились	Не змінилися	Зменшились	33,13

Tor також користується значним попитом (39,40%), що вказує на його важливість як засобу забезпечення анонімності в інтернеті, особливо для користувачів, які прагнуть більш високого рівня захисту від спостереження. Tor (The Onion Router) хоча не є безпосереднім шифруванням даних, все ж використовує багатошарове шифрування для маршрутизації інтернет-трафіку через декілька вузлів, що допомагає приховати IP-адресу користувача і забезпечує анонімність. Цей метод часто використовується злочинцями для приховування своєї діяльності в темному вебі.

I2P, хоча й менш розповсюджений (28,30%), все ж таки залишається важливим інструментом для певної частини користувачів, які надають перевагу децентралізованим анонімним мережам.

Використання шифрування для захисту даних, таких як BitLocker (34,00%), VeraCrypt (31,40%) та TrueCrypt (32,30%), свідчить про актуальність цих рішень для захисту особистих та конфіденційних даних.

Водночас, останнім часом, що включає і період воєнного стану, VPN-сервіси показали відносне розширення масштабів використання. Це може бути пов'язано з підвищенням обізнаності про безпеку даних та приватність серед користувачів.

Tor також показав позитивну динаміку зростання, що свідчить про стійкий інтерес до цього інструменту серед користувачів, які прагнуть зберегти анонімність в інтернеті.

Стабільне використання спостерігається для BitLocker, що може бути зумовлено його популярністю серед корпоративних користувачів і організацій.

Незначне зменшення використання спостерігається у випадку з TrueCrypt, що може бути пов'язано з наявністю альтернатив.

Оцінюючи ризики використання у майбутньому (після війни), VPN-сервіси та власноналаштовані VPN мають найвищий прогнозований рівень ризику (39,28% та 37,73% відповідно). Це може бути наслідком можливих

нових регуляцій, зловживань чи викликів, пов'язаних із забезпеченням анонімності та безпеки в умовах зростаючої кіберзагрози.

Tor також має високий ризик (36,44%), що вказує на можливість подальших спроб його блокування або моніторингу в різних країнах.

Ризики для шифрувальних рішень, таких як BitLocker, VeraCrypt та TrueCrypt, залишаються відносно стабільними (близько 33-34%), що може свідчити про меншу ймовірність значних змін у їх використанні, але все ще враховувати можливі нові вразливості або загрози.

Результати опитування підкреслюють важливість VPN та інших рішень для анонімізації в сучасних умовах, зокрема з огляду на загострення уваги до питань приватності та безпеки в кіберпросторі. У той же час, шифрування даних залишається критично важливим для захисту особистої та корпоративної інформації. Прогнозовані ризики свідчать про необхідність постійного моніторингу та вдосконалення цих технологій для забезпечення їх надійності в майбутньому.

Серйозною загрозою для безпеки та правопорядку залишається використання злочинцями Darknet, що є прихованою частиною інтернету, яка використовується для анонімної діяльності, часто незаконної. Злочинці використовують його для торгівлі наркотиками, зброєю та людьми, а також для кіберзлочинів, таких як продаж вкрадених даних і шкідливого програмного забезпечення. Анонімність і шифрування ускладнюють роботу правоохоронних органів, роблячи відстеження злочинців майже неможливим. Крім того, використання криптовалют у Darknet сприяє відмиванню грошей та іншим фінансовим злочинам.

Торгівля незаконними товарами в Darknet має кілька переваг. По-перше, транзакції тут дуже анонімні; ні покупцю, ні продавцю не потрібно розкривати особисту інформацію, хоча покупець все ж має надати адресу для доставки фізичних товарів. Транзакції здійснюються за допомогою віртуальних валют, які важко відстежити. Крім того, ризик фізичної небезпеки тут менший порівняно з вуличною торгівлею. Darknet доступний для будь-кого з

підключенням до Інтернету, незалежно від віку чи місцезнаходження, і пропонує широкий вибір постачальників та незаконних товарів. Також покупці можуть оцінювати якість товарів і надійність постачальників.

Ці фактори зробили торгівлю незаконними товарами доступною не лише новим клієнтам, які інакше могли б не мати можливості чи бажання взаємодіяти з реальними кримінальними постачальниками, але й новим кримінальним торговцям. Багато з них можуть працювати самотійно, що було б складно на реальних ринках, де домінують організовані злочинні групи.

Аналіз даних вказує на те, що Darknet продовжує бути важливою платформою для різноманітних видів кіберзлочинності, причому окремі напрями показують значне зростання масштабів. Зловмисники активно користуються як криптографічними інструментами, так і вразливостями програмного забезпечення для досягнення своїх цілей. У майбутньому ризики, пов'язані з цими видами активності, залишатимуться високими, що підкреслює необхідність підвищеної уваги до кібербезпеки з боку урядів, організацій і окремих користувачів.

Ринки в Darknet продовжують зростати з кожним роком, як за чисельністю, так і за розміром. Нові ринки відкриваються або спонтанно, або заповнюючи порожнечу, яка утворилася після інших ринків, які закрилися або добровільно, або після екзит-скаму, або в результаті заходів, вжитих правоохоронними органами. Ринки в Darknet продовжують становити серйозну загрозу, забезпечуючи легкий, анонімний доступ до великої кількості незаконних товарів, які сприяють вчиненню інших різноманітних злочинів.

Спектр кримінальних ринків та інших інтересів в Darknet є значним (рис. 4.21). Проте правоохоронні органи переважно зосереджують увагу на найбільш активних напрямках та, які несуть найбільшу загрозу для суспільства, зокрема: ринок наркотиків, зброї, контрафакту, торгівлі онлайн-матеріалами, пов'язаними з насильством над дітьми тощо.

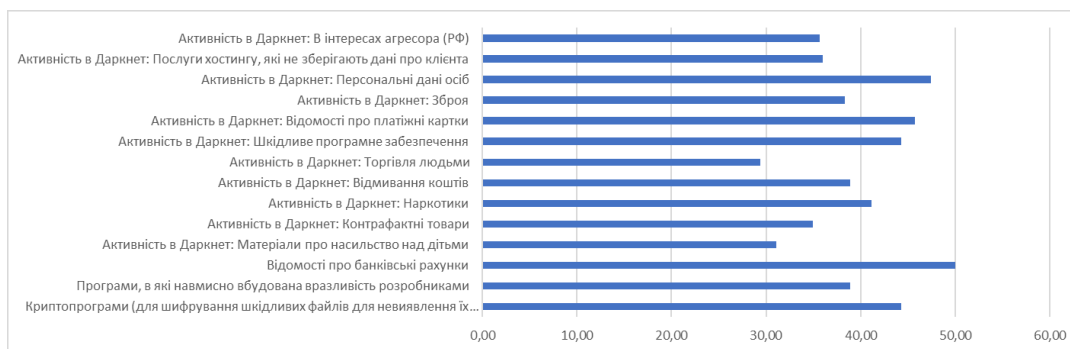


Рис. 4.21 Активність злочинців в Darknet

На основі експертних даних видно, що найпоширенішою формою активності в Darknet є використання криптопрограм, які спрямовані на шифрування шкідливих файлів, щоб уникнути виявлення антивірусними програмами (табл. 4.36). Це підтверджується високим показником сучасного поширення (44,3%) серед усіх видів активності. Відомості про банківські рахунки (50%), персональні дані осіб (47,4%), відомості про платіжні картки (45,7%), а також шкідливе програмне забезпечення (44,3%) також займають значну частку у загальній структурі кіберзлочинності.

Таблиця 4.36

Активність злочинців в Darknet

АКТИВНІСТЬ В ДАРКНЕТ	Оцінка сучасного поширення	%	Масштаби збільшилися	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
Криптопрограми (для шифрування шкідливих файлів для невиявлення їх антивірусами)		44,30				38,60
Програми, в які навмисно вбудована вразливість розробниками		38,90				37,32
Відомості про банківські рахунки		50,00				39,65
Матеріали про насильство над дітьми		31,10				35,74
Контрафактні товари		34,90				35,76
Наркотики		41,10				40,30
Відмивання коштів		38,90				37,52
Торгівля людьми		29,40				35,56
Шкідливе програмне забезпечення		44,30				37,86
Відомості про платіжні картки		45,70				39,23
Зброя		38,30				39,95
Персональні дані осіб		47,40				39,32
Послуги хостингу, які не зберігають дані про клієнта		36,00				36,83
В інтересах агресора (рф)		35,70				37,10

Також варто відзначити високий рівень активності, пов'язаної з програмами, в які навмисно вбудована вразливість розробниками (38,9%),

відмиванням коштів (38,9%), та операціями, що проводяться в інтересах агресора (35,7%).

За останні роки, враховуючи і період воєнного стану, масштаби використання Darknet злочинцями переважно залишалися стабільними. Водночас, певним збільшенням характеризуються напрями, що стосуються: відомостей про банківські рахунки та платіжні картки, персональні дані осіб та діяльність в інтересах агресора. Це стосується і поширення криптограм для шифрування шкідливих файлів та шкідливого програмного забезпечення. Помітно збільшився масштаб активності, пов'язаної з відмиванням коштів, що свідчить про важливість фінансової анонімності у Darknet та наркотиками і зброєю, що зумовлює популярність цих напрямів серед злочинців через високий попит на нелегальні товари та послуги.

Ризик використання активності в Darknet у майбутньому після війни залишається високим для багатьох категорій. Найбільший ризик мають наркотики (40,3%) та зброєю (39,95%), а також поширення відомостей про банківські рахунки (39,65%), платіжні картки (39,23%) та персональні дані осіб (39,32%), вказуючи на важливість захисту конфіденційної інформації. Також варто відзначити високий ризик для криптопрограм (38,6%) і шкідливого програмного забезпечення (37,86%), що свідчить про постійну актуальність кібербезпеки.

Ринок наркотиків безсумнівно є найбільшим кримінальним ринком у Darknet, де пропонується майже будь-який клас наркотиків і відправляється в будь-яку точку світу. Хоча вважається, що більшість продавців є одиночними правопорушниками з невеликим оборотом, експерти Європол зазначають про високу ймовірність діяльності організованих злочинних груповань, які отримують значні прибутки.

За результатами опитування, сучасне поширення цього виду активності оцінюється на рівні 41,1%. Це досить високий показник, який свідчить про значний попит на наркотики в нелегальному онлайн-середовищі. Згідно з даними, масштаби торгівлі наркотиками через Darknet помітно збільшилися за

останні роки. Ймовірно це зростання пояснюється кількома факторами. Перш за все, Darknet надає високий рівень анонімності як для покупців, так і для продавців, що мінімізує ризик викриття правоохоронними органами. Використання криптовалют для транзакцій додатково ускладнює відстеження фінансових потоків, роблячи такі операції привабливими для злочинців. Крім того, пандемія COVID-19 також могла стати каталізатором зростання торгівлі наркотиками в Darknet, оскільки багато традиційних способів постачання та збуту були порушені карантинними обмеженнями. У цих умовах споживачі та продавці звернулися до онлайн-каналів, що дозволяють уникнути особистих контактів та зменшити ризик зараження.

Прогнозований ризик використання торгівлі наркотиками через Darknet у майбутньому оцінюється на рівні 40,3%, що є одним з найвищих показників серед усіх видів активності в Darknet. Такий високий ризик пояснюється декількома причинами. По-перше, попит на наркотики не зменшується, а Darknet продовжує залишатися надійним і анонімним каналом для їх придбання. По-друге, з кожним роком технології анонімності стають більш досконалими, що ускладнює роботу правоохоронних органів і робить боротьбу з цією проблемою більш складною. Крім того, розвиток нових технологій, таких як шифрування і безпечні канали зв'язку, може ще більше зміцнити позиції Darknet як платформи для нелегальної торгівлі наркотиками.

Отже, торгівля наркотиками в Darknet є однією з найбільш серйозних загроз, яка демонструє тенденцію до зростання. Ця сфера злочинної активності використовує переваги сучасних технологій анонімності та шифрування, що значно ускладнює її виявлення та припинення. У зв'язку з цим, необхідність у посиленні заходів кібербезпеки та розробці нових методів боротьби з онлайн-наркоторгівлею залишається критично важливою.

Така онлайн-спільнота здійснює свою діяльність окремо від інших спільнот, що працюють на кримінальних ринках. Ці клієнти та товари не є бажаними на кримінальних ринках, а тому вони утворюють свої власні закриті спільноти в Darknet. Інтернет-торгівля матеріалами, пов'язаними з

насильством над дітьми, через Darknet є одним із найбільш жахливих аспектів кіберзлочинності. За результатами опитування експертів, поширення цього виду діяльності становить 31,1%, що свідчить про значну кількість таких злочинних операцій у мережі. Darknet продовжує бути платформою, яка забезпечує анонімність і прихованість для тих, хто бере участь у створенні, розповсюдженні та споживанні подібного контенту.

Дані свідчать, що масштаби інтернет-торгівлі матеріалами, пов'язаними з насильством над дітьми, через Darknet за останні роки незначно зросли, але викликає серйозну стурбованість стабільність цієї злочинної діяльності. Збільшення може бути зумовлене кількома факторами, серед яких розвиток технологій шифрування, що забезпечують ще більшу анонімність злочинців, а також розширення доступу до інтернету в різних куточках світу. Darknet залишається привабливим середовищем для тих, хто прагне приховати свою діяльність від правоохоронних органів, використовуючи анонімні мережі, такі як Tor, і криптовалюти для здійснення фінансових транзакцій.

Рівень ризику використання Darknet для інтернет-торгівлі матеріалами, пов'язаними з насильством над дітьми, у майбутньому оцінюється на рівні 35,74%. Хоча цей показник є дещо нижчим у порівнянні з іншими видами злочинної діяльності в Darknet, він все одно вказує на серйозну загрозу. Це пояснюється тим, що злочинці, які займаються такими діями, швидко адаптуються до нових технологій і методів уникнення виявлення. Наприклад, використання платних доступів, шифрованих приватних каналів зв'язку та складних мереж розподілу контенту дозволяє злочинцям захищати свої операції від правоохоронців. Крім того, поєднання легкого доступу до технологій та зростання кількості платформ, які пропонують анонімність, створює ідеальні умови для продовження та навіть зростання цієї злочинної діяльності.

Отже, інтернет-торгівля матеріалами, пов'язаними з насильством над дітьми, через Darknet є однією з найбільш небезпечних і неприйнятних форм кіберзлочинності. Незважаючи на певну стабільність рівня поширення,

високий ризик у майбутньому вимагає вжиття негайних заходів з боку міжнародної спільноти, урядів і правоохоронних органів. Це включає розвиток нових технологій для моніторингу та виявлення подібного контенту, а також посилення законодавства і покарання за такі злочини. Спільні зусилля правоохоронців і технологічних компаній можуть допомогти зменшити масштаби цього жахливого явища і забезпечити більший захист дітей від насильства.

Більшість спільнот, пов'язаних із кіберзлочинністю, в яких можна придбати і продати інструменти та послуги для вчинення кіберзлочинів, як правило, працюють за межами Darknet, на спеціальних форумах у глибокому Інтернеті. Незважаючи на те, що співвідношення інструментів та послуг для вчинення кіберзлочинів, що доступні на ринках в Darknet, до тих, що доступні на форумах кіберзлочинців у глибокому Інтернеті, залишається незрозумілим, деякі держави-члени ЄС відзначають, що такі послуги, як «куленепробивний» хостинг, шкідливе ПЗ та програма-вимагач як послуга є легко доступними.

Інструменти та послуги для вчинення кіберзлочинів через Darknet стають все більш популярними і доступними, що значно ускладнює боротьбу з кіберзлочинністю. Результати опитування експертів демонструють, що використання Darknet для придбання таких інструментів та послуг є суттєво поширеним. Darknet пропонує широкий спектр ресурсів для злочинців, від програмного забезпечення для атак до спеціалізованих послуг з навчання хакінгу. Це середовище забезпечує високий рівень анонімності, що дозволяє користувачам уникати виявлення правоохоронними органами.

Згідно з дослідженням, інструменти та послуги для кіберзлочинів займають значну частку в Darknet. Наприклад, криптопрограми для шифрування шкідливих файлів, які уникають виявлення антивірусами, мають поширеність на рівні 44,3%. Це свідчить про те, що подібні програми є одними з основних засобів, якими користуються кіберзлочинці для здійснення атак. Послуги хостингу, які не зберігають дані про клієнта (36%), також широко використовуються для забезпечення анонімності та уникнення

відповідальності. Це дозволяє зловмисникам розміщувати свої ресурси, не залишаючи слідів, що значно ускладнює їх виявлення та притягнення до відповідальності.

За останні роки масштаби використання інструментів та послуг для кіберзлочинів через Darknet дещо змінилися. Наприклад, збільшилася поширеність шкідливого програмного забезпечення, яке доступне через Darknet та криптопрограм для шифрування шкідливих файлів, які уникають виявлення антивірусами, а використання хостинг-послуг із високим рівнем анонімності характеризується відносною стабільністю. Такі показники свідчать про підвищення інтересу до цих послуг, що може бути викликано зростанням складності кіберзахисту та бажанням злочинців використовувати новітні технології для досягнення своїх цілей. Розвиток інструментів, таких як експлойти, що використовують невідомі вразливості («нульові дні»), став поширеним явищем, оскільки злочинці прагнуть знайти нові способи обходу систем безпеки.

Рівень ризику використання інструментів та послуг для кіберзлочинів через Darknet у майбутньому оцінюється досить високо. Наприклад, криптопрограми мають ризик на рівні 38,6%, що є одним із найвищих серед інших злочинних активностей. Високий ризик пов'язаний із зростанням професіоналізму кіберзлочинців та постійним удосконаленням методів атаки. Це створює серйозні виклики для кібербезпеки, оскільки антивірусні рішення і традиційні методи захисту стають менш ефективними. Збільшення кількості послуг, що пропонуються «кіберзлочинцями на замовлення», також становить значну загрозу. Такі послуги, що включають оренду ботнетів, викрадення даних, шантаж і навіть організацію кібератак на конкурентів, можуть мати серйозні наслідки для бізнесу та національної безпеки.

Отже, інструменти та послуги для вчинення кіберзлочинів через Darknet є невід'ємною частиною сучасного ландшафту кіберзлочинності. Їх поширення та адаптація до нових умов технологічного середовища створюють серйозні виклики для правоохоронних органів та спеціалістів з кібербезпеки.

Необхідні скоординовані зусилля на глобальному рівні для розробки ефективних стратегій протидії кіберзлочинності, що включають впровадження новітніх технологій, посилення законодавства та міжнародної співпраці. Лише завдяки комплексному підходу можна зменшити вплив кіберзлочинів на суспільство та забезпечити захист від їхніх руйнівних наслідків.

Порушення прав інтелектуальної власності є розповсюдженим і зростаючим світовим явищем. Більшість підроблених продуктів може порівняно легко продаватися в поверхневому Інтернеті або змішуватися з оригінальними товарами. Як наслідок, на контрафактні товари припадає лише від 1,5 % до 2,5 % пропозицій на ринках в Darknet. Більше того, найбільш часто зустрічаються ті контрафактні товари, які є явно незаконними: фальшиві банкноти та підроблені ідентифікаційні документи, на які припадає майже третина і майже чверть пропозицій, відповідно. Більшість розслідувань правоохоронних органів в ЄС щодо контрафактних товарів у Darknet стосуються фальшивих банкнот.

Інтернет-торгівля контрафактними товарами є серйозною проблемою, яка має значні економічні, соціальні та екологічні наслідки. Вона загрожує діяльності чесного бізнесу, що платить податки, і підриває економіку держави. Контрафактні товари часто не відповідають стандартам якості та безпеки, що може призвести до шкоди здоров'ю споживачів. Крім того, торгівля підробками підтримує тіньовий бізнес та організовану злочинність. Виробництво і розповсюдження контрафактної продукції також сприяє втраті робочих місць та зменшенню податкових надходжень. [47]

Використання контрафактних товарів у Darknetі є значною проблемою, яка має свої особливості та ризики. Контрафактні товари займають значну частину ринку Darknet, з оцінкою сучасного поширення на рівні 34.90%. Це свідчить про те, що попит на такі товари залишається стабільно високим.

Масштаби використання контрафактних товарів у Darknet мають тенденцію до збільшення, що може бути пов'язано з підвищеним попитом та

доступністю. Водночас, значна частина ринку залишається стабільною, що свідчить про постійний попит на ці товари. Незначна частина ринку зменшується, можливо, через посилення заходів безпеки та боротьби з контрафактом.

Ризик використання контрафактних товарів у Darknet після війни залишається високим (35.76%). Це може бути пов'язано з економічною нестабільністю та зростанням попиту на дешеві товари. В умовах післявоєнного періоду, коли економіка може бути ослаблена, попит на контрафактні товари може зрости, що створює додаткові ризики.

Таким чином, контрафактні товари залишаються значною частиною ринку Darknet, з тенденцією до зростання та високими ризиками у майбутньому. Це вимагає посилення заходів безпеки та боротьби з контрафактом для зменшення негативного впливу на економіку та суспільство.

Скомпрометовані дані – це ще один ключовий товар, яким зазвичай продається в Інтернеті, а потім використовується для сприяння шахрайству. Як правило, це фінансові дані, наприклад скомпрометовані дані платіжних карток, як «дампи» (дані, скопійовані з магнітної смуги картки), так і «CVV-коди» (дані, необхідні для здійснення оплати картою в Інтернеті або через телефон). Проте будь-які дані, які можуть бути використані для шахрайства чи вчинення інших злочинів, також є доступними для продажу. Сюди входить все, від списків повних персональних даних та відсканованих документів до списків адрес електронної пошти та імен облікових записів.

На сьогоднішній день *відомості про банківські рахунки* залишаються одними з найпопулярніших товарів у Darknet. Оцінка сучасного поширення цих даних становить 50%. Це вказує на те, що половина злочинних операцій, пов'язаних із фінансовою інформацією, включає саме відомості про банківські рахунки. Злочинці активно шукають ці дані, щоб отримати доступ до коштів, здійснювати незаконні транзакції та відмивати гроші. Популярність таких

даних пояснюється їхньою універсальністю і можливістю використовувати їх у різних фінансових злочинах.

За останні роки спостерігається помітне збільшення активності навколо банківських рахунків у Darknet. Експерти вказали на зростання обсягів злочинних операцій із цими даними. Це може бути пов'язано з розвитком технологій, що дозволяють злочинцям отримувати доступ до таких даних більш ефективно. Крім того, економічна нестабільність та загальне зростання кількості користувачів онлайн-банкінгу підвищують привабливість цього типу інформації. Водночас, значна частина респондентів вважають, що масштаби залишаються на стабільному рівні, що свідчить про постійний попит і попередню високу активність у цій сфері.

Експерти прогнозують, що ризик використання відомостей про банківські рахунки залишиться високим і після закінчення війни. Оцінка ризику складає близько 40%. Післявоєнний період може супроводжуватися економічною нестабільністю та відновленням банківської системи, що створить нові можливості для зловмисників. У цей час банки та користувачі можуть виявитися більш вразливими до кіберзлочинів, що підвищує ймовірність використання цієї інформації у злочинних схемах.

Відомості про платіжні картки є одним із основних об'єктів інтересу злочинців у Darknet. Поточна оцінка поширення цих даних становить 45,7%. Злочинці використовують ці дані для проведення несанкціонованих платежів, зняття коштів через банкомати та онлайн-шахрайства. Відомості про платіжні картки легко монетизуються, що робить їх дуже цінним товаром у кримінальному середовищі.

Незважаючи на зростання загальної кількості випадків кіберзлочинності, незначна кількість експертів зазначили про збільшення масштабів використання даних про платіжні картки. Це може свідчити про те, що заходи безпеки банківських установ та постачальників платіжних послуг стають більш ефективними, стримуючи зростання злочинної активності в цій сфері. Водночас, значна кількість експертів вважає, що масштаби

залишаються стабільними, що підкреслює постійний інтерес до таких даних серед злочинців.

Очікується, що ризик використання даних про платіжні картки залишатиметься високим і після закінчення війни, оцінюється він на рівні 39,23%. Війна створює умови, в яких послаблюються заходи контролю та нагляду, що відкриває додаткові можливості для злочинців. Післявоєнний період може характеризуватися відновленням економічної діяльності, збільшенням кількості транзакцій, що може сприяти збільшенню кількості кіберзлочинів, пов'язаних з платіжними картками.

Персональні дані осіб є одними з найважливіших активів у Darknet, і їхня популярність залишається високою. Поточна оцінка поширення цих даних становить 47,4%. Персональні дані використовуються злочинцями для різних видів шахрайства, включаючи крадіжку особистості, соціальну інженерію, створення фальшивих акаунтів або здійснення несанкціонованих фінансових операцій. Вони також можуть слугувати базою для подальшого збору більш цінної інформації.

За останні роки ситуація з використанням персональних даних дещо стабілізувалася. Менша кількість експертів відзначають збільшення масштабів цієї активності. Водночас значна частина вважають, що масштаби залишилися незмінними. Це може свідчити про високу насиченість ринку персональними даними та стабільний попит на них. З одного боку, злочинці вже мають достатній доступ до таких даних, а з іншого – заходи безпеки поступово покращуються, обмежуючи можливості несанкціонованого збору інформації.

Ризик використання персональних даних у майбутньому оцінюється на рівні 39,32%. Після закінчення війни можна очікувати підвищення активності з боку злочинців, оскільки в умовах відновлення суспільства та економіки потреба у контролі за особистими даними зростатиме. Зростання використання цифрових технологій під час і після війни може створити додаткові можливості для зловживань персональними даними. Злочинці

можуть використовувати вразливості в інформаційних системах та менш захищені канали для отримання доступу до персональної інформації.

Таким чином, загалом відомості про банківські рахунки, платіжні картки та персональні дані залишаються одними з найбільш цінних категорій інформації в Darknet. Поточна ситуація свідчить про стабільний попит на ці дані, який зберігається завдяки можливості їх використання у фінансових шахрайствах, крадіжці особистості та інших злочинах. Хоча за останні роки спостерігається певне збільшення активності щодо банківських рахунків та персональних даних, загалом масштаби злочинної діяльності залишаються на стабільно високому рівні. У майбутньому, після закінчення війни, ризик використання цих даних залишається значним, оскільки суспільство стикнеться з новими викликами у сфері кібербезпеки під час відновлення та реорганізації.

Лише на декількох ринках озброєння відкрито вказано як категорія товарів, що продаються на їхніх сайтах. На цих ринках такі пропозиції становлять, як правило, менше 1,5 % від загальної кількості пропозицій, хоча в AlphaBay цей показник становив більше 5 000 пропозицій. З огляду на кількість терористичних атак та рівень такої загрози, потенційна легка доступність вогнепальної зброї та вибухових речовин є тривожною тенденцією.

Продаж зброї є ще однією важливою категорією злочинної діяльності у Darknet. Поточний рівень поширення цієї діяльності становить 38,3%. Незаконна торгівля зброєю через Darknet включає продаж вогнепальної зброї, боєприпасів, вибухових речовин та інших засобів насильства. Такі операції часто проводяться анонімно, що дозволяє покупцям і продавцям уникати правоохоронних органів.

Масштаби продажу зброї в Darknet незначно змінилися за останні роки. Певна частка експертів відзначили збільшення активності в цій сфері, що може бути пов'язано зі зростанням попиту на зброю через конфлікти та нестабільність. Водночас більша частина респондентів вважають, що

масштаби залишилися стабільними, що свідчить про постійний попит на зброю серед злочинців, які використовують Darknet для нелегальних закупівель.

Оцінка ризику використання Darknet для продажу зброї після війни залишається високою і становить 39,95%. Після завершення бойових дій залишки зброї та боєприпасів можуть легко потрапити на чорний ринок. Крім того, зростання потреб у безпеці, а також можливий підйом злочинності в постконфліктний період можуть підвищити попит на зброю серед населення. Це створює додаткові ризики і підвищує ймовірність використання Darknet для нелегальних операцій із продажу та придбання зброї.

Таким чином, діяльність, пов'язана з торгівлею зброєю, залишається значущою проблемою в Darknet. Спостерігається стабільний попит і висока активність злочинців. За останні роки масштаби цих злочинів характеризуються збільшенням та стабільно високим рівні, що свідчить про тривалий інтерес до цієї злочинної діяльності. У майбутньому, після закінчення війни, очікується, що ризик продовження інтернет-торгівлі зброєю залишатиметься значним. Економічна та соціальна нестабільність, поєднана з послабленим контролем у постконфліктний період, створить додаткові можливості для нелегального обігу зброї через Darknet.

Правоохоронні органи спостерігають перехід до використання злочинцями захищених додатків та інших сервісів у всіх сферах злочинності. Більшість таких додатків є програмами відомих розробників, які користуються популярністю серед населення. Оскільки вони стають все більш захищеними, наприклад, включають наскрізне шифрування, вони легко приймаються злочинцями, які хочуть мати надійний та безпечний засіб зв'язку. Це створює додаткові труднощі для правоохоронних органів, оскільки багато традиційних методів розслідування, наприклад прослуховування, стають неефективними.

На основі даних опитування експертів щодо способів комунікації між злочинцями в кіберпросторі можна зробити кілька важливих висновків (табл. 4.37). Насамперед, форуми Deep Web і Darknet залишаються

найпоширенішим методом комунікації серед злочинців, демонструючи найвищий рівень використання – 46%. Це підтверджує, що цей спосіб є особливо привабливим завдяки його анонімності та важкодоступності для правоохоронних органів. Значна частина експертів вважають, що масштаби використання цих форумів збільшилися за останні роки, і вони оцінюються як найризикованіші для використання у майбутньому (37,85%).

Таблиця 4.37

Інструменти комунікації між злочинцями в кіберпросторі

КОМУНІКАЦІЇ МІЖ ЗЛОЧИНЦЯМИ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
Форуми Deep Web/Darknet		46,00	51	103	39	37,85
Email		32,00	24	108	47	32,80
Відкриті форуми, соціальні мережі		42,90	44	107	40	35,70
ICQ		20,30	15	96	50	28,98
IRC		18,00	13	102	43	28,81
Jabber		26,90	29	102	42	32,23
Веб-чат		31,10	27	105	45	31,41

Відкриті форуми та соціальні мережі також займають значне місце в арсеналі злочинців із поширеністю 42,9%. Їхня відкритість і доступність роблять їх привабливими для швидкої комунікації та обміну інформацією. Хоча значна частина експертів вважають, що їх використання зросло, відсоток тих, хто вважає, що масштаби залишилися незмінними, теж залишається значним. Ризик використання цих платформ після війни теж є високим – 35,7%.

Значну частку комунікацій все ще займає електронна пошта (32%). Проте, на відміну від форумів у Darknet, використання email демонструє тенденцію до зниження масштабів його використання. Однак ризик використання email у майбутньому залишається суттєвим, із показником 32,8%, що вказує на те, що цей канал комунікації все ще є важливим для злочинців.

Традиційні засоби комунікації, такі як ICQ і IRC, сьогодні використовуються значно рідше, із поширеністю на рівні 20,3% та 18% відповідно. Ці способи втратили популярність, причому значна частина експертів вказують на зменшення масштабів їх використання. Відповідно, вони мають найнижчий ризик використання в майбутньому. Internet Relay Chat (IRC) – один з найстаріших інструментів для спілкування в Інтернеті, який дає змогу створювати групові чати, приватні повідомлення, передавати дані та обмінюватися файлами. Незважаючи на зменшення рівня його використання, потенціал його за рівнем ризику у майбутньому залишається значним (28,81%).

Jabber і веб-чати займають проміжне положення. Поширеність Jabber становить 26,9%, а веб-чатів – 31,1%. Хоча їх використання також зменшується, вони все ще залишаються актуальними через їх здатність забезпечити певний рівень захищеності та анонімності. Jabber забезпечує зашифровану комунікацію та має додаткову перевагу, яка полягає в тому, що користувачі можуть розмішувати власні приватні jabber-сервери. Ризик їх використання після війни оцінюється на рівні 32,23% та 31,41% відповідно, що свідчить про їхню потенційну значимість для злочинців у майбутньому.

Отже, можна зробити висновок, що злочинці в кіберпросторі продовжують використовувати широкий спектр каналів комунікації, адаптуючи свої стратегії залежно від рівня анонімності та безпеки, які можуть запропонувати ці платформи. Форми комунікації, що гарантують найвищий рівень конфіденційності, залишаються найбільш поширеними та ризикованими з точки зору їх можливого використання у майбутньому.

На основі наданих даних щодо *спілкування між злочинцями та жертвами* можна зробити наступні висновки (табл. 4.38).

Серед засобів комунікації, які найчастіше використовуються для взаємодії між злочинцями та їхніми жертвами, найпоширенішим є Telegram. З поширеністю 66%, Telegram залишається головним каналом, який використовують злочинці для зв'язку з жертвами.

Інструменти комунікації між злочинцями та жертвами кіберзлочинів

Спілкування між злочинцями та жертвами	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
Email		34,00				32,59
FaceTime		27,10				29,97
Messenger		46,00				35,07
Skype		26,90				29,82
Viber		52,30				40,18
Web-based chatroom		21,40				30,15
WhatsApp		56,30				41,59
Telegram		66,00				45,40
IMO		19,70				29,07
Signal		39,40				35,46
Веб-чат		30,30				31,10
WeChat		21,40				29,49
QQ		19,10				28,81
Snapchat		20,60				29,11
Riot		18,60				28,74
Threema		21,70				29,08
LINE		16,30				28,23
Wire		16,60				28,11
Voxer		15,40				28,69
Slack		16,90				28,30
GroupMe		16,60				28,26
IM+		16,60				28,18

Більш частина експертів відзначають збільшення масштабів його використання, що свідчить про зростаючу популярність цього месенджера. Рівень ризику використання Telegram після війни оцінюється на рівні 45,4%, що є найвищим серед усіх засобів комунікації, проаналізованих у цій таблиці (*прим.: збір даних та їх аналіз здійснювався до подій серпня 2024 року, пов'язаних із арештом власника Telegram, які можуть вплинути на майбутні тенденції*).

Другим за поширеністю є WhatsApp, який використовують 56,3% злочинців. Більшість експертів зазначають, що масштаби використання цього месенджера збільшились за останні роки. Ризик його використання після війни також високий і становить 41,59%.

Viber також має високу поширеність – 52,3%. Цей месенджер продовжує залишатися популярним, з огляду на те, що значна частка експертів вважає, що масштаби його використання зросли. Ризик використання Viber після війни оцінюється в 40,18%, що робить його одним із основних засобів, на які варто звернути увагу.

Messenger від Facebook також є одним із ключових каналів комунікації між злочинцями та жертвами, з поширеністю 46%. Значна частина експертів відзначають збільшення масштабів його використання, а рівень ризику після війни становить 35,07%.

Серед інших засобів, які також активно використовуються, варто відзначити Signal з поширеністю 39,4% та високим ризиком використання у майбутньому (35,46%). Email залишається традиційним методом комунікації, маючи 34% поширення, але демонструє помірний рівень ризику в майбутньому (32,59%).

Менш поширені способи комунікації, такі як Skype, FaceTime, та веб-чати, мають поширеність від 26,9% до 30,3% і помірний рівень ризику використання у майбутньому (приблизно 30%). Вони також показують змішані тенденції щодо змін у масштабах використання. Наприклад, значна частка експертів вказує на зменшення використання Skype.

Найменш поширеними засобами комунікації, які мають поширеність менше 20%, є платформи на кшталт Voxer, GroupMe, та IM+, які, хоча й використовуються злочинцями, не мають такої ж популярності, як більш відомі месенджери. Рівень ризику їх використання після війни залишається на низькому рівні, що вказує на їхню менш значущу роль у майбутньому.

Отже, спілкування між злочинцями та жертвами в основному відбувається через популярні месенджери, такі як Telegram, WhatsApp, Viber та Messenger, які забезпечують швидкий і зручний зв'язок. Зростання масштабів їх використання свідчить про те, що ці платформи продовжуватимуть залишатися основними каналами для злочинців, особливо в контексті збереження їхньої популярності та функціональних можливостей.

Зменшення використання традиційних платформ, таких як Skype і FaceTime, свідчить про зміну тенденцій у виборі каналів комунікації, де пріоритет віддається більш сучасним і захищеним месенджерам.

4.3.2. Міжсекторальні фактори злочинності: соціальна інженерія, Інтернет речей

Соціальна інженерія – це використання обману, щоб переконати людину мимовільно розкрити конфіденційну інформацію або виконати якусь дію, яку вона, в іншому випадку не вчинила б. Хоча це виглядає доволі просто, в багатьох кіберзлочинах, значною мірою використовується соціальна інженерія. Причина цього проста: ІТ-системи безпеки є об'єктивними, діють за вимірюваними правилами і параметрами, а тому їх важче зламати шляхом безпосередньої технічної атаки. Люди ж є суб'єктивними, і цією суб'єктивністю можна скористатися, щоб обійти ці технічні заходи безпеки, спираючись, натомість, на довірливість жертви та помилки в судженнях.

Соціальна інженерія використовується у багатьох кіберзалежних злочинах, щоб закріпитися в цільовій мережі чи на комп'ютері. Деякі з основних загроз шкідливого програмного забезпечення використовують спам, що завантажується шкідливим програмним забезпеченням разом із іншими методами зараження або виключно як засіб для зараження своїх цілей.

Загальний підхід полягає у прикріпленні до електронного листа шкідливого вкладення, часто це є документ Microsoft Office, що містить у собі шкідливий макрокود. Як альтернативний варіант, повідомлення може містити посилання на шкідливу URL-адресу, яка потім намагатиметься заразити цільовий комп'ютер під час відвідування сайту. Проте згідно з деякими повідомленнями, у майже 60% атак зловмисне програмне забезпечення взагалі не використовується, а натомість зловмисники покладаються лише на скомпрометовані облікові дані та соціальну інженерію.

Подібним чином, соціальна інженерія значною мірою використовується в багатьох кібернезалежних злочинах, наприклад входження в довіру дитині з метою розбещення (грумінг) в мережі Інтернет. У платіжному шахрайстві соціальна інженерія використовується для отримання від жертв справжніх платіжних карток та PIN-кодів. Соціальна інженерія також є ключовим компонентом всіх інших шахрайств в мережі Інтернет, включаючи шахрайство з IT-підтримкою, шахрайство з авансовими платежами та романтичне шахрайство, які все ще є поширеним.

Методи соціальної інженерії залишаються широко поширеними серед кіберзлочинців (табл. 4.39). Найбільш популярним методом є фішинг через електронну пошту, який отримав підтримку від 54% опитаних експертів, що свідчить про його активне використання та значну загрозу для конфіденційної інформації. Вішинг, або телефонне шахрайство, також залишається популярним методом із підтримкою 51,7% експертів, що вказує на його поширеність серед кіберзлочинців. Смішинг, який здійснюється через SMS, має оцінку поширення 43,4%, що підтверджує його значне використання в злочинній діяльності.

Таблиця 4.39

Методи соціальної інженерії, що використовуються злочинцями

СОЦІАЛЬНА ІНЖЕНЕРІЯ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшились	Ризик після війни, %
Фішинг (через електронну пошту)		54,00				42,48
Вішинг (по телефону)		51,70				42,77
Смішинг (через SMS)		43,40				39,50
CEO Fraud		26,00				33,41
Шахрайство з авансовими платежами		42,60				38,09
"Романтична афера"		29,70				33,13
Шахрайство типу "підтримка Microsoft"		28,00				32,62
Вербування грошових мулів		38,30				37,73

Фішинг, смішинг та вішинг – це форми соціальної інженерії, в яких використовуються небажані повідомлення електронною поштою, SMS або телефоном, коли зловмисник представляється третьою стороною, як правило,

намагаючись переконати жертву розкрити конфіденційну інформацію, наприклад, облікові дані або деталі платежу. Зловмисники намагаються отримати облікові дані для будь-яких облікових записів, причому найбільш поширеними їхніми цілями є сфера електронної комерції, банківські та фінансові послуги, соціальні мережі та сервіси грошових переказів тощо.

За даними експертів фішинг, вішинг та смішинг відносно пропорційно використовуються при вчиненні усіх самих поширених кіберзлочинів (табл. 4.40). Водночас, характерним є використання цих методів соціальної інженерії при вчиненні злочинів щодо несанкціонованого втручання в роботу комп'ютерних систем та мереж та шахрайства.

Інші методи соціальної інженерії, такі як шахрайство з авансовими платежами (42,6%), вербування грошових мулів (38,3%), «романтичні афери» (29,7%), шахрайство типу «підтримка Microsoft» (28%), та CEO Fraud (26%), також залишаються актуальними та поширеними, хоча й із меншою частотою в порівнянні з більш популярними методами.

Таблиця 4.40

Злочини, що пов'язані з використанням соціальної інженерії

Види злочинів	361 ККУ	361_1 ККУ	361_2 ККУ	362 ККУ	363 ККУ	176 ККУ	185 ККУ	200 ККУ	ч. 3, 4 ст.190 ККУ
Фішинг (через електронну пошту)									
Вішинг (по телефону)									
Смішинг (через SMS)									

За останні роки масштаби використання методів соціальної інженерії суттєво змінилися. Зокрема, масштаби фішингу через електронну пошту та вішингу по телефону збільшилися. Це вказує на те, що традиційні методи соціальної інженерії залишаються ефективними і продовжують активно використовуватися. Смішинг також показав значне зростання, що може бути пов'язано з поширенням мобільних пристроїв та SMS як зручного каналу для

шахрайства. Інші методи, такі як шахрайство з авансовими платежами (42,6%) та вербування грошових мулів (38,3%), також показали збільшення, що вказує на розширення злочинної діяльності в цих напрямках. Менше зростання було помічено у «романтичних аферах» (29,7%) та шахрайстві типу «підтримка Microsoft» (28%).

Експерти прогнозують, що ризики, пов'язані з використанням соціальної інженерії, залишатимуться високими і в майбутньому. Фішинг має найвищий рівень ризику (42,48%), а вішинг – 42,77%, що свідчить про те, що ці методи продовжуватимуть бути загрозливими для користувачів. Явище фішингу продовжує зростати з року в рік, а фішингові електронні листи продовжують ставати все більш професійними і таким, що викликають довіру. Смішинг також оцінюється як значний ризик (39,5%), враховуючи його поширення. Вербування грошових мулів (37,73%) і шахрайство з авансовими платежами (38,09%) теж вважаються потенційно небезпечними методами, які можуть використовуватися після війни. Інші методи, такі як шахрайство типу «підтримка Microsoft» (32,62%) та «романтичні афери» (33,13%), мають дещо нижчі, але все одно значні рівні ризику.

Таким чином, експертні дані свідчать про те, що соціальна інженерія залишається ключовим інструментом кіберзлочинців. Використання методів, таких як фішинг, вішинг та смішинг, є поширеним і зростає, що вимагає постійного вдосконалення заходів захисту. Незважаючи на певне зменшення уваги до окремих методів, таких як шахрайство типу «підтримка Microsoft», загальна картина свідчить про стабільно високий рівень ризиків, які залишатимуться актуальними і в післявоєнний період. Це вимагає підвищеної уваги з боку організацій та користувачів для захисту від подібних загроз.

Інтернет речей (IoT) стає все більш привабливою ціллю для кіберзлочинців через його швидке зростання та недостатню безпеку багатьох пристроїв. Більшість IoT-пристроїв мають слабкі паролі, відсутність регулярних оновлень безпеки та обмежені можливості захисту, що робить їх вразливими для атак. Зловмисники можуть використовувати ці пристрої для

створення ботнетів, проведення DDoS-атак, шпигунства або отримання несанкціонованого доступу до мереж. Вразливість IoT становить значну загрозу, оскільки зламані пристрої можуть використовуватися для проникнення у критично важливі системи, такі як системи охорони здоров'я, енергетичні мережі та транспортна інфраструктура.

За даними опитування, використання IoT-пристроїв кіберзлочинцями є досить поширеним явищем, хоча ступінь поширеності варіюється залежно від конкретної активності (табл. 4.41). Наприклад, відомості на нетипових смарт-пристроях активно використовуються кіберзлочинцями, про що зазначили 28,6% експертів; шкідливе програмне забезпечення, націлене на IoT-пристрої – 28,0%; використання IoT як проксі-сервісів – 26,6%, що свідчить про популярність цієї практики серед злочинців. Пристрої IoT, що використовуються як частина ботнету, також отримали значну оцінку поширеності – 25,4%. Ці дані підкреслюють важливість IoT як інструменту в сучасній кіберзлочинності, що створює значні ризики для безпеки.

Таблиця 4.41

Злочини, що пов'язані з використанням IoT

ІНТЕРНЕТ РЕЧЕЙ	Оцінка сучасного поширення	%	Масштаби збільшились	Масштаби не змінилися	Масштаби зменшилися	Ризик після війни, %
Відомості на нетипових смарт-пристроях	-	28,60				31,37
Пристрої IoT використовуються як частина ботнету	-	25,40				31,82
Пристрої IoT використовуються як проксі-сервіси	-	26,60				31,38
Шкідливе програмне забезпечення націлене на IoT пристрої	-	28,00				31,10

Експерти відзначили, що масштаби злочинного використання IoT пристроїв за останні роки є переважно стабільними. Водночас висловили помірну стурбованість щодо ризиків, пов'язаних із використанням IoT пристроїв у майбутньому. Рівень ризику оцінюється в межах 31-32%, залежно від конкретного використання. Використання IoT пристроїв як частина ботнету має найвищий рівень ризику (31,82%). Трохи нижчим характеризується рівень ризику використання IoT пристроїв як проксі-сервісів (31,38%) та відомості на нетипових смарт-пристроях (31,37%). Шкідливе ПЗ

націлене на IoT також оцінюються як значний ризик (31,10%). Це свідчить про те, що кіберзлочинці продовжуватимуть використовувати IoT пристрої у своїх злочинних схемах, і зростання ризиків у післявоєнний період є цілком можливим. IoT-пристрої залишатимуться важливим інструментом у руках кіберзлочинців, що потребує посилення заходів безпеки та уваги з боку захисту інформаційної безпеки.

Таким чином, використання IoT пристроїв кіберзлочинцями є поширеною та зростаючою проблемою. Незважаючи на відносно помірні темпи зростання, ризики, пов'язані з використанням IoT у злочинних цілях, залишаються значними. Це вимагає постійного вдосконалення захисту IoT-пристроїв та контролю за такими пристроями, посилення й впровадження нових заходів безпеки, а також підвищення обізнаності серед користувачів про потенційні загрози.

Для здійснення цілеспрямованих атак з використанням соціальної інженерії зловмисникам часто потрібно виконувати збирання певних даних і проводити певні дослідження, щоб отримати інформацію, наприклад, про структуру компанії, дані постачальника та адреси електронної пошти працівників. Зростаюча кількість даних про стиль життя, дії та звички, що формуються Інтернетом речей, уможливають ідентифікацію особи за унікальними особливостями її стилю життя. Це створює нові можливості для збору даних, які можуть використовуватися для фішингу.

Водночас, злочинці часто вдаються до «старих» методів, оскільки вони виявляються ефективними, тоді як галузь і правоохоронні органи зосереджують свою увагу на боротьбі з сучасними популярними або новими тактиками. Зі зростанням числа випадків, пов'язаних із зараженням IoT-пристроїв шкідливим програмним забезпеченням, ймовірно, ми можемо побачити зростання кількості подальших атак такого характеру, в яких використовуватимуться бот-мережі Інтернету речей.

Висновки до розділу 4

Аналіз сучасних методологічних засад виявлення та аналізу кіберзлочинності дозволяє стверджувати, що трансформація злочинної діяльності у цифровому просторі вимагає радикального перегляду традиційних підходів до кримінологічного моніторингу. Встановлено, що ключовою проблемою залишається термінологічна невизначеність, оскільки поняття «кіберзлочинність» охоплює як специфічні атаки на комп'ютерні дані, так і традиційні злочини, вчинені за допомогою мережевих технологій. Сучасна методологія повинна базуватися на комплексному поєднанні технічного аналізу (цифрова криміналістика) та соціально-поведінкових досліджень. Важливим аспектом є визнання того, що цифрові докази є надзвичайно волатильними, що потребує впровадження інструментів динамічного аналізу в режимі реального часу. Доведено, що ефективна протидія неможлива без врахування транскордонного характеру правопорушень, де зловмисники використовують юрисдикційні розриви для уникнення відповідальності. Методологічний апарат має включати моделі предиктивного аналізу, які дозволяють ідентифікувати аномальну активність ще до моменту настання тяжких наслідків. Це передбачає глибоку інтеграцію алгоритмів машинного навчання та великих даних у процес документування злочинів. Окрему увагу приділено необхідності гармонізації методик збору доказів із міжнародними стандартами, зокрема Будапештською конвенцією, що є критичним для успішної міжнародної співпраці. Таким чином, методологічне оновлення стає фундаментом для побудови дієвої системи стратегічного прогнозування загрозового ландшафту, де першочерговим завданням є перехід від реактивної фіксації подій до проактивного виявлення латентних загроз та ідентифікації складних злочинних схем.

Дослідження пріоритетних напрямів стратегічного забезпечення протидії кіберзлочинності вказує на зміщення акцентів у бік захисту критичної інфраструктури та приватних даних в умовах масового впровадження

Інтернету речей (IoT). Виявлено, що стрімке зростання кількості підключених пристроїв створює безпрецедентну за масштабами поверхню атаки, де слабка захищеність побутових пристроїв стає інструментом для проведення масштабних DDoS-атак або проникнення в корпоративні мережі. Пріоритетним вектором стратегії має стати впровадження обов'язкових стандартів безпеки для виробників обладнання, що дозволить мінімізувати ризики на етапі проектування систем. Аналіз показує, що кіберзлочинці все частіше поєднують технічні вразливості з методами соціальної інженерії, що робить людський фактор найбільш критичною ланкою в системі захисту. Стратегічне планування повинно враховувати адаптивність злочинних угруповань, які швидко опановують новітні технології (штучний інтелект, дипфейки) для автоматизації фішингу та створення шкідливого ПЗ. У цьому контексті важливою є розбудова національної системи кібергігієни та підвищення обізнаності громадян, оскільки індивідуальна вразливість трансформується у колективний ризик для всієї держави. Ефективна стратегія має базуватися на принципах державно-приватного партнерства, де обмін інформацією про загрози між спецслужбами та технологічними компаніями відбувається в автоматизованому режимі. Тільки через посилення інституційної спроможності правоохоронних органів у поєднанні з жорстким контролем за обігом криптовалют та інших засобів анонімізації доходів можна досягти суттєвого зниження економічної привабливості кіберзлочинності.

Завершальним етапом аналізу є оцінка ефективності міжнародної співпраці та правових механізмів, що визначають спроможність держави протистояти гібридним загрозам у кіберпросторі. Встановлено, що класичні методи міжнародної правової допомоги є занадто повільними для цифрової епохи, що вимагає розробки нових протоколів прямої взаємодії між провайдерами та органами розслідування на міжнародному рівні. Доведено, що боротьба з кіберзлочинністю безпосередньо корелює з рівнем загальної кіберстійкості країни: що вища здатність систем до самовідновлення, то менш ефективними стають атаки зловмисників. Удосконалення законодавства має

йти шляхом криміналізації нових видів суспільно небезпечних діянь, пов'язаних із використанням штучного інтелекту в злочинних цілях. Важливим висновком є необхідність створення спеціалізованих міждисциплінарних підрозділів, які поєднують компетенції юристів, аналітиків даних та технічних фахівців. Стратегічний успіх залежить від здатності держави забезпечити безперервний цикл навчання та утримання кадрів у державному секторі. Окрім того, особливого значення набуває розвиток «етичного хакінгу» та підтримка наукових розробок у сфері кібербезпеки, що дозволяє випереджати злочинні інновації. Логіка розвитку протидії кіберзлочинності вимагає переходу до моделі «стійкого правопорядку», де юридичні норми є гнучкими та адаптивними до технологічних змін, а правоохоронна діяльність інтегрована в загальну архітектуру національної безпеки. Тільки такий інтегрований підхід дозволить Україні не лише ефективно розслідувати скоєні злочини, а й формувати безпечне цифрове середовище, здатне витримувати цілеспрямований тиск з боку як організованої злочинності, так і ворожих державних акторів.

ВИСНОВКИ

За результатами дослідження вирішено наукову проблему щодо розбудови національної системи кіберстійкості в Україні та зроблено такі висновки:

1. Дослідження генезису концепції «стійкості» підтверджує її міждисциплінарну природу та визначає еволюційний перехід від статичних інженерних моделей (повернення до вихідного стану) до динамічних екологічних та адаптивних систем (здатність до трансформації).

Теоретичним підґрунтям сучасної кіберстійкості визначено зміну парадигми: від спроб побудови «непроникного захисту» до створення емерджентних властивостей системи, що забезпечують її функціонування в умовах неминучих інцидентів. Ключовим результатом еволюції є перехід до «динамічної адаптивності» та принципу «граціозної деградації», де стійкість розглядається не як стабільний стан, а як безперервний процес навчання, самоорганізації та підтримки критичних функцій під час складних кібератак. Таким чином, кіберстійкість обґрунтовано як якісно новий етап системної інженерії, що базується на управлінні ризиками в умовах високої невизначеності.

2. Розмежування понять дозволило встановити їхню комплементарну природу: якщо «кібербезпека» зосереджена на мінімізації ймовірності реалізації загрози, то «кіберстійкість» визнає неминучість компрометації та фокусується на підтримці життєздатності системи й мінімізації наслідків інцидентів.

В основі цієї нової парадигми лежить інтегрована чотирьохкомпонентна модель, яка включає спроможності передбачати загрози через проактивний аналіз, витримувати деструктивні впливи без втрати критичних функцій, оперативно відновлюватися до стабільного стану та адаптуватися шляхом трансформації архітектури на основі отриманого досвіду. Функціональний взаємозв'язок цих компонентів формує безперервний цикл самоорганізації, де

фаза адаптації стає підґрунтям для нового етапу передбачення. Ключовим елементом цієї парадигми є зміщення акценту з «непроникності» на життєздатність системи, де через механізми адаптивної диверсифікації, сегментації та обманних технологій досягається критичне підвищення «вартості атаки» для зловмисника. Таким чином, кіберстійкість визначено як стратегічну характеристику, що забезпечує виконання критичних функцій навіть за умов часткового успіху атаки, перетворюючи досвід інцидентів на оновлені механізми самоорганізації та захисту.

3. Аналіз світового досвіду свідчить про глобальну трансформацію парадигми захисту: від пасивної «кібербезпеки» до активної «кіберстійкості», що базується на визнанні неминучості інцидентів та здатності системи зберігати життєздатність під час атак.

Дослідження підтверджує, що успішні національні моделі розбудови кіберстійкості базуються на трьох фундаментальних принципах, які утворюють цілісну систему захисту. Першим складником є нормативна обов'язковість, що на прикладі досвіду ЄС демонструє перехід від добровільних рекомендацій до жорсткого регулювання відповідальності виробників цифрових продуктів та безпеки ланцюгів постачання. Другим принципом виступає технологічна адаптивність, реалізована в моделі США через впровадження інженерних стандартів NIST та архітектури «нульової довіри», які забезпечують швидке відновлення їхніх критичних функцій. Третім ключовим елементом є соціотехнічна синергія, притаманна досвіду Великої Британії, що передбачає розбудову «колективної стійкості» через розвинене публічно-приватне партнерство та активне залучення людського капіталу на всіх рівнях – від загальнодержавного до регіонального.

Для України пріоритетним визначено шлях творчого синтезу: адаптація європейського права для сертифікації продуктів, імплементація американських технічних стандартів для захисту промислових систем та впровадження британських моделей регіональної стійкості. Такий інтегрований підхід дозволить Україні трансформувати досвід відсічі збройній

агресії у стійку цифрову екосистему, здатну не лише витримувати сучасні кібершоки, а й виступати гарантом безпеки в європейському цифровому просторі.

4. Доведено, що інституціоналізація кіберстійкості є не лінійним впровадженням окремих технічних або організаційних заходів, а системним процесом інтеграції різномірних інструментів управління кіберризиками, а також є процесом переходу від статичного захисту до динамічної моделі адаптації та відновлення систем. Обґрунтовано, що домінуючі міжнародні підходи (зокрема стандарти та галузеві практики) мають обмеження, пов'язані з відсутністю пріоритезації заходів і надмірною технократичністю, що знижує їх адаптивність до кризових умов. Доведено, що найбільш ефективною є модель, яка поєднує нормативний вплив держави, економічні стимули ринку та методологічну підтримку стандартів, забезпечуючи баланс між примусом і саморегуляцією.

Встановлено, що ключовим елементом сучасної інституціоналізації є імплементація стандартів Директиви NIS2, яка впроваджує жорстку відповідальність керівництва та обов'язковість звітування про інциденти. Це дозволяє трансформувати кіберстійкість із вузькотехнічного завдання на стратегічний компонент державного управління. Такий підхід створює умови для формування «культури стійкості», де кожен суб'єкт господарювання стає активним учасником системи національної безпеки, що підвищує загальну адаптивність критичної інфраструктури до гібридних загроз.

5. Дослідження суб'єктного складу підтвердило формування в Україні багаторівневої ієрархічної системи, де НКЦК при РНБО виконує роль стратегічного координатора та методологічного хабу. Встановлено чіткий розподіл функцій: Адміністрація Держспецзв'язку реалізує регуляторні завдання, НКЦК забезпечує стандартизацію, а Мінцифра стимулює ринкові механізми розвитку галузі. Особливу увагу приділено міжнародній суб'єктності України, яка в умовах повномасштабної війни трансформувалася з реципієнта технологій на ключового донора практичного досвіду. Участь у

CCDCOE НАТО та мережі CSIRT легітимізує українські протоколи відсічі агресії як основу для майбутніх міжнародних стандартів колективної стійкості. Зроблено висновок, що сучасна архітектура суб'єктів забезпечує інституційну цілісність системи, дозволяючи ефективно поєднувати національні оборонні спроможності з міжнародними механізмами взаємодії у кіберпросторі.

6. У ході дослідження доведено, що цивільно-військове співробітництво є фундаментом національної кіберстійкості, що трансформує класичну модель CIMIC у гнучку мережеву екосистему. Виявлено термінологічну прогалину в українському правовому полі, де фактична взаємодія суб'єктів у кіберпросторі випереджає її законодавче закріплення. Сформовано авторське визначення дефініції «Cyber-CIMIC» та розроблено стратегічні правки до Закону України «Про основні засади забезпечення кібербезпеки України». Запропоновані зміни дозволяють інституціоналізувати роль НКЦК як стратегічного хабу, легалізувати статус волонтерських ІТ-спільнот та впровадити економічні стимули, такі як «регуляторні пісочниці», для приватних операторів критичної інфраструктури. Ефективність моделі «Cyber-CIMIC» забезпечується синергією між військовою спроможністю, державним регулюванням та інноваційним потенціалом приватного сектору. Реалізація цих підходів забезпечить перехід від ситуативної координації до системної інтеграції ресурсів, що підвищить адаптивність держави до гібридних загроз, дозволить трансформувати практичний досвід у глобальні стандарти безпеки нового покоління та забезпечить сумісність із євроатлантичними стандартами безпеки.

7. Сучасне методологічне забезпечення кіберстійкості України ґрунтується на синергії OSINT, форсайту та ризик-орієнтованого підходу, що дозволяє трансформувати систему захисту з реактивної у проактивну та адаптивну. Використання OSINT виступає фундаментом інформаційної актуальності, забезпечуючи аналітичну розвідку верифікованими даними з відкритих джерел для миттєвого реагування на поточні загрози та розуміння

тактик супротивника. Впровадження методів форсайту розширює горизонт планування, дозволяючи через сценарне моделювання та аналіз «слабких сигналів» конструювати альтернативні варіанти майбутнього та випереджати технологічні виклики. Ключовим інтегратором цієї системи стає ризик-орієнтований підхід (згідно зі стандартом ISO 31000), який на основі математико-статистичного аналізу експертних оцінок забезпечує об'єктивну пріоритезацію ресурсів та мінімізацію потенційних наслідків. Таким чином, поєднання фактологічної точності розвідки, стратегічного прогнозування та прагматичного управління ризиками формує цілісну модель інтелектуальної стійкості держави, здатну до еволюційного самовідновлення в умовах постійної гібридної агресії.

8. На основі проведеного ризик-орієнтованого аналізу та верифікації експертних оцінок, стратегія кіберстійкості України має трансформуватися з моделі фрагментарного технічного захисту в цілісну систему національної відмовостійкості. Ключовим стратегічним пріоритетом визначено гібридизацію та ешелонований захист критичної інфраструктури, що передбачає впровадження моделі «системної різноманітності», де цифровізація енергетичного та оборонного комплексів обов'язково поєднується з модернізацією аналогових систем як останньої лінії оборони від кібертерористичних атак.

Паралельно з цим, стратегія фокусується на впровадженні інтелектуального моніторингу та предиктивної аналітики, де використання технологій штучного інтелекту та аналізу великих даних дозволяє перейти від реактивного реагування на інциденти до завчасного виявлення «слабких сигналів» кібершпигунства. Важливою складовою цієї моделі є протидія когнітивним загрозам та деструктивним ІПСО, оскільки високий ризик використання кібератак для дискредитації влади та розколу суспільства вимагає створення єдиної екосистеми контрпропаганди та захисту інформаційного простору Сил оборони України.

9. Розроблено та практично застосовано матрицю показників кіберстійкості, яка дозволила кількісно оцінити стан вітчизняної кіберінфраструктури. Діагностика виявила формування «техноцентричної моделі стійкості», де технічні та інформаційні домени (середній показник ~55%) випереджають управлінські та соціальні механізми (51–52%). Встановлено, що найбільш критичною ланкою є етап планування в соціальному домені (51,75%), що вказує на дефіцит міжвідомчої координації. Водночас найвищу ефективність система демонструє на стадії відновлення інформаційного домену (55,14%) та в процесах адаптації, що підтверджує здатність національної інфраструктури ефективно навчатися на реальних інцидентах і трансформувати досвід атак у стратегічний актив.

10. Доведено концептуальну перевагу моделі «нارощування спроможностей» над пасивною моделлю «фіксації вразливостей». Емпіричний аналіз зафіксував диспропорцію між високим рівнем захищеності центральних вузлів інформаційної інфраструктури (спроможність > 59%) та низькою витривалістю регіональних систем і приватного сектору (ризик на місцевому та індивідуальному рівнях < 50%), що свідчить про глибокий безпековий розрив. Виявлено «страх інновацій» у регуляторних органах (низька мотивація до нетрадиційного оповіщення - 34–46%) та критичний стан наукового забезпечення (ризик < 46%). Обґрунтовано пакет правових реформ, що включає дефініцію «кіберстійкості» у базовому законі, створення регіональних центрів стійкості при ОВА, декриміналізацію етичного хакінгу та запровадження Державного фонду кіберінновацій для реанімації наукового циклу.

Розроблено та представлено авторську концепцію «стійкість через право», яка передбачає перехід від декларативного регулювання до юридичної фіксації чотирьох функціональних спроможностей суб'єктів: *передбачення, витримування, відновлення та адаптація*. Запропоновано конкретні кроки щодо гармонізації українського законодавства із Директивою ЄС NIS2,

зокрема в частині легалізації адаптивного управління ризиками та залучення спільноти етичних дослідників до зміцнення критичної інфраструктури.

11. Аналіз сучасних методологічних засад виявлення та аналізу кіберзлочинності дозволяє стверджувати, що трансформація злочинної діяльності у цифровому просторі вимагає радикального перегляду традиційних підходів до кримінологічного моніторингу. Сучасна методологія повинна базуватися на комплексному поєднанні технічного аналізу (цифрова криміналістика) та соціально-поведінкових досліджень та забезпечувати перехід від пасивної фіксації кіберзлочинів до динамічного управління ризиками.

Важливим аспектом є визнання того, що цифрові докази є надзвичайно волатильними, що потребує впровадження інструментів динамічного аналізу в режимі реального часу. Методологічний апарат має включати моделі предиктивного аналізу, які дозволяють ідентифікувати аномальну активність ще до моменту настання тяжких наслідків. Таким чином, методологічне оновлення стає фундаментом для побудови дієвої системи стратегічного прогнозування ландшафту загроз, де першочерговим завданням є перехід від реактивної фіксації подій до проактивного виявлення латентних загроз та ідентифікації складних злочинних схем.

Застосування багаторівневої системи фільтрації експертних даних дозволило шляхом відсіювання логічних помилок підвищити якість вибірки та виявити реальні статистичні розбіжності у сприйнятті загроз (наприклад, щодо активності в Darknet та відмивання коштів). Доведено, що використання методів Data Mining, аналізу соціальних мереж та регресійного моделювання в поєднанні з експертною думкою забезпечує репрезентативність аналізу навіть в умовах високої анонімності та транскордонності кіберзлочинного середовища.

12. У ході дослідження ідентифіковано on-line шахрайство як найбільш масовий вид кіберзлочину (36% від загальної сукупності), причому 84% таких діянь кваліфікуються за частинами 3 та 4 ст. 190 ККУ. Виявлено домінування

операційної системи Kali Linux (41% при втручаннях у системи) та програмного забезпечення для Brute-force і DoS-атак. Встановлено критично високий рівень організованості злочинності: понад 70% випадків розповсюдження дитячої порнографії та 50% несанкціонованих втручань вчиняються у складі ОЗУ. Аналіз підтвердив кореляцію між досвідом експертів та оцінкою ризиків, а також зафіксував значну частку злочинів (до 17%), що мають ознаки співпраці з агресором у межах гібридної війни.

Логіка розвитку протидії кіберзлочинності вимагає переходу до моделі «стійкого правопорядку», де юридичні норми є гнучкими та адаптивними до технологічних змін, а правоохоронна діяльність інтегрована в загальну архітектуру національної безпеки. Тільки такий інтегрований підхід дозволить Україні не лише ефективно розслідувати злочини, а й формувати безпечне цифрове середовище, здатне витримувати цілеспрямований тиск з боку як організованої злочинності, так і ворожих державних акторів.

13. Встановлено, що фінансова мотивація є ключовим драйвером кіберзлочинності (50-60%), де домінують шахрайства з платежами (67,1%). Виявлено стійку ієрархію криптоінструментів, де Bitcoin залишається лідером для розрахунків (54,9%) та вимагання викупу, тоді як Monero та Zcash набирають популярності через підвищену анонімність. Доведено, що грошові мули (дропи) є критичною ланкою у процесі переведення активів у фіат (60,9%). Аналіз активності в Darknet підтвердив високу затребуваність криптопрограм (44,3%) та банківських даних (50%), а вивчення каналів комунікації показало домінування Telegram (66%) у взаємодії «злочинець-жертва» та форумів Deep Web (46%) у розрахунках між зловмисниками. Аналіз показує, що кіберзлочинці все частіше поєднують технічні вразливості з методами соціальної інженерії, що робить людський фактор найбільш критичною ланкою в системі захисту.

Подальше стратегічне планування повинно враховувати адаптивність злочинних угруповань, які швидко опановують новітні технології (штучний інтелект, дипфейки) для автоматизації фішингу та створення шкідливого ПЗ.

У цьому контексті важливою є розбудова національної системи кібергігієни та підвищення обізнаності громадян, оскільки індивідуальна вразливість трансформується у колективний ризик для всієї держави. Водночас, через посилення інституційної спроможності правоохоронних органів у поєднанні з жорстким контролем за обігом криптовалют та інших засобів анонімізації доходів можна досягти суттєвого зниження економічної привабливості кіберзлочинності.

14. Проведено критичний огляд законодавчого поля України, за результатами якого сформовано пропозиції щодо удосконалення нормативно-правового регулювання із врахуванням сучасних глобальних викликів та, пов'язаних із воєнною агресією та кібервійною проти України, а також спрямованих на гармонізацію вітчизняних стандартів із Директивою ЄС про мережеву та інформаційну безпеку (NIS2), зокрема:

1) до Закону України «Про основні засади забезпечення кібербезпеки України»:

додати статтю 1 пунктом такого змісту: *«цивільно-військове співробітництво у сфері кібербезпеки (Cyber-CIMIC) – система заходів з організації взаємодії між суб'єктами сектору безпеки і оборони, державними органами, приватним сектором та громадянським суспільством задля підвищення національної кіберстійкості, захисту критичної інформаційної інфраструктури та спільної відсічі кіберагресії»;*

частину другу статті 5 доповнити словами: *«...здійснює координацію цивільно-військового співробітництва у сфері кібербезпеки на стратегічному рівні, забезпечуючи інтеграцію спроможностей волонтерських кіберспільнот та приватних технологічних компаній до загальної системи спротиву;...»;*

доповнити статтю 8:

частиною восьмою: *«Суб'єкти приватного сектору, що залучаються до заходів цивільно-військового співробітництва, отримують право на використання спеціальних правових режимів («регуляторних пісочниць») за умови забезпечення автоматизованого обміну даними про кіберінциденти з*

державними центрами реагування (CERT-UA) та дотримання стандартів сумісності НАТО»;

а також частиною девятою: *«Запровадити інститут добровільного кіберрезерву як форми реалізації цивільно-військового співробітництва, що передбачає залучення цивільних фахівців на договірній основі до виконання завдань з кібероборони без обов'язкового набуття статусу військовослужбовця, із визначенням меж їхньої юридичної відповідальності та соціального захисту»;*

2) внести зміни до Закону України «Про захист прав споживачів»: закріпити «Права на кіберзахист» як базового цифрового права та запровадити концепцію «мінімального гарантованого рівня цифрової безпеки» для забезпечення обов'язкової відповідності цифрових продуктів і послуг стандартам кіберстійкості;

3) внести зміни до КПК України та законів про ОРД, контррозвідальну та розвідальну діяльність, які б дозволили залучати наукові установи як офіційних експертних контрб'юторів до аналізу складних кіберінцидентів;

4) прийняти Закон України «Про стимулювання інновацій у сфері кібербезпеки та кіберстійкості». Юридичний механізм має передбачати створення Державного фонду кіберінновацій, наповнення якого здійснюватиметься шляхом фіксованих відрахувань від ліцензійних зборів у сфері телекомунікацій та штрафів за порушення законодавства про захист персональних даних. Крім того, доцільним є законодавче закріплення частки (не менше 1%) бюджетних призначень сектору безпеки та оборони на проведення НДДКР (науково-дослідних та дослідно-конструкторських робіт) виключно за напрямом кіберстійкості. Це дозволить перетворити фінансування з «залишкового» на «пріоритетне».

4) розробити та затвердити на рівні Кабінету Міністрів України

Типове положення про цифрову безпеку територіальної громади, яке б визначало обов'язковий перелік заходів із захисту реєстрів та комунальних сервісів;

Порядок функціонування національних наукових кібер-полігонів, що забезпечить науковцям правовий доступ до знеособлених масивів даних про реальні атаки для розробки прогнозних моделей, що є відповіддю на потребу в когнітивній адаптації;

правовий інститут «муніципального офіцера з кібербезпеки» або делегування цих функцій спеціалізованим сервісним центрам на умовах аутсорсингу, що дозволить вирішити проблему кадрового дефіциту в регіонах;

механізм «субвенцій на кіберстійкість» – цільового фінансування з державного бюджету для технічного переоснащення найбільш вразливих громад;

механізм «Кібер-ваучерів» – державної субсидії для малих підприємств на отримання базових консультацій або аудитів від акредитованих приватних компаній;

внести зміни до освітніх стандартів та трудового законодавства щодо обов'язкового періодичного тестування працівників державного сектору та критичної інфраструктури закріпити, статус «цифрової грамотності» як компонента цивільного захисту;

юридичного статусу «міждисциплінарних освітньо-наукових центрів кіберстійкості» (Cyber Resilience Hubs) на базі провідних ЗВО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Американський адмірал підтвердив, що Росія веде кібервійну проти України. URL: <https://web.archive.org/web/20160429082331/http://ain.ua/2014/03/17/515999>
2. Аніщук В.В., Зицик С.Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 3 (83). С. 19–23. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf>
3. Безверхнюк Т.М. Система ресурсного забезпечення регіонального управління: концептуальні засади розбудови і механізми функціонування: дис. ... д-ра наук з держ. упр.: 25.00.02. Одеса, 2009. 441 с.
4. Бекетова Г.С., Ахметов Б.Б., Корченко О.Г., Лахно В.А. Design of a model for intellectual detection of cyber-attacks, based on the logical procedures and the coverage matrices of features. *Ukrainian Scientific Journal of Information Security*. 2016. Vol. 22 (3). P. 242–254. DOI: <https://doi.org/10.18372/2225-5036.22.11096>
5. Бірюков Д.С. Поняття «стійкість» в сучасних безпекових дослідженнях. *Вісник Дніпропетровського університету*. 2015. № 5. С. 220–237.
6. Богдан Б. Нормативно-правові засади захисту критичної інформаційної інфраструктури. *Пропілеї права та безпеки*. 2025. Вип. 6-7. С. 35-37.
7. Брежнєва Т.В. Сстійкість як ключовий елемент колективної оборони НАТО. *Стратегічні пріоритети*. 2017. № 3 (44). С. 12-20.
8. Бурдяк П. Людський фактор в кібербезпеці: кіберосвіта як системна відповідь на зростаючі загрози в цифровому просторі України та ЄС. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2025. Вип. 17. С. 328-346. DOI: <https://doi.org/10.31861/mediaforum.2025.17.328-346>

9. Василенко В.М. Національна кібербезпека в контексті цифровізації суспільства: роль поліції у захисті критичної інфраструктури. *Вісник Харківського національного університету внутрішніх справ*. 2025. Том. 109 (2). С. 392–405. DOI: 10.32631/v.2025.2.33
10. Вербовський І., Шелуха О. Управління кіберризиками в освітньому середовищі. *Економіка. Управління. Інновації*. 2025. № 2(37). DOI: [https://doi.org/10.35433/ISSN2410-3748-2025-2\(37\)-19](https://doi.org/10.35433/ISSN2410-3748-2025-2(37)-19)
11. Верещак О.О. Військово-цивільне співробітництво та національна стійкість: досвід НАТО. *Дніпровський науковий часопис публічного управління, психології, права*. 2023. № 2. С.152-157. DOI: <https://doi.org/10.51547/ppp.dp.ua/2023.2.26>
12. Веселова Л.Ю. Кібернетична безпека в умовах гібридної війни: адміністративно-правові засади: монографія. Одеса: Видавничий дім «Гельветика». 2020. 488 с.
13. Вівчар І., Постельжук О., Валюх Л. Кібербезпека як сфера міжнародного співробітництва у період глобальної кризи безпеки. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2025. Вип. 2(65). С. 122-143. DOI:10.21564/2663-5704.65.331787
14. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. 2019. № 1(28). С. 108–117. DOI:10.37750/2616-6798.2019.1(28).273351.
15. Галушко О., Селівьорстова Т. Кібербезпека в управлінні ланцюгами постачань (SCM). *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2022. Вип. 2. С. 537–542. DOI:10.31733/2078-3566-2022-6-537-542
16. Гарасимчук О., Партика А., Нємкова О., Совин Я. Інтегрований підхід до забезпечення кібербезпеки та дослідження кібезлочинів критичної інфраструктури за допомогою системи моніторингу інцидентів вірусів-вимагачів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука,*

техніка». 2023. Вип. 1(21). С. 286–296. DOI: <https://doi.org/10.28925/2663-4023.2023.21.286296>

17. Гнатюк С., Бердибаєв Р., Сидоренко В., Жигаревис О., Смірнова Т. Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. Вип. 3(19). С. 176–196. DOI:10.28925/2663-4023.2023.19.176196

18. Гонтар О. Динамічна оцінка ризиків інформаційної безпеки для підприємств критичної інфраструктури України. *Наука і техніка сьогодні*. 2025. № 13(54). С. 1974-1992.

19. Горліченко С.О. Методи управління ризиками інформаційної безпеки: Стандарт ISO/IEC 27001 ТА CIS CRITICAL SECURITY CONTROLS. *Безпека інформації*. 2024. Вип. 30(1). С.190–196. DOI:10.18372/2225-5036.30.18620.

20. Гречанінов В. Моделі та технології інтелектуального захисту інформаційних систем критичної інфраструктури для підвищення стійкості. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2025. Вип. 1(29). С. 877–896. DOI: <https://doi.org/10.28925/2663-4023.2025.29.948>

21. Гулак В.М., Бурячок В.Л., Складанний П.М., Кузьменко Л.В. Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка*. 2020. Вип. 2(10). С. 6–28. DOI:10.28925/2663-4023.2020.10.628

22. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. *Правові новели*. 2025. № 26. 157-166. DOI: <https://doi.org/10.32782/ln.2025.26.189>

23. Демедюк С.В. OSINT в контексті виявлення та запобігання кіберзлочинам. *Південноукраїнський правничий часопис*. 2024. № 4.С. 38-41. DOI: <https://doi.org/10.32850/sulj.2024.4.7>

24. Демедюк С.В. OSINT в контексті кібербезпеки. *Юридичний бюлетень*. № 34. 2024. С.200-207.
25. Демедюк С.В. Захист критично важливих послуг у цифрову епоху. *Наука і правоохорона*. 2023. № 3(61). С.26-34.
26. Демедюк С.В. Зміст та особливості експертної вибірки в оцінюванні кіберризиків. *Морська безпека та оборона*. 2025. №1. С.17-24. DOI: <https://doi.org/10.32782/msd/2025.1/03>
27. Демедюк С.В. Інституціоналізація кіберстійкості. *Наука і правоохорона*. 2023. № 4(62). С.31-41.
28. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. *Наука і правоохорона*. 2024. № 1(63). С.133-141.
29. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона*. 2023. № 2(60). С.78-85.
30. Демедюк С.В. Розділ 1. Стратегічний ландшафт застосування OSINT в секторі національної безпеки. *OSINT Open Source Intelligence. Теорія та методологія*: монографія / Користін О., Демедюк С., Барановський О., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. С. 21-36.
31. Демедюк С.В. Розділ 26. Кібервійна та форсайт кіберстійкості. *Реалізація філософії ІЛР в системі кримінального аналізу Національної поліції України*: монографія / О.Є. Користін, Б.А. Денисенко, С.В. Демедюк та ін. ; за заг. ред. д-ра юрид. наук, проф. О.Є. Користіна. Київ: ВАЙТЕ, 2024. С. 343-357. DOI: <https://doi.org/10.36486/978-966-2310-66-5-26>
32. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона*. 2023. № 1(59). С.77-85.
33. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154. DOI: [https://doi.org/10.36486/np.2024.3\(65\).12](https://doi.org/10.36486/np.2024.3(65).12)

34. Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ. URL: https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D0%BF%D0%B0%D1%80%D1%82%D0%B0%D0%BC%D0%B5%D0%BD%D1%82_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D1%80%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D1%83%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%B5%D1%81%D1%96%D0%B2_%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B8_%D1%83_%D1%81%D1%84%D0%B5%D1%80%D1%96_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D0%A1%D0%91%D0%A3

35. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналітична доповідь / за заг. ред. Д. Дубова. Київ: НІСД, 2018.84 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberbezpeka.pdf?utm_source=chatgpt.com

36. Держспецзв'язку затвердила каталог заходів, базові заходи, форму плану та методичні рекомендації з кіберзахисту. URL: <https://cip.gov.ua/ua/news/derzhspeczv-yazku-zatverdila-katalog-zakhodiv-bazovi-zakhodi-formu-planu-ta-metodichni-rekomendaciyi-z-kiberzakhistu>

37. Держспецзв'язку затвердила методичні рекомендації щодо ролі та вимог до CISO та підрозділів з кіберзахисту. URL: <https://cip.gov.ua/ua/news/derzhspeczv-yazku-zatverdila-metodichni-rekomendaciyi-shodo-rol-i-ta-vimog-do-ciso-ta-pidrozdiliv-z-kiberzakhistu#:~:text=%D0%9F%D1%80%D0%B8%20%D1%86%D1%8C%D0%BE%D0%BC%D1%83%20%D0%BE%D0%BA%D1%80%D0%B5%D0%BC%D0%BE%20%D0%BD%D0%B0%D0%B3%D0%BE%D0%BB%D0%BE%D1%88%D1%83%D1%94%D1%82%D1%8C%D1%81%D1%8F%20%D0%BD%D>

0%B0,%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83%20%D0%B2%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B0%D1%85%20%D0%B4%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%BE%D1%97%20%D0%B2%D0%BB%D0%B0%D0%B4%D0%B8

38. Держспецзв'язку попередило про спроби Росії масштабувати кібератаки проти України. URL: https://lb.ua/society/2025/04/09/670239_derzhspetszvyazku_poperedilo_pro.html?utm_source=chatgpt.com

39. Деркаченко Я.А., Дзюба Т.М. Забезпечення кіберстійкості України за сучасних умов: цифрові навички та компетентності. *Зв'язок*. 2021. Вип. 3 С.12-16. DOI: 10.31673/2412-9070.2021.031216

40. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.2020 № 1295. URL: <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text>

41. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 1106. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text>

42. Деякі питання реалізації інструменту Ukraine Facility: Постанова Кабінету Міністрів України від 15 листопада 2024 р. № 1318. URL: <https://zakon.rada.gov.ua/laws/show/1318-2024-%D0%BF#Text>

43. Джалладова І.А.-К., Камінський О.Є. Соціально-психологічна стійкість систем кібербезпеки. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2025. Вип. 53(2). С. 43–50. DOI: 10.33099/2311-7249/2025-53-2-43-50.

44. 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. URL:

https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA

45. Дія підтвердила безпечність застосунку за допомогою програми багбаунті. URL: https://diia.gov.ua/news/diya-projshla-perevirku-bagbaunti-ta-pidtverdila-bezpechnist-zastosunku?utm_source=chatgpt.com

46. Доктрина «Цивільно-військове співробітництво». URL: <https://sprotyvg7.com.ua/wp-content/uploads/2022/03/%D0%A1%D0%9F-9-0001.01-%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0-%D1%86%D0%B8%D0%B2%D1%96%D0%BB%D1%8C%D0%BD%D0%BE-%D0%B2%D1%96%D0%B8%CC%86%D1%81%D1%8C%D0%BA%D0%BE%D0%B2%D0%B5-%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%82%D0%BD%D0%B8%D1%86%D1%82%D0%B2%D0%BE.pdf>

47. Дослідження IP офісу щодо контрафакту в Україні. URL: <https://nipo.gov.ua/opytuvannia-kontrafaktni-tovary/>

48. ДСТУ ISO 31000: 2018 Менеджмент ризиків. Принципи та настанови (ISO 31000: 2018, IDT). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf

49. Ємельянов В., Бондар Г. Кібербезпека як компонент національної безпеки та кіберзахисту критичної інфраструктури України. *Державне управління та регіональний розвиток*. 2019. Вип. 5. С. 493–523. DOI: 10.34132/pard2019.05.02

50. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. URL: <https://infocenter.rada.gov.ua/uploads/documents/28982.pdf>

51. Зубко Г.Ю. Розвиток інституційної спроможності держави у сфері безпеки та стійкості життєво важливої інфраструктури. *Прикарпатський юридичний вісник*. 2019. Вип. 2 (27). Том 2. С. 9–14.

52. Іванченко Є., Корченко О., Зарицький О., Зибін С., Вишневська Н. Аналіз поняття кіберстійкості критичної інфраструктури. *Захист інформації*. 2023. ТОМ 25. № 4. С.221-233.

53. Івкова В.С., Опірський І.Р. Дослідження існуючих засобів та підходів до проведення osint в контексті інформаційної безпеки особи та держави. *Комп'ютерні системи та мережі*. 2025. Вип. 7 (1). С. 143–159. DOI: <https://doi.org/10.23939/csn2025.01.143>

54. Ільєнко А., Телющенко В., Дубчак О. Сучасні кіберзагрози критичної інфраструктури України та світу. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. Вип. 3(27). С. 150–164. DOI: <https://doi.org/10.28925/2663-4023.2023.27.719>

55. Інститут дослідження кібервійни. URL: <https://ua.understandingcyberwar.org/>

56. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова. URL: <https://ipme.kiev.ua/>

57. Іпполітова І.Я., Мащенко М.А., Іпполітов Є.М. Управління інформаційною безпекою у ланцюгах постачання: ризики цифрової взаємозалежності, моделі довіри та стратегії кіберстійкості. *Соціальний розвиток: економіко-правові проблеми*. 2025. № 7-8. С. 1-17. URL: <https://doi.org/10.70651/3083-6018/2025.7-8.04>.

58. Калайда Ю.П. Гібридні кібератаки в умовах українсько-російської кібервійни. *Інформація і право*. 2025.С. 206-214. DOI: 10.37750/2616-6798.2025.4(55).346481

59. Кібератаки проти Естонії (2007). URL: https://reporter.zp.ua/kiberataki-proti-estoniyi-2007-wnq.html?utm_source=chatgpt.com

60. Коваленко Д., Замрій І. Експериментальне дослідження адаптивного алгоритму маршрутизації для С2С логістики. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. Вип. 4(28). С. 26–40. DOI: <https://doi.org/10.28925/2663-4023.2025.28.815>

61. Колісніченко Н., Войновський М. Інституційна та інституціональна спроможність місцевого самоврядування: сутність понять та особливості визначення. *Теоретичні та прикладні питання державотворення*. 2015. Вип. 16. С. 296-309.

62. Користін О.Є. Інституційна спроможність у сфері лісового господарства. *Наука і правоохоронна*. № 3 (61). 2023. С. 71-81. DOI: 10.36486/np.2023.3(61).7

63. Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет»*. 2023. №06. С. 708-713. DOI: <https://doi.org/10.24144/2788-6018.2023.06.122>

64. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59. DOI: <https://doi.org/10.32850/sulj.2023.3.10>

65. Користін О.Є., Кардашевський Ю.Р. Кіберзлочинність у банківській сфері. *Наука і правоохоронна*. 2024. № 3-4 (65-66). С. 155-163.

66. Користін О.Є., Свиридчук Н.П. Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023 Том 2. № 77. С. 66-74. DOI: <https://doi.org/10.24144/2307-3322.2023.77.2.11>

67. Користін О.Є., Цюприк І.В., Свиридчук Н.П., Прокоф'єва-Янчилієнко Д.М. Оцінювання ризиків розвитку системи кримінальної юстиції України. *Наука і правоохорона*. 2021. № 2. С.108-116.

68. Корченко А.А., Щербина В.П., Вишнева Н.С. A methodology for building cyberattack-generated anomaly detection systems. *Ukrainian Information Security Research Journal*. 2016. Vol. 18. No. 1. P. 30–38. DOI: <https://doi.org/10.18372/2410-7840.18.10110>

69. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінки ризиків інформаційної безпеки: Монографія. Київ: ТОВ «Компринт», 2017. 435 с.

70. Костюченко Я.М. Співпраця України та ЄС у сфері кібербезпеки: механізми боротьби з кіберзлочинністю. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2025. Вип. 15. DOI: 10.54929/2786-5746-2025-15-01-10

71. Красніков С.А. Розвиток національної системи кібербезпеки України. *Інформація і право*. 2025. Вип. 4(55). С. 191-198. URL: [https://doi.org/10.37750/2616-6798.2025.4\(55\).346414](https://doi.org/10.37750/2616-6798.2025.4(55).346414)

72. Красніков С.А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право*. 2023. Вип. 3(46). С. 191-198. DOI: 10.37750/2616-6798.2023.3(46).287214

73. Кутков О.О. Механізм державного регулювання цивільно-військового співробітництва в умовах змін воєнно-політичної обстановки в державі. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. Вип. 5. С. 96-100. DOI:10.51547/ppr.dp.ua/2024.5.13

74. Кутков О.О. Нормативно-правове забезпечення діяльності цивільно-військового співробітництва в сучасних умовах воєнно політичної обстановки: публічно управлінський аспект. *Дніпровський науковий часопис публічного управління, психології, права*. 2024. Вип. 6. С.82-86. DOI DOI:10.51547/PPP.DP.UA/2024.6.13

75. Лисеюк А., Свінцицька Т. Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи. *Право та інноваційне суспільство*. 2024. Вип. 2 (23). С. 89-95. DOI: 10.37772/2309-9275-2024-2(23)-8.

76. Лугіна Н.А., Лучук А.М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис*. 2023. № 1(10). С. 180–186. DOI: 10.33244/2617-4154-1(10)-2023-180-186

77. Мазулевський О. Жолобович Н. Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. Вип. 51(3). с. 34–40. DOI: 10.33099/2311-7249/2024-51-3-34-40.

78. Менчинська М., Лук'янчиков Б. Електронні докази з блокчейн-систем під час воєнного стану: проблема допустимості. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Том. 4 (92). С. 343-349. DOI: 0.24144/2307-3322.2025.92.4.47

79. Науковці НАН України беруть участь у проєкті AGILE: стрес-тестування цифрових систем для підвищення стійкості критичної інфраструктури. URL: https://www.nas.gov.ua/news/naukovci-nan-ukrani-berut-uchast-u-proyekti-agile-stres-testuvannya-cifrovih-sistem-dlya-pidvishchennya-stiykosti-kritichno-infrastrukturi?utm_source=chatgpt.com

80. Національний інститут стратегічних досліджень. URL: <https://niss.gov.ua/publikacii>

81. Не лише DDoS-атаки. Як працює українська IT Армія із 300 тисяч фахівців. URL: https://dou.ua/lenta/articles/it-army-of-ukraine/?utm_source=chatgpt.com

82. Овсійчук Т.П. Теоретико-правові аспекти визначення віртуальних активів як предмета незаконного збагачення. *Науковий вісник Ужгородського Національного Університету*. 2025. Том 3 (88). С. 157-161. DOI: 10.24144/2307-3322.2025.88.3.23

83. Основні завдання Державного центру кіберзахисту Держспецзв'язку. URL: <https://scpc.gov.ua/uk/main-functions-and-tasks>

84. Палко Д., Мирутенко Л. Метод побудови профілю ключових факторів ризику кібербезпеки сучасних розподілених інформаційних систем. *Захист інформації*. 2025. Вип. 26(2). С. 236–252. DOI:10.18372/2410-7840.26.20014.

85. Пархоменко І., Савонік М. Запобігання загрозам хибних конфігурацій aws інфраструктури як коду на основі тестування. *Електронне*

фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Вип. 1(29). С. 236–251. DOI: <https://doi.org/10.28925/2663-4023.2025.29.887>

86. Передерій О.С., Кулачок-Тітова Л.В. Організаційно-правові заходи забезпечення безпеки цифрових послуг в аспекті протидії кіберзлочинності в Україні. *Вісник Кримінологічної асоціації України*. 2025. № 1(44). С. 570-578. DOI: 10.32631/vsa.2025.1.44

87. Петренко К. Особливості інституційної спроможності громадських об'єднань в Україні. *Наукові записки. ІПіЕНД ім. І.Ф. Кураса НАН України*. 2015. Вип. 4 (78). С. 376-388. URL: https://ipien.gov.ua/wp-content/uploads/2018/07/petrenko_osoblyvosti.pdf

88. Петченко М., Черкаський О., Черкаський Д., Переметчик Д., Зубченко Д. а ін. Інтелектуальні підходи до виявлення та реагування на гібридні кібератаки в телекомунікаційних мережах. *Телекомунікаційні та інформаційні технології*. 2025. № 1. С. 80-87. URL: <https://tit.duikt.edu.ua/index.php/telecommunication/article/view/2636>

89. Пискун І.В., Ткач Ю.М., Хорошко В.О., Хохлачова Ю.Є., Аясрах А.З, Аль-Далваш А. Кількісно-якісна оцінка та визначення рівня кібербезпеки інформаційних систем держави. *Ukrainian Scientific Journal of Information Security*. 2020. Vol. 26. No. 3. P. 131-138. DOI: 10.18372/2225-5036.26.14974

90. Північноатлантичний договір: міжнародний документ. Офіційний сайт Верховної Ради України. URL: http://zakon5.rada.gov.ua/laws/show/950_008

91. Поляков О.М. Міжнародне співробітництво України у сфері боротьби з кібертероризмом. *Інформація і право*. 2025. Вип. 4 (55). С. 233-240. DOI: 10.37750/2616-6798.2025.4(55).346485

92. Пономарьов О.П., Пивоварчук С., Козубцова Л., Козубцов І., Бондареко Т., Терещенко Т. Гібридна побудова системи кібербезпеки: адміністративно-правові засади військово-цивільного співробітництва. *Кібербезпека: освіта, наука, техніка*: Електронне фахове наукове видання. 2023. Вип. 3 (19). С. 109–121. DOI: 10.28925/2663-4023.2023.19.109121

93. Потенко О.С., Комаров М.Ю., Артемчук В.О., Зубок В.Ю., Гончар С.Ф. Порівняльний аналіз нових українських та міжнародних стандартів інформаційної безпеки. *Електронне моделювання*. 2025. Т. 47 (5). № 5. С.56-74.

94. Предтечею нової хвилі масштабної агресії рф може стати наступ у кіберпросторі – Секретар РНБОУ. URL: <https://np.pl.ua/2023/02/predtecheiu-novoi-khvyli-masshtabnoi-ahresii-rf-mozhe-staty-nastup-u-kiberprostor-sekretar-rnbou/>

95. Про CERT-UA. URL: <https://cert.gov.ua/about-us>

96. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX. URL: <https://zakon.rada.gov.ua/laws/show/2149-20#Text>

97. Про внесення змін до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518: Постанова Кабінету Міністрів України 3 листопада 2025 р. № 1470. URL: <https://zakon.rada.gov.ua/laws/show/1470-2025-%D0%BF#Text>

98. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15>

99. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>

100. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: Постанова Кабінету Міністрів України від 16 травня 2023 р. № 497. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-poshuku-ta-vyivlennia-a497>

101. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

102. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20>

103. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242/2016. URL: <https://zakon.rada.gov.ua/laws/show/242/2016>

104. Про Національну поліцію: Закон України від 02.02.2015 № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>

105. Про оборону України: Закон України від 06.12.1991 № 1932-XII. URL: <https://zakon.rada.gov.ua/laws/show/1932-12#Text>

106. Про основи національного спротиву: Закон України від 16.07.2021 № 1702-IX. URL: <https://zakon.rada.gov.ua/laws/show/1702-20#Text>

107. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>

108. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30 грудня 2021 року. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>

109. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 р. №392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>

110. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

111. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ

Президента України від 26 травня 2015 р. №287/2015. URL: <https://zakon.rada.gov.ua/laws/show/287/2015>

112. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. URL: <https://zakon.rada.gov.ua/laws/show/2229-12>

113. Проект Закону про Кіберсили Збройних Сил України. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/45453>

114. Прокопович-Ткаченко Д., Зверев В., Козаченко І. Інтеграція операційних центрів управління безпекою (SOC) у систему національної безпеки України. *Системи та технології*. 2024. № 3. С. 106-114. URL: DOI: 10.33405/2786-8613/2025/1/5/336736

115. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін.; за заг. ред. Користіна О.Є. Київ: «ВАІТЕ», 2024. 444 с. DOI: <https://doi.org/10.36486/978-966-2310-66-5>

116. Резнікова О.О. Забезпечення стійкості держави і суспільства до терористичної загрози в Україні та світі. *Стратегічні пріоритети*. 2017. № 3 (44). С. 22-28.

117. Користін О., Крищенко К. Сучасні тенденції відмивання коштів у кіберпросторі. *Наука і правоохорона*. 2024. № 3-4 (65-66). С. 164-174.

118. Річний аналітичний огляд. НКЦК. USAID. Жовтень 2023 – вересень 2024. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf

119. Російські хакери у 2023 році збільшили кількість атак на Україну: що відомо. URL: [unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vidomo-](https://unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vidomo-12426765.html?_gl=1*b62dke*_ga*NTUzMzI0Mzg3LjE2OTc0Nzg3NzY.*_ga_TECJ2YKWSJ*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE4MC41NS4wLjA.*_ga_DENC12J6P3*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE3OS41Ni4wLjA)

[12426765.html?_gl=1*b62dke*_ga*NTUzMzI0Mzg3LjE2OTc0Nzg3NzY.*_ga_TECJ2YKWSJ*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE4MC41NS4wLjA.*_ga_DENC12J6P3*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE3OS41Ni4wLjA](https://unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vidomo-12426765.html?_gl=1*b62dke*_ga*NTUzMzI0Mzg3LjE2OTc0Nzg3NzY.*_ga_TECJ2YKWSJ*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE4MC41NS4wLjA.*_ga_DENC12J6P3*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE3OS41Ni4wLjA)
A

120. Світличний В.А. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека*. 2023. № 3 (90). С. 226-236.

121. Сидоренко В., Максимець А. Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. Вип. 3(27). С. 560–571. DOI: <https://doi.org/10.28925/2663-4023.2025.27.779>

122. 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. DOI: <https://doi.org/10.23939/law2024.41.314>

123. Складанний П., Гулак Г., Корнієць В. Коаліційний підхід до управління кібербезпекою інформаційних систем що застосовують хмарні технології. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. Вип. 4(28). С. 8–25. DOI: 10.28925/2663-4023.2025.27.825

124. Словник української мови: [в 11 т.] / [ред. кол.: І.К. Білодід (гол.) та ін.]; АН УРСР, Ін-т мовознавства ім. О.О. Потебні. Том 9. Київ: Наукова думка, 1978. 916 с.

125. Смірнова Т. Дослідження методів, моделей та сучасних іт-рішень для підтримки технологічних процесів у критичній інфраструктурі держави. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. Вип. 2(30). С. 195–208. URL: <https://doi.org/10.28925/2663-4023.2025.30.962>

126. Степанов О.О., Скорик Ю.В. Перспективи використання підходу INFRASTRUCTURE AS CODE та огляд популярних рішень. *Радіоелектроніка та молодь у XXI столітті: матеріали 27-го Міжнар. молодіж. форуму, 10–12 травня 2023 р.* Харків: ХНУРЕ, 2023. Т. 4. С. 135-136.

127. Ткач Д., Васильєва О. Енергетичний сектор України у воєнний і післявоєнний період: стратегічні підходи та інноваційні рішення. *European*

Scientific Journal of Economic and Financial Innovation. 2025. Вип. 1(15). С. 299-308. URL: <https://doi.org/10.32750/2025-0126>

128. Управління кібербезпекою. URL: https://learn.ztu.edu.ua/pluginfile.php/406445/mod_resource/content/1/%D0%A3%D0%9A%20%D0%9B%D0%95%D0%9A%D0%A6%D0%86%D0%AF1.pdf

129. Україна імплементує директиву NIS2 щодо безпеки мереж і інформаційних систем. URL: https://interfax.com.ua/news/telecom/1050728.html?utm_source=copilot.com

130. Українська ІТ-армія налічує понад 300 тисяч кіберфахівців. URL: https://imi.org.ua/news/ukrayinska-it-armiya-narahovuye-ponad-300-tysyach-kiberfahivtsiv-mintsyfry-i44578?utm_source=chatgpt.com

131. Федієнко О.П. Міжнародні стандарти оцінки кіберстійкості. *Інформація і право*. 2024. № 3(50) С. 124-135. DOI: [https://doi.org/10.37750/2616-6798.2024.3\(50\).311680](https://doi.org/10.37750/2616-6798.2024.3(50).311680)

132. Храмов С., Опірський І. Аналіз сучасного стану кібератак в Україні під час війни. *Захист інформації*. 2024. Вип. 26(1). С. 187–196. DOI:10.18372/2410-7840.26.18842

133. Червяков О.І. Особливості забезпечення кібербезпеки як провідної складової національної безпеки України. *Вісник Кримінологічної асоціації України*. 2026. Вип. 33(3). С. 511-518. DOI: <https://doi.org/10.32631/vca.2024.3.47>

134. Шиповський В. Модель оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури під впливом гібридних кібератак з використанням алгоритмів машинного навчання. *Ukrainian Scientific Journal of Information Security*. 2024. Вип. 30 (2). С. 235–243. URL: <https://doi.org/10.18372/2225-5036.30.19234>

135. Шульга В.П., Іванченко Є.В., Вишневська Н.С., Бербер А.С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. *Сучасний захист інформації*. 2024. Вип. 3(59). С. 6–19. URL: <https://doi.org/10.31673/2409-7292.2024.030001>.

136. Якимчук М.Ю. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. *Нове українське право*. 2021. № 4(27). С. 182-186. DOI: 10.51989/NUL.2021.4.27

137. Яковів І., Шарадкін Д., Куліков В. Моделі інтеграції інформації розвідки кіберзагроз. *Information Technology and Security*. 2025. Vol. 13(2). P. 236–252. URL: <https://doi.org/10.20535/2411-1031.2025.13.2.344710>.

138. «He immutable – значить не бекап»: як захистити дані, коли хакери тепер можуть легко стерти навіть резервні копії. URL: https://dev.ua/news/de-novo-1748963032?utm_source=chatgpt.com

139. A Refresher on Regression Analysis. URL: <https://hbr.org/2015/11/a-refresher-on-regression-analysis>

140. Adeyinka F., Oluyemi E.S., Victor A.N., Uchenna U.C., Ogedengbe O., Ale S. Parametric Equation for Capturing Dynamics of Cyber Attack Malware Transmission with Mitigation on Computer Network. *International Journal of Mathematical Sciences and Computing*. 2017. Vol. 3. No. 4. P. 37-51. DOI: 10.5815/ijmsc.2017.04.04

141. Advancing Cyber Resilience: Principles and Tools for Boards. Geneva: World Economic Forum, 2017. URL: https://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

142. Agarwal V.K., Garg S.K., Kapil M., Sinha D. Cyber Crime Investigations in India: Rendering Knowledge from the Past to Address the Future. *ICT and critical infrastructure: proceedings of the 48th annual convention of CSI*. 2014. Vol 2: Springer International Publishing Switzerland. P. 593–600. DOI:10.1007/978-3-319-03095-1_64

143. Akhgar B., Bayerl P.S., Sampson F. *Open Source Intelligence Investigation: From Strategy to Implementation*. Advanced Sciences and Technologies for Security Applications. Springer International Publishing AG. 2016. 304 p. DOI: 10.1007/978-3-319-47671-1

144. Akhgar B., Saathoff G.B., Arabnia H.R., Hill R., Staniforth A., Bayerl P.S. *Application of big data for national security: a practitioner's guide to emerging technologies*. Butterworth-Heinemann, 2015.

145. Alberts C., Behrens S., Pethia R., Wilson W. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. 1999, September 1. (SEI Report CMU/SEI-99-TR-017). DOI: <https://doi.org/10.1184/R1/6575906.v1>

146. Alberts D. Information age Transformation. Getting to a 21st Century Military. DOD Command and Control Research Program. Monograph. 2002. URL: http://www.dodccrp.org/files/Alberts_IAT.pdf

147. Alberts D., Hayes R. Code of Best Practice for Experimentation. CCRP Publication Series, Washington. 2002. URL: http://dodccrp.org/files/Alberts_Experimentation.pdf

148. Allen J., Curtis P. Measures for Managing Operational Resilience. *Technical Report*. CMU/SEI-2011-TR-019. 2011. URL: https://www.sei.cmu.edu/documents/877/2011_005_001_15407.pdf

149. Althonayan A., Andronache A. Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. Oxford, UK, 2019. P. 1-9. DOI: 10.1109/CyberSA.2019.8899445

150. Ansell C., Boin A., Keller A. Managing transboundary crises: identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*. 2010. Vol. 18(4). URL: https://www.researchgate.net/publication/48327974_Managing_Transboundary_Crises_Identifying_the_Building_Blocks_of_an_Effective_Response_System

151. Anwar S., Yamin T. Civil Military Cooperation (CIMIC) in Cyber Security Domain: Analyzing Pakistan's Prospects. *Global Strategic & Security Studies Review*. 2021. Vol. VI(I). P. 68-81. DOI:10.31703/gsssr.2021(VI-I).08

152. Arce I. The Weakest Link Revisited. *IEEE Security and Privacy*. 2003. Vol. 1. (2). P. 72–76. DOI: 10.1109/MSECP.2003.1193216
153. Aven T. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*. 2016. Vol. 253. No. 1. P. 1–13. URL: <https://doi.org/10.1016/j.ejor.2015.12.023>
154. Ayres I., Braithwaite J. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press, 1992. 204 p. URL: <https://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf>
155. Badman A., Robertson D. What is immutable infrastructure? URL: https://www.ibm.com/think/topics/immutable-infrastructure?utm_source=chatgpt.com.
156. Bagheri S., Ridley G. Organisational cyber resilience: research opportunities. *Australasian Conference on Information Systems*. 2017.
157. Bakkensen L.A., Fox-Lent C., Read L.K., Linkov I. Validating Resilience and Vulnerability Indices in the Context of Natural Disasters: Validating Resilience and Vulnerability Indices. *Risk Analysis*. 2017. Vol. 37. No. 5. P. 982–1004.
158. Barber C. Cyber Security Predicting the Future. *ITNOW*. 2020. Vol. 62. Is.1. P. 30–31. DOI:10.1093/itnow/bwaa013
159. Bartol N., Bates B., Goertzel K., Winograd T. Measuring cyber security and information assurance. State of the Art Report. 2009. URL: <https://csiac.dtic.mil/state-of-the-art-reports/measuring-cyber-security-and-information-assurance/>
160. Beck U. *Risk Society: Towards a New Modernity*. London: Sage Publications, 1992. 260 p.
161. Benson M.H., Craig R.K. The end of sustainability. *Society & Natural Resources*. 2014. Vol. 27 (7). P. 777–782. DOI: 10.1080/08941920.2014.901467

162. Blockchain Analysis for National Security and Law Enforcement Agencies: A Primer. URL: <https://www.chainalysis.com/blog/blockchain-analysis-national-security-law-enforcement/>

163. Blockchain Forensic Forum 2025: розвиток судової експертизи у сфері блокчейну в Україні. Київський науково-дослідний інститут судових експертиз. URL: <https://kndise.gov.ua/en/article/blockchain-forensic-forum-2025-rozvytok-sudovoyi-ekspertyzy-u-sferi-blokcheynu-v-ukrayin>

164. Bodeau D., Graubart R. *Cyber Resilience Metrics: Key Observations*. The MITRE Corporation. 2016. 10 p. URL: <https://www.mitre.org/sites/default/files/2021-08/pr-16-0779-cyber-resilience-metrics-key-observations.pdf>

165. Bodeau D., Graubart R. *Cyber Resiliency Assessment: Enabling Architectural Improvement*. MITRE Technical Report. MTR120407. 2013. 120 p. URL: https://www.mitre.org/sites/default/files/pdf/12_3795.pdf

166. Bodeau D., Graubart R. *Cyber Resiliency Design Principles*. MITRE Technical Report. 2017. URL: <https://www.mitre.org/news-insights/publication/cyber-resiliency-design-principles>

167. Bodeau D., Graubart R. *Cyber Resiliency Engineering Framework*. MITRE Technical Report. MTR110237. 2011. 78 p. URL: <https://apps.dtic.mil/sti/trecms/pdf/AD1108457.pdf>

168. Bodeau D., Graubart R. Structured Cyber Resiliency Analysis Methodology (SCRAM). *MITRE Corporation*. 2016. URL: <https://www.mitre.org/news-insights/publication/structured-cyber-resiliency-analysis-methodology>

169. Bodeau D., Graubart R., Heinbockel W., Laderman E. *Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*. MITRE Technical Report. MTR140499. 2015. 63 p. URL: <https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf>

170. Bodeau D., Graubart R., McQuaid R., Woodill J. *Cyber Resiliency Metrics Catalog*. MITRE Technical Report. 2018. URL: <https://www.mitre.org/sites/default/files/2021-11/pr-18-3376-cyber-resiliency-metrics-catalog.pdf>
171. Bodeau D., Graubart R. *Cyber Resiliency and NIST SP 800-53 Rev.4 Controls*. MITRE Technical Report. 2013. URL: <https://www.mitre.org/sites/default/files/publications/13-4047.pdf>
172. Boeke S., Heintl C., Veenendaal M. A. Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe. 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon). 2015. DOI:10.1109/CYCON.2015.7158469
173. Bonanno G.A. Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely aversive events? *American Psychologist*. 2004. Vol. 59(1). P. 20–28. DOI:10.1037/0003-066X.59.1.20
174. Bostick T.P., Connelly E.B., Lambert J.H., Linkov I. Resilience Science, Policy and Investment for Civil Infrastructure. *Reliability Engineering & System Safety*. 2018. Vol. 175. P. 19–23. URL: <https://doi.org/10.1016/j.ress.2018.02.025>
175. Braithwaite J. What's wrong with the sociology of punishment? *Theoretical Criminology*. 2003. Vol. 7. P. 5–28.
176. Brantingham P.L. Computational Criminology. *European Intelligence and Security Informatic Conference*. IEEE Computer Society. 2011. DOI:10.1109/EISIC.2011.79
177. Brassett J., Croft S., Vaughan-Williams N. Introduction: An Agenda for Resilience Research in Politics and International Relations. *Politics*. 2013. Vol. 33. №. 4. P. 221-228.
178. Brunsson N., Jacobsson B. A World of Standards. Oxford: Oxford University Press, 2000. DOI:10.1093/acprof:oso/9780199256952.001.0001
179. Building NIS2 compliance and resilience: Strategic recommendations for EMEA organizations. URL: <https://cdn-dynmedia->

1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/security/microsoft-general-building-nis2-compliance-resilience-strategic-recommendations-for-emea-organizations.pdf

180. Burden K., Palmer C. Internet crime: Cyber Crime – A new breed of criminal? *Computer Law & Security Review*. 2003. Vol. 19. No. 3. P. 222–227. DOI: [https://doi.org/10.1016/S0267-3649\(03\)00306-6](https://doi.org/10.1016/S0267-3649(03)00306-6)

181. Bures O. EU Counterterrorism Policy: A Paper Tiger? *Terrorism and Political Violence*. 2006. Vol. 18 (1). P. 57–78. DOI: 10.1080/09546550500174905

182. Burt D., Kleiner A., Nicholas J. P., Sullivanl K. Cyberspace 2025: Today's Decisions, Tomorrow's Terrain. Navigating the Future of Cybersecurity Policy. Microsoft. 2014. 47 p.

183. Busch L. Standards: Recipes for Reality. Cambridge: The MIT Press Cambridge, Massachusetts London, England. 2011.

184. Button M. *Doing Security: Critical Reflections and an Agenda for Change*. Basingstoke: Palgrave Macmillan. 2008. 272 p.

185. Byczyński M. The Legal Status of 'Civilian Hackers' under International Humanitarian Law. *Acta Universitatis Lodziensis. Folia Iuridica*. 2024. Vol. 106. P. 97–109. URL: <https://doi.org/10.18778/0208-6069.106.06>

186. Caralli R.A., Allen J.H., White D.W., Young L.R., Mehravari N., Curtis P.D. *CERT® Resilience Management Model, Version 1.2*. Software Engineering Institute, Carnegie Mellon University. 2016. 35 p. URL: <https://apps.dtic.mil/sti/trecms/pdf/AD1145855.pdf>

187. Carías J.F., Labaka L., Sarriegi J. M., Hernantes J. Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *Sensors*. 2019. Vol. 19, No. 1. P.1-16. DOI: 10.3390/s19010138

188. Carías J.F., Arrizabalaga S., Labaka L. Hernantes J. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access*. 2021. Vol. 9. P. 80741-80762. DOI: 10.1109/ACCESS.2021.3085530

189. Carías J.F., Borges M.R.S., Labaka L., Arrizabalaga S., Hernantes J. Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access*. 2020. Vol. 8. P. 174200-174221. DOI: 10.1109/ACCESS.2020.3026063
190. Carias J.F., Labaka L., Sarriegi J.M., Hernantes J. Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *In Proceedings of the 2018 Global Internet of Things Summit* (Bilbao, Spain, 4–7 June 2018). *Sensors*. 2019. Vol. 19 (1). DOI:10.3390/s19010138
191. Cartwright N., Hardie J. *Evidence-based policy: a practical guide to doing it better*. Oxford; New York: Oxford University Press, 2012. 196 p.
192. Castells M. *The Internet Galaxy: Reflexions on the Internet, Business, and Society*. Oxford: Oxford University Press. 2021. 292 p.
193. Cavelty M.D., Kaufmann M., Soby K.K. Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*. 2015. Vol. 46 (1). P. 3–14. DOI: <https://doi.org/10.1177/0967010614559637>
194. Cavelty M.D., Suter M. *The Art of CIIP Strategy: Taking Stock of Content and Processes*. 2012. DOI:10.1007/978-3-642-28920-0_2
195. CERT® Resiliency Engineering Framework (REF) Outline. Preview version, v0.95R, 2008. Software Engineering Institute. URL: http://book.itep.ru/depositary/security/REFv0.95R_cert.pdf
196. CERT-UA. URL: <https://uk.wikipedia.org/wiki/CERT-UA>
197. Chandrasekharan P.C. *Robust control of linear dynamical systems*. Missouri: Academic Press. 1996.
198. Chen L.P., Zhang C.Y. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Science*. 2014. Vol. 275. P. 314–347. URL: <https://doi.org/10.1016/j.ins.2014.01.015>.
199. Chonka A., Xiang Y., Zhou W., Bonti A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*. 2011. Vol. 34 (4). P. 1097–1107. DOI: <https://doi.org/10.1016/j.jnca.2010.06.004>

200. *CISA Strategic Plan 2023-2025*. Cybersecurity and Infrastructure Security Agency. 2022. 35 p. URL: <https://ec.europa.eu/newsroom/cipr/items/765280/en>

201. *Cochrane Handbook for Systematic Reviews of Interventions*. Edited by Higgins J.P.T., Thomas J., Chandler J., Cumpston M., Li T., Page M.J., Welch V.A. Second Edition, 2019. URL: <https://dariososafoula.wordpress.com/wp-content/uploads/2017/01/cochrane-handbook-for-systematic-reviews-of-interventions-2019-1.pdf>

202. Collier Z., DiMase D., Walters S., Tehranipoor M.M., Lambert J.H., Linkov I. Cybersecurity standards: managing risk and creating resilience. *Computer*. 2014. Vol. 47. P. 70–76. DOI: <https://doi.org/10.1109/MC.2013.448>

203. Conference Board of Canada. Building Cyber Resilience. URL: <https://www.rjmcgregor.com/wp-content/uploads/2018/09/Building-Cyber-Resilience.pdf>

204. Cook T., Hibbitt S., Hill M. Blackstone's crime investigator's handbook. Oxford: Oxford University Press, 2013. 472 p.

205. Coordinated vulnerability disclosure policies in the EU. European Union Agency for Cybersecurity (ENISA), 2022. 90 p. URL: <https://www.enisa.europa.eu/sites/default/files/publications/Coordinated%20Vulnerability%20Disclosure%20policies%20in%20the%20EU.pdf>

206. Coordinated Vulnerability Disclosure Program. URL: <https://www.cisa.gov/resources-tools/programs/coordinated-vulnerability-disclosure-program>

207. Cyber Resilience for the C-Suite. UpGuard. URL: <https://www.upguard.com/resources/cyber-resilience-for-the-c-suite>

208. Cyber resilience of on-board systems and equipment (UR E27). IACS. 2022. 14 p. URL: <https://www.american-club.com/files/files/ur-e27-new-apr-2022.pdf>

209. Cyber resilience of ships (UR E26). IACS. 2022. 32 p. URL: <https://www.american-club.com/files/files/ur-e26-new-apr-2022.pdf>

210. Cyber Resilience Review (CRR): Method Description and Self-Assessment User *Guide*. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. CISA. 2020. URL: https://www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf

211. Cyber Resilience: Safeguarding the Digital Organization. Cisco Public. 2016. URL: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cyber-resilience-safeguarding-digital-org-wp.pdf

212. Cyber risk and resilience: Mitigating risks and business impact. KPMG. 2021. URL: <https://assets.kpmg.com/content/dam/kpmg/in/pdf/2021/07/cyber-risk-and-resilience-mitigating-risks-and-resilience.pdf>

213. Cyber Security Strategy. Ministry of Defense. Estonia. 2008. URL: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSSL_2008_en.pdf?utm_source=chatgpt.com

214. Cybersecurity Skills Development in the EU. The certification of cybersecurity degrees and ENISA's Higher Education Database. *ENISA*. 2023: URL: <https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu>

215. Danish M. Enhancing Cyber Security Through Predictive Analytics: Real-Time Threat Detection and Response. *International Journal of Advanced Computer Science and Applications(IJACSA)*. 2025. Vol. 16 (8). DOI: 10.14569/IJACSA.2025.0160804

216. Danowski J.A. *Counterterrorism mining for individuals semantically similar to watchlist members*. In: Kock Wiil U. (ed) Counterterrorism and open source intelligence. Springer Berlin Heidelberg. 2011. P. 223–247. DOI:10.1007/978-3-7091-0388-3_12

217. Davidson J.L., Jacobson C., Lyth A., Dedekorkut-Howes A., Baldwin C.L., Ellison J.C., Holbrook N.J., Howes M.J., Serrao-Neumann S., Singh-Peterson L., Smith T.F. Interrogating resilience: toward a typology to improve its

operationalization. *Ecology and Society*. 2016. Vol. 21(2). DOI: <http://dx.doi.org/10.5751/ES-08450-210227>

218. Department of defense strategy for operating in cyberspace. Department of Defense. 2011. URL: <https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf>

219. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST / Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R.. Special Publication 800-160, Vol. 2. 2021. 294 p. DOI: <https://doi.org/10.6028/NIST.SP.800-160v2r1>

220. Digital Defense Report 2024: The foundations and new frontiers of cybersecurity. Microsoft. 114 p. URL: <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf>

221. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD 2015. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc/9789264245471-en.pdf

222. DiMase D., Collier Z.A., Heffner K., Linkov I. Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*. 2015. Vol. P. 35, 291–300. DOI:10.1007/s10669-015-9540-y

223. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *Official Journal of the European Union*. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

224. Directive on security of network and information systems (NIS). URL: <https://digital-strategy.ec.europa.eu/en/library/directive-security-network-and-information-systems-nis-directive>
225. Disaster Resilience: A National Imperative. National Research Council. Washington, DC: The National Academies Press, 2012. 244 p. URL: <https://www.nationalacademies.org/read/13457/chapter/1>
226. Disterer G. ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*. 2013. Vol. 4. P. 92–100. DOI:10.4236/jis.2013.42011
227. Dobrynychuk O., Lukashenko V. Energy critical infrastructure under attack: incident analysis and implications for ICS/SCADA resilience. *Ukrainian Scientific Journal of Information Security*. 2025. Vol. 31. Issue 2. P. 112-129. DOI: 10.18372/2225-5036.31.20706.
228. Dornhege G., Millan J., Hinterberger T., McFarland D., Müller K. Toward Brain–Computer Interfacing. Cambridge, MA: MIT Press. 2007. URL: <http://www.ece.uprm.edu/~manian/toward%20brain%20computer%20interfacing.pdf>
229. Downes B.J., Miller F., Barnett J., Glaister A., Ellemor H. How do we know about resilience? An analysis of empirical research on resilience, and implications for interdisciplinary praxis. *Environmental Research Letters*. 2013. Vol. 8. P. 1-8. DOI:10.1088/1748-9326/8/1/014041
230. Dubynskyi G., Zubok V. The resilience of critical information infrastructure topology in the cyberspace. *International Science Journal of Engineering & Agriculture*. 2025. Vol. 4 (1). P.103–110. DOI: <https://doi.org/10.46299/j.isjea.20250401.09>
231. Dunn Cavelty M., Kaufmann M., Soby Kristensen K. Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*. 2015. Vol. 46. P. 3–14.

232. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*. 2019. Vol. 5, No. 1. P. 1–17. DOI: <https://doi.org/10.1093/cybsec/tyz013>

233. Eckmaier R., Fumy W., Mouille S., Quemard J.-P., Polemi N., Rumpel R. Risk Management Standards. Analysis of standardisation requirements in support of cybersecurity policy. ENISA. 2022. URL: https://www.enisa.europa.eu/sites/default/files/publications/O.7.2-T2-Risk_Management_standards.pdf

234. Ellis J., Fisher D., Longstaff T. A., Pesante L., Pethia R.D. Report to the President's Commission on Critical Infrastructure Protection. Special Report. CMU/SEI-97-SR-003. 1997. DOI: 10.1184/R1/6583157.v1

235. ENISA Threat Landscape 2022. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf>

236. EU Agency presents 1st report ever on how to measure IT resilience. ENISA, 2011. URL: https://www.enisa.europa.eu/news/enisa-news/eu-agency-presents-1st-report-ever-on-how-to-measure-resilience?utm_source=chatgpt.com#contentList

237. EU Cyber Resilience Act: Briefing. European Parliamentary Research Service. 2024. 12 p. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI\(2022\)739259_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf)

238. European Union Cyber Resilience Act: A Compliance Guide for Connected Devices. DigiCert. 2025. 8 p. URL: <https://www.digicert.com/content/dam/digicert/pdfs/whitepaper/digicert-eu-cra-whitepaper-en.pdf>

239. Executive Order 13636 of February 12, 2013. URL: <https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity>

240. Executive Order 14028 on Improving the Nation's Cybersecurity. The White House, 2021. URL: <https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf>

241. Fallah M. A puzzle-based defence strategy against flooding attacks using game theory. *IEEE Transactions on Dependable and Secure Computing*. 2010. Vol. 7 (1). P. 5–19. DOI: 10.1109/TDSC.2008.13

242. Federal Bureau of Investigation, Intelligence Branch, Intelligence Collection Disciplines. URL: <https://www.fbi.gov/how-we-investigate/intelligence>

243. Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. 2023. URL: <https://nsarchive.gwu.edu/themes/custom/nsarchive/templates/pdfjs/web/viewer.html?file=https%3A%2F%2Fnsarchive.gwu.edu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Fs9zfme-rssdn%2F2023-02-16-Google-TAG-Fog-of-War-How-Ukraine-Conflict-Transformed-Cyber-Threat-Landscape-Website.pdf>

244. Fomin V., Vries H., Barlette Y. ISO/IEC 27001 Information systems security management standard: Exploring the reasons for low adoption. *EuroMOT 2008 - The Third European Conference on Management of Technology*. Nice, France. September 2008. URL: https://www.researchgate.net/publication/228898807_ISOIEC_27001_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption

245. Foresight Best Practices. URL: <https://www.futuresplatform.com/blog/megatrends-trends-and-change-drivers-the-larger-picture-and-path-dependencies>

246. Foresight Challenges. A study to enable foresight on emerging and future cybersecurity challenges. European Union Agency for Cybersecurity (ENISA). 2021. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Foresight%20Challenges.pdf>

247. Foresight. The Manual. Singapore: UNDP Global Centre for Public Service Excellence GCPSE, 2014. URL: https://www.undp.org/sites/g/files/zskgke326/files/publications/GCPSE_Foresight_Manual_online.pdf
248. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. NIST. 2014. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf>
249. Futures platform. URL: <https://www.futuresplatform.com/product>
250. Gaining Ground on the Cyber Attacker: 2018 State of Cyber Resilience. Accenture Security, 2018. URL: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-78/accenture_gaininggroundcyber_transcript_051418.pdf
251. Gallagher S. Candid camera: Dutch hacked Russians hacking DNC, including security cameras. *Ars Technica*. 2018. URL: <https://arstechnica.com/information-technology/2018/01/dutch-intelligence-hacked-video-cameras-in-office-of-russians-who-hacked-dnc/>
252. Ganin A.A., Massaro E., Gutfraind A., Steen N., Keisler J.M., Kott A., Mangoubi R. S., Linkov I. Operational resilience: concepts, design and analysis. *Scientific Reports*. 2016. Vol. 6. DOI:10.1038/srep19540
253. Garland D. The Culture of Control: Crime and Social Order in Contemporary Society. Oxford: Oxford University Press, 2001.
254. Ghaderipour Y., Dinari H. A Flow-Based Technique to Detect Network Intrusions Using Support Vector Regression (SVR) over Some Distinguished Graph Features. *International Journal of Mathematical Sciences and Computing*. 2020. Vol. 6. No. 4. Pp.1-11. DOI: 10.5815/ijmsc.2020.04.01
255. Giddens A. Risk and responsibility. *Modern Law Review*. 1999. Vol. 62. P. 1-10.
256. Gisladdottir V., Ganin A. A., Keisler J. M., Kepner J., Linkov I. Resilience of Cyber Systems with Over- and Underregulation. *Risk Analysis*. 2017. Vol. 37 (9). P.1644-1651. URL:

https://www.researchgate.net/publication/311549952_Resilience_of_Cyber_Systems_with_Over-_and_Underregulation_Perspective

257. Global Cybersecurity Outlook. WEF. 2024. URL: <https://www.weforum.org/reports/global-cybersecurity-outlook-2024/>

258. Gnatiuk S., Bakalynsky A., Myalkovsky D., Pakholchenko, D. Resilience and constantly of information infrastructure functioning within the national resilience system. *Political Science and Security Studies Journal*. 2022. Vol. 3(1). P. 26-31. DOI: <https://doi.org/10.5281/zenodo.6385602>

259. Goldammer P., Annen H., Stöckli P.L., Jonas K. Careless responding in questionnaire measures: Detection, impact, and remedies. *The Leadership Quarterly*. 2020. Vol. 31(4). DOI: <https://doi.org/10.1016/j.leaqua.2020.101384>

260. Good Practice Guide on National Exercises: Enhancing the Resilience of Public Communications Networks. ENISA, 2009. URL: <https://nukib.gov.cz/download/publikace/navody/cviceni/National%20Exercises%20Good%20Practice%20Guide.pdf>

261. Gorur R. The invisible infrastructure of standards. *Critical Studies in Education*. 2013. Vol. 54, Iss. 2. P. 132–42. URL: <https://doi.org/10.1080/17508487.2012.736871>

262. Gottschalk P. *White-Collar Crime: Detection, Prevention and Strategy in Business Enterprises*. Universal-Publishers, Boca Raton, Florida, USA, 2010. 197 p.

263. Gottschalk P., Filstad C., Glomseth R., Solli-Sæther H. Information management for investigation and prevention of white-collar crime. *International Journal of Information Management*. 2011. Vol. 31 (3). P. 226–233. DOI: 10.1016/j.ijinfomgt.2010.07.002

264. Govil J. Ramifications of cyber crime and suggestive preventive measures. *IEEE International Conference on Electro/Information Technology*. 2007. P. 610–615. DOI:10.1109/EIT.2007.4374526

265. Guide for Conducting Risk Assessments. NIST Special Publication 800-30. Rev.1. 2012. 95 p.

266. Guide to Cyber Threat Information Sharing. NIST. Special Publication 800-150. URL: <https://csrc.nist.gov/pubs/sp/800/150/final>
267. H.R.2029 - Consolidated Appropriations Act, 2016. 114th Congress (2015-2016). URL: <https://www.congress.gov/bill/114th-congress/house-bill/2029>
268. Haegeman K., Spiesberger M., Könnölä T. Evaluating foresight in transitional research programming. *Technological Forecasting and Social Change*. 2017. Vol. 115. P. 313–326. DOI: 10.1016/j.techfore.2016.07.017
269. Haimes Y.Y. On the Definition of Resilience in Systems. *Risk Analysis*. 2009. Vol. 29, No. 4. P. 498–501. DOI: 10.1111/j.1539-6924.2009.01216.x
270. Haimes Y.Y. *Risk Modeling, Assessment, and Management*. 3rd ed. New York: Wiley, 2009. 1040 p.
271. Haimes Y.Y. On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis*. 2006. Vol. 26 (2). P. 293–296.
272. Haimes Y.Y. Total risk management. *Risk Analysis*. 1991. Vol. 11 (2). P. 169–171.
273. Halvin S., Kenett D.Y., Ben-Jacob E., Bunde A., Choen R., Hermann H., Kantelhardt J.W., Kertesz J., Kirkpatrick S., Kurths J., Portugali J., Solomon S. Challenges in network science: Applications to infrastructures, climate, social systems, and economics. *European Physical Journal: Special Topics*. 2012. Vol. 214. P. 273–293. DOI: 10.1140/epjst/e2012-01695-x
274. Hamilton M.C., Lambert J.H., Connelly E.B., Barker K. Resilience analytics with disruption of preferences and lifecycle cost analysis for energy microgrids. *Reliability Engineering & System Safety*. 2016. Vol. 150. P. 11-21.
275. Harfield C., Harfield K. *Intelligence: investigation, community and partnership*. Oxford: OUP Oxford, 2008.
276. Hassell S., Beraud P., Cruz A., Ganga G., Martin S., Toennies J. Evaluating Network Cyber Resiliency Methods using Cyber Threat, Vulnerability and Defense Modeling and Simulation. MILCOM 2012 - 2012 IEEE Military Communications Conference (Orlando, FL, USA). 2012. P. 1-6. DOI: 10.1109/MILCOM.2012.6415565

277. Herrington L., Aldrich R. The Future of Cyber-Resilience in an Age of Global Complexity. *Politics*. 2013. Vol. 33(4). P. 299–310.
278. History and Creation of the CSF 1.1. NIST. URL: <https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework>
279. Holdsworth J., Badman A. Infrastructure as code, defined. URL: <https://www.ibm.com/think/topics/infrastructure-as-code>
280. Holling C.S. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*. 1973. Vol. 4. P. 1–23.
281. Holling C.S. *Engineering resilience versus ecological resilience*. In: Schulze P.E. (ed.). *Engineering within Ecological Constraints*. Washington DC: National Academy Press. 1996. P. 31-43.
282. Hollnagel E., Pariès J., Woods D. D., Wreathall J. *Resilience Engineering in Practice: A Guidebook*. Ashgate Publishing, 2011. 362 p. DOI: <https://doi.org/10.1201/9781317065265>
283. Hoque N., Bhuyan H., Baishya R.C., Bhattacharyya D.K., Kalita J.K.V. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*. 2014. Vol. No. 40. P. 307–324. DOI:10.1016/j.jnca.2013.08.001
284. Identifying Emerging Cyber Security Threats and Challenges for 2030. ENISA. 2023. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf>
285. IFTF. URL: <https://www.iftf.org/>
286. Iqbal F., Binsalleeh H., Fung B.C.M., Debbabi M. A unified data mining solution for authorship analysis in anonymous textual communications. *Information Science*. 2013. Vol. 231. P. 98–112. URL: <https://dmas.lab.mcgill.ca/fung/pub/IBFD13ins.pdf>
287. Iqbal F., Fung B.C.M., Debbabi M. Mining Criminal Networks from Chat Log. *IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*. 2012. P. 332–337. DOI: 10.1109/WI-IAT.2012.68

288. Information Sharing and Analysis Centers (ISACs). URL: <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/information-sharing-and-analysis-centers-isacs>

289. Infrastructure Resilience Planning Framework (IRPF). CISA. February 2024. Version 1.2. URL: https://cisecuritysummit.com/InfrastructureResiliencePlanningFrameworkv12_JAN2024_508c.pdf

290. *ISO/IEC 27031:2025: Cybersecurity — Information and communication technology readiness for business continuity*. International Standard. Edition 2. 2025. 33 p.

291. ISO/IEC. ISO/IEC 27035-1: Information Technology – Security Techniques – Information Security Incident Management – Part 1: Principles of Incident Management. Geneva: ISO, 2016. URL: https://www.researchgate.net/publication/228898807_ISOIEC_27001_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption

292. ISOfocus. The cyber secrets. URL: [https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20\(2013-NOW\)/en/2019/ISOfocus_132/ISOfocus_132_en.pdf](https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20(2013-NOW)/en/2019/ISOfocus_132/ISOfocus_132_en.pdf)

293. IT Army of Ukraine. URL: https://en.wikipedia.org/wiki/IT_Army_of_Ukraine?utm_source=chatgpt.com

294. Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*. 2025. Vol. 17. Is. 19. P. 8757. <https://doi.org/10.3390/su17198757>

295. Jackson M. Chapter 1. Practical Foresight Guide. 2013. URL: <https://www.shapingtomorrow.com/files/media-centre/pf-ch01.pdf>

296. Jansen W. *Directions in security metrics research*. The National Institute of Standards and Technology (NISTIR 7564). 2009. URL: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf

297. Joseph J. Resilience as embedded neoliberalism: a govern mentality approach. *Resilience: International Policies, Practices and Discourses*. 2013. Vol. 1(1). P. 38-52. DOI: 10.1080/21693293.2013.765741
298. Joshi Ch., Singh U.K. Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*. 2017. Vol. 35. P. 128-137. DOI:10.1016/j.jisa.2017.06.006
299. Journal of Cybersecurity. Oxford Academic. URL: <https://academic.oup.com/cybersecurity/pages/About>
300. Kahan J.H. Resilience Redux: Buzzword or Basis for Homeland Security. *Homeland Security Affairs*. 2015. URL: www.hsaj.org/articles/1308
301. Kaplan S., Garrick J. On the quantitative definition of risk. *Risk Analysis*. 1981. Vol. 1. P. 11–27. DOI:10.1111/j.1539-6924.1981.tb01350.x
302. Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. *International Journal of Computer Network and Information Security*. 2024. Vol. 16. №. 1. P. 24-34. DOI: <https://doi.org/10.5815/ijcnis.2024.01.02>
303. Kayser V., Knut B. Extending the knowledge base of foresight: The contribution of text mining. *Technological Forecasting and Social Change*. 2017. Vol. 116. P. 208-215.
304. Kekül H., Ergen B., Arslan H. A New Vulnerability Reporting Framework for Software Vulnerability Databases. *International Journal of Education and Management Engineering*. 2021. Vol. 11. No. 3. P. 11-19. DOI: 10.5815/ijeme.2021.03.02
305. Kekül H., Ergen B., Arslan H. Estimating Missing Security Vectors in NVD Database Security Reports. *International Journal of Engineering and Manufacturing*. 2022. Vol. 12. No. 3. P. 1-13. DOI: 10.5815/ijem.2022.03.01
306. Kelly S., Leverett E., Oughton E.J., Copic J., Thacker S., Pant R., Pryor L., Kassara G., Evan T., Ruffle S.J., Tuveson M., Coburn A.W., Ralph D., Hall J.W. *Integrated Infrastructure: Cyber Resiliency in Society. Mapping the Consequences*

of an Interconnected Digital Economy. Cambridge Risk Framework series. Centre for Risk Studies, University of Cambridge. 2016. URL: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf>

307. Korystin O., Svyrydiuk N. Activities of Illegal Weapons Criminal Component of Hybrid Threats. *Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021)*. Series: *Advances in Social Science, Education and Humanities Research*. 22 March 2021. Vol. 170. P. 86-91. DOI: 10.2991/aebmr.k.210320.016

308. Korystin O., Svyrydiuk N., Tkachenko V. Fiscal Security of the State Considering Threats of Macroeconomic Nature. *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL2021)*. Series: *Advances in Social Science, Education and Humanities Research*. 27 August 2021. Vol. 188. P. 65-69. DOI: 10.2991/AEBMR.K.210826.012

309. Korystin O., Svyrydiuk N., Vinogradov A. The Use of Sociological Methods in Criminological Research. *Proceedings of the International Conference on Social Science, Psychology and Legal Regulation (SPL 2021)*. Series: *Advances in Social Science, Education and Humanities Research*. 18 December 2021. Vol. 617. P.1-6. DOI: 10.2991/assehr.k.211218.001

310. Korystin O., Demediuk S., Likhovitskyy Y., Kardashevskyy Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns, *International Journal of Information Technology and Computer Science*. 2025. Vol. 17. No. 2. P.24-35. DOI: <https://doi.org/10.5815/ijitcs.2025.02.03>

311. Kott A., Arnold C. The promises and challenges of continuous monitoring and risk scoring. *IEEE Security & Privacy*. 2013. Vol. 11 (1). P. 90–93. DOI: 10.1109/MSP.2013.19

312. Kovalchuk T.I., Korystin O. Y., Sviridyuk N. P. Hybrid threats in the civil security sector in Ukraine. *Problems of Legality*. 2019. № 147. 163–175. URL: <https://doi.org/10.21564/2414-990x.147.180550>

313. KPI created the first educational cyber incident response team in Ukraine. URL: https://dev.ua/en/news/u-kpi-stvoryly-pershu-v-ukraini-osvitniu-komandu-reahuvannia-na-kiberintsydeny-1769690762?utm_source=chatgpt.com

314. Krasznay C. The Role of Civilian Cybersecurity Companies in Military Cyber Operations. *Land Forces Academy Review*. 2024. Vol. 29 (1). DOI: 10.2478/raft-2024-0001

315. Kshetri N. Pattern of global cyber war and crime: a conceptual framework. *Journal of Information Management*. 2005. Vol. 11 (4). P. 541–562. DOI: <https://doi.org/10.1016/j.intman.2005.09.009>

316. Kuehl D. *From cyberspace to cyberpower: defining the problem*. In: Kramer F., Starr S., Wentz L. (eds.). *Cyberpower and National Security*. Washington DC: National Defense University Press, 2009.

317. Kyiv International Cyber Resilience Forum 2026 (19-20th February). URL: <https://cyberforumkyiv.org/en>

318. Lambrinoudakis C., Gritzalis S., Xenakis C., Katsikas S., Karyda M., Tsochou A. Papadatos K., Rantos K., Pavlosoglou Y., Gasparinatos S., Pantazis A., Zacharis A. Compendium of Risk Management Frameworks with Potential Interoperability. Supplement to the interoperable EU risk management framework report. European Union Agency for Cybersecurity. 2022. URL: <https://op.europa.eu/en/publication-detail/-/publication/8e61634f-afd3-11ec-83e1-01aa75ed71a1/language-en>

319. Layton Timothy P. *Information Security: Design, implementation, measurement, and compliance*. Auerbach Publications. 2016. 260 p.

320. Lei S. The NIST Cybersecurity Framework: overview and potential impacts. *SciTech Lawyer*. 2014. Vol. 10. P. 16–19. URL: https://www.americanbar.org/content/dam/aba/publications/scitech_lawyer/2014/summer/nist_cybersecurity_framework_overview_potential_impacts.pdf

321. Lindelauf R., Borm P., Hamers H. *Understanding Terrorist Network Topologies and Their Resilience Against Disruption*. In: Kock Wiil U. (ed.) *Counterterrorism and Open Source Intelligence*. Springer, Vienna, 2011. P. 61–72. DOI:10.1007/978-3-7091-0388-3_5

322. Linkov I., Kott A. Fundamental Concepts of Cyber Resilience: Introduction and Overview. *Springer*. 2018. URL: https://www.researchgate.net/publication/325461632_Fundamental_Concepts_of_Cyber_Resilience_Introduction_and_Overview

323. Linkov I., Eisenberg D., Bates M., Chang D., Convertino M., Allen J., Flynn S., Seager T. Measurable resilience for actionable policy. *Environmental Science & Technology*. 2013. Vol. 47 (17). P. 10108–10110. DOI: 10.1021/es403443n

324. Linkov I., Eisenberg D., Plourde K., Seager T. P., Allen J., Kott A. Resilience metrics for cyber systems. *Environment Systems and Decisions*. 2013. Vol. 33, No. 4. P. 471–476.

325. Linkov I., Kott A. *Cyber Resilience of Systems and Networks*. Springer International Publishing, 2018. 490 p.

326. Lowrance W.W. *Of Acceptable Risk: Science and the Determination of Safety*. Los Altos, CA: William Kaufmann. 1976. 180 p.

327. Lubis M., Lubis M., Safitra M.F., Fakhurroja H., Muttaqin A. N. Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. *Sensors*. 2025. V. 25(15). P. 4545. URL: <https://doi.org/10.3390/s25154545>

328. Masten A.S. Ordinary magic: resilience processes in development. *American Psychologist*. 2001. Vol. 56(3). P. 227–238. DOI: 10.1037/0003-066X.56.3.227

329. Masten AS. Resilience theory and research on children and families: Past, present, and promise. *Journal of Family Theory & Review*. 2018. Vol. 10(1). P. 12–31.

330. McDaniels T., Chang S., Cole D., Mikawoz J., Longstaff H. Fostering resilience to extreme events within infrastructure systems: Characterizing decision

contexts for mitigation and adaptation. *Global Environmental Change*. 2008. Vol. 18. P. 310–318. DOI: 10.1016/j.gloenvcha.2008.03.001

331. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. 2007. URL: <https://www.first.org/cvss/v2/cvss-v2-guide.pdf>

332. Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks. ENISA. December 2014. URL: <https://www.enisa.europa.eu/sites/default/files/publications/Methodologies%20for%20the%20identification%20of%20Critical%20Information%20Infrastructure%20assets%20and%20services.pdf>

333. Muhammad Noman Khalid, Muhammad Iqbal, Kamran Rasheed, Malik Muneeb Abid. Web Vulnerability Finder (WVF): Automated Black-Box Web Vulnerability Scanner. *International Journal of Information Technology and Computer Science*. 2020. Vol. 12. No. 4. P. 38–46. DOI: 10.5815/ijitcs.2020.04.05

334. Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A., Sadhukhan S.K. Cyber-risk decision models: To insure IT or not? *International Journal of Decision Support Systems*. 2013. Vol. 56. P. 11–26. URL: <http://dx.doi.org/10.1016/j.dss.2013.04.004>

335. Nakashima E. *Israel hacked Kaspersky, then tipped the NSA that its tools had been breached*. The Washington Post, 2017. URL: https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html

336. National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK. 2022. 130 p. URL: https://data.parliament.uk/DepositedPapers/Files/DEP2021-0992/National_Cyber_Strategy_2022.pdf

337. National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. URL:

https://assets.publishing.service.gov.uk/media/5a74c796ed915d502d6caefc/52309_Cm_9161_NSS_SD_Review_web_only.pdf

338. National Security Strategy. White House. 2010. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

339. NATO Defence Ministers agree to enhance collective defence and deterrence. URL: https://www.nato.int/cps/en/natohq/news_132356.htm?selectedLocale=en

340. NATO's Readiness Action Plan. Strategic Benefits and Outstanding Challenges. URL: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-1/Arnold.pdf

341. Nazareth Derek L., Choi Jae. A system dynamics model for information security management. *Information & Management*. 2015. Vol. 52 (1). P. 123-134. DOI: doi.org/10.1016/j.im.2014.10.009

342. NIST. URL: <https://www.nist.gov/cyberframework>

343. NISTEP. URL: https://www.nistep.go.jp/en/?page_id=56

344. OASIS Open. STIX Version 2.1. 2021. URL: <https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>

345. OED Online. Resilience. URL: www.oed.com/view/Entry/163619

346. Olsson L., Jerneck A., Thoren H., Persson J., O'Byrne D. Why resilience is unappealing to social science: Theoretical and empirical investigations of the scientific use of resilience. *Science Advances*. 2015. Vol. 1 (4). DOI: [10.1126/sciadv.1400217](https://doi.org/10.1126/sciadv.1400217)

347. Organizational Resilience – Concepts and Evaluation Method / Robert B. et al. Presses internationales Polytechnique, 2010. 46 p.

348. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. 460 с.

349. OSINT Open Source Intelligence. Теорія та методологія: монографія / Користін О., Демедюк С., Барановський О., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. 304 с.

350. *Overview EU Cyber Resilience Act*. ABB. 2024. 5 p. URL: https://library.e.abb.com/public/c87c6a5acc7443e19a6ed0e4c72d314b/9AKK108471A6145_en_A_Cybersecurity%20Guide%20EU%20CRA.pdf?x-sign=ItWWeq6GekkG8yFqPKIx87Bt%2BNxMtBWxIZYsabwKnmJgnQEwM8sYWMed6ZJt21Lv

351. Park J., Seager T.P., Rao P.S., Convertino M., Linkov I. Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis*. 2013. Vol. 33, No. 3. P. 356–367.

352. Parmadi B.D., Ramli K. Beyond Silos – Unifying Military and Civilian Cyber Threat Intelligence for National Security. *International Journal on Perceptive and Cognitive Computing*. 2026. Vol. 12(1). P. 34–46. DOI:10.31436/IJPCC.V12I1.575

353. Patil A.H., Goveas N., Rangarajan K. Regression Test Suite Prioritization using Residual Test Coverage Algorithm and Statistical Techniques. *International Journal of Education and Management Engineering*. 2016. Vol.6. No.5. P.32-39. DOI: 10.5815/ijeme.2016.05.04

354. Peltier Thomas R. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. New York: Auerbach Publications. 2016. 312 p. DOI: 10.1201/9780849390326

355. Perlroth N., Shane S. How Israel caught Russian hackers scouring the world for U.S. secrets. *The New York Times*, 2017. URL: <https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html>

356. Perrow C. *Normal Accidents: Living with High-Risk Technologies*. BasicBooks, 1984. 366 p. URL: <https://maritimesafetyinnovationlab.org/wp-content/uploads/2021/04/Normal-Accidents-Living-With-High-Risk-Technologies-Perrow.pdf>

357. Petersen R.R., Rhodes C.J., Kock Wiil U. Node Removal in Criminal Networks. *European Intelligence and Security Informatics Conference*. 2011. P. 360–365. DOI: 10.1109/EISIC.2011.57
358. Pitt M. The Pitt review: lessons learned from the 2007 floods. Cabinet Office, London, 2008.
359. POLI.design and Oblo, Service Design Tools, Tools. URL: <https://servicedesigntools.org/tools>
360. Preda M., Popescu V., Argint C., Iancu,N., Raicu G., ENE G. Enhancing Civil-Military Cyber Resilience Lessons from the ECYBRIDGE Tabletop Exercise. *International Journal of Information Security and Cybercrime*. 2025. Vol. XIV (1). P. 11-27. DOI: 10.19107/IJISC.2025.01.01
361. Press L. The Past, Present and Future of the Internet in Cuba. 2011. URL: https://thecubaneconomy.com/articles/2011/10/larry-press-on-the-past-present-and-future-of-the-internet-in-cuba/#_ftn1
362. Prior T., Hagmann J. Measuring resilience: Methodological and political challenges of a trend security concept. *Journal of Risk Research*. 2014. Vol. 17. №. 3. P. 281–298. DOI: 10.1080/13669877.2013.808686
363. Purser S. Standards for cyber security. Volume 35: Best Practices in Computer Network Defense: Incident Detection and Response. Amsterdam: IOS Press, 2014. P. 97–106. DOI:10.3233/978-1-61499-372-8-97
364. Ranjan R., Sahoo G. A new clustering approach for anomaly intrusion detection. *International Journal of Data Mining & Knowledge Management Process*. 2014. Vol. 4. No. 2. P. 29–38. DOI: 10.5121/ijdkp.2014.4203
365. Recommendation on Cyber Resilience (No. 166). IACS. 2020. 57 p. URL: https://www.steamshipmutual.com/sites/default/files/downloads/articles/2020/IACS-Recommendation-on-Cyber-resilience-No-166-2020_04.pdf
366. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU)

2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*. URL: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

367. Resilience. URL: <http://www.merriam-webster.com/dictionary/resilience>

368. Responsible Disclosure Policy. URL: https://elaad.nl/responsible-disclosure-policy/?utm_source=chatgpt.com

369. Richardson G.E. The metatheory of resilience and resiliency. *Journal of Clinical Psychology*. 2002. Vol. 58(3). P. 307–321.

370. Roscoe Pound. *The Need of a Sociological Jurisprudence*. URL: <https://scispace.com/papers/the-need-of-a-sociological-jurisprudence-4zz8f7zfe0>

371. Rosenquist M., Casey T. Prioritizing Information Security Risks with Threat Agent Risk Assessment. *Intel Information Technology*. 2009. URL: https://www.researchgate.net/profile/Timothy-Casey/publication/335589639_Prioritizing_Information_Security_Risks_with_Threat_Agent_Risk_Assessment_TARA/links/5d6eb83c92851c1b3b278279/Prioritizing-Information-Security-Risks-with-Threat-Agent-Risk-Assessment-TARA.pdf

372. Ross R., Graubart R., Bodeau D., McQuaid R. Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Draft NIST Special Publication 800-160, 2018. Vol. 2. 158 p. URL: <https://csrc.nist.gov/files/pubs/sp/800/160/v2/ipd/docs/sp800-160-vol2-draft.pdf>

373. Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says. URL: https://www.reuters.com/technology/cybersecurity/russia-conducted-mass-cyber-attack-ukraines-state-registries-deputy-pm-says-2024-12-19/?utm_source=chatgpt.com

374. Russian Electronic Warfare in Ukraine: Between Real and Imaginable. *Jamestown*. URL: <https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/>

375. S.3414 - CSA2012. 112th Congress (2011-2012). URL: <https://www.congress.gov/bill/112th-congress/senate-bill/3414>

376. Schackelford S., Proia A., Martell B., Craig A. Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. (June 5, 2014). *Texas International Law Journal*. 2015. *Indiana Legal Studies Research Paper*. No. 291. URL: <https://ssrn.com/abstract=2446631>

377. Sędkowski W. Welcome to Cyberwar. URL: https://warsawinstitute.org/welcome-to-cyberwar/?utm_source=chatgpt.com

378. Seligman M.E.P., Csikszentmihalyi M. Positive psychology: An introduction. *American Psychologist*. 2000. Vol. 55(1). P. 5–14.

379. Senge Peter M. The fifth discipline: the art and practice of the learning organization. New York: Doubleday/Currency. 1990.

380. Shan A., Seunghwan M. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. *Sensors*. 2024. Vol. 24(15). URL: <https://doi.org/10.3390/s24154888>

381. Simmons C., Ellis C., Shiva S., Dasgupta D., Wu Q. AVOIDIT: A Cyber Attack Taxonomy. *Computer Science CTIT technical reports series*. 2009. URL: [https://www.researchgate.net/profile/S-Shiva/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy/links/544e58360cf2bca5ce90aebb/AVOIDIT-A-Cyber-Attack-Taxonomy.pdf](https://www.researchgate.net/profile/Shiva/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy/links/544e58360cf2bca5ce90aebb/AVOIDIT-A-Cyber-Attack-Taxonomy.pdf)

382. Smith J.E., Ozcan S. Science and technology foresight baker's dozen: A pocket primer of comparative and combined foresight methods. *Foresight*. 2011. Vol. 13 (2). P. 79-96. DOI: 10.1108/14636681111126265

383. Soodo A., Enbody R. *Targeted cyber attacks. Multi-staged Attacks Driven by Exploits and Malware*. Elsevier. 2014. ISBN 9780128006047

384. Soomro Zahoor Ahmed, Mahmood Hussain Shah, Javed Ahmed Information security management needs more holistic approach: A literature review. *International Journal of Information Management*. (2016). Vol. 36 (2). P. 215-225. DOI:10.1016/j.ijinfomgt.2015.11.009

385. Spanos G., Sioziou A., Angelis L. WIVSS: A New Methodology for Scoring Information Systems Vulnerabilities. *Proceedings of the 17th Panhellenic Conference on Informatics*. 2013. P. 83–90. DOI: 10.1145/2491845.2491871.

386. Standards and Their Stories. How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life / Edited by M. Lampland, S. Leigh Star. Ithaca & London: Cornell University Press, 2009.

387. Sterbenz J.P. G., Hutchison D., Cetinkaya E.K., Jabbar A., Rohrer J.P., Schöller M., Smith P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*. 2010. Vol. 54, No. 8. P. 1245–1265.

388. Stolfo S.J., Bellovin S.M., Keromytis A.D., Hershkop S., Sean W., Smith S.W., Sinclair S. Insider Attack and Cyber Security: Beyond the Hacker. 1-st edition. Boston, MA: Springer. 2008. DOI:10.1007/978-0-387-77322-3

389. Stouffer K., Lightman S., Pillitteri V., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security. 2015. DOI: <https://doi.org/10.6028/NIST.SP.800-82r2>

390. Strengthening Digital Society against Cyber Shocks: Global State of Information Security. Survey 2018. URL: <https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf>

391. Stuxnet. URL: https://en.wikipedia.org/wiki/Stuxnet?utm_source=chatgpt.com

392. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. General Editor Schmitt Michael N. 2nd Edition. Cambridge University Press. 2017.

393. Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press, Cambridge, 2013. URL: <https://scispace.com/pdf/tallinn-manual-on-the-international-law-applicable-to-cyber-1ypzb2oq5n.pdf>

394. Task force report: Resilient Military Systems and the Advanced Cyber Threat. Defense Science Board. 2013. URL: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf>
395. Teach the Future. URL: <https://www.teachthefuture.org/>
396. The Cyber Resilience Act: Summary of the legislative text. An official website of the European Union. URL: <https://digital-strategy.ec.europa.eu/en/policies/cra-summary>
397. The Cyber Resilience Blueprint: A New Perspective on Security. Mountain View: Symantec, 2015.
398. The Global Risks Report 2019, 14th Edition. Geneva: World Economic Forum, 2019. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
399. The NIS2 Directive: A high common level of cybersecurity in the EU. 2023. 13 p. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI\(2021\)689333_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
400. The Strategic Framework for a Cyber Resilient Scotland. Scottish Government. 2021. 39 p. URL: <https://dera.ioe.ac.uk/id/eprint/37463/1/strategic-framework-cyber-resilient-scotland%20%28redacted%29.pdf>.
401. The Third Annual Study on the Cyber Resilient Organization. Traverse City: Ponemon Institute, 2018.
402. The UK's Strategy for Countering Terrorism. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty. July 2011. URL: <https://info.publicintelligence.net/UK-CT-Contest.pdf>
403. Threat Taxonomy. A tool for structuring threat information. ENISA. 2016. URL: <https://www.enisa.europa.eu>
404. Tiirmaa-Klaar H. Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*. 2016. Vol. 1, No. 1. P. 94–106.

405. Tkachov A., Korolov R., Rahimova I., Aksonova I., Sevriukova Y. Cybersecurity challenges and solutions for critical infrastructure protection. *Ukrainian Scientific Journal of Information Security*. 2024. Vol. 30(1). P. 58–66. URL: <https://doi.org/10.18372/2225-5036.30.18604>

406. Traffic Light Protocol (TLP). FIRST Standards Definitions and Usage Guidance — Version 2.0. URL: <https://www.first.org/tlp/>

407. Ukraine Shares Cyber Defense Experience in War at European Parliament Hearings. URL: <https://www.rnbo.gov.ua/en/Diialnist/7392.html>

408. Ukraine's decentralized warfare: the battle of the common person. URL: https://asiatimes.com/2024/11/ukraines-decentralized-warfare-the-battle-of-the-common-person/?utm_source=chatgpt.com

409. United Nations. Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes. 2024.

410. Vanatta N., Johnson B.D. Threatcasting: a framework and process to model future operating environments. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*. 2018. Vol. 16. P. 79 - 88.

411. Vysotska V., Nazarkevych M., Vladov S., Lozynska O., Markiv O., Romanchuk R., Danylyk V. Devising a method for detecting information threats in the Ukrainian cyber space based on machine learning. *Eastern-European Journal of Enterprise Technologies*. 2024. Vol. 6(2 (132)) P. 36–48. URL: <https://doi.org/10.15587/1729-4061.2024.317456>

412. Waller M.A. Resilience in ecosystemic context: Evolution of the concept. *American Journal of Orthopsychiatry*. 2001. Vol. 71(3). P. 290–297. DOI: 10.1037/0002-9432.71.3.290

413. Weidt F., Silva R. Systematic Literature Review in Computer Science-A Practical Guide. *Relatórios Técnicos do DCC/UFJF*. 2016. Vol. 1(8). P. 1-7.

414. Werner E., Smith R.S. *Overcoming the Odds: High Risk Children from Birth to Adulthood*. Ithaca: Cornell University Press. 1992. 280 p.

415. What is Foresight? European Foresight Platform (EFP). URL: <http://www.foresight-platform.eu/community/forlearn/what-is-foresight/>

416. Wheat T., Kirichenko D. Democratization of Irregular Warfare. Emerging Technology and the Russo-Ukrainian War. URL: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Nov-Dec-2024/Democratization-of-Irregular-Warfare/?utm_source=chatgpt.com

417. Wilding N. Cyber resilience: How important is your reputation? How effective are your people? *Business Information Review*. 2016. Vol. 33, No. 2. P. 94–99.

418. Yakoviv I. Model of four cyber attack information environments. Collection. Information Technology and Security. 2023. Вип. 11(2). С. 175–192. URL: <https://doi.org/10.20535/2411-1031.2023.11.2.293768>

419. Yakoviv I., Sharadkin D., Kulikov V. Cyber threat information intelligence integration models. *Collection «Information Technology and Security»*. 2025. Вип. 13 (2). С. 236–252. URL: <https://doi.org/10.20535/2411-1031.2025.13.2.344710>

420. Yoon J., Kyungho L. Advanced assessment model for improving effective ness of information security measurement. *International Journal of Advanced Media and Communication*. 2016. Vol. 6 (1). P. 4-19.

421. Zero Trust Architecture. NIST. Special Publication 800-207. 2020. 59 p. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

422. Zhang D.J. Integrating Cyber Security into Nuclear Digital I&C Safety Systems. *18th International Conference on Nuclear Engineering*. Vol. 1. P. 897-901. DOI: 10.1115/ICONE18-30345

423. Zollo M., Winter S. Deliberate learning and the evolution of dynamic capabilities. *Organization science*. 2002. Vol.13. № 3 (3). P. 339–351.

424. Zybin S., Bielozorova Y., Risk-based Decision-making System for Information Processing Systems. *International Journal of Information Technology and Computer Science*. 2021.Vol.13.No.5. P.1-18. DOI: 10.5815/ijitcs.2021.05.01

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати

дисертації

Монографії

1. Демедюк С.В. Розділ 26. Кібервійна та форсайт кіберстійкості. Реалізація філософії ІЛР в системі кримінального аналізу Національної поліції України: монографія / О.Є. Користін, Б.А. Денисенко, С.В. Демедюк та ін. ; за заг. ред. д-ра юрид. наук, проф. О.Є. Користіна. Київ: ВАЙТЕ, 2024. С. 343-357. DOI: <https://doi.org/10.36486/978-966-2310-66-5-26>

2. Демедюк С.В. Розділ 1. Стратегічний ландшафт застосування OSINT в секторі національної безпеки. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. С. 21-36.

Статті у наукових періодичних виданнях інших держав, у тому числі проіндексованих у базах даних Web of Science Core Collection, Scopus

1. Demedyuk S.V., Demedyuk T.S. Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. 2018. Vol. 68 № 6. P. 278-290. DOI: 10.33407/itlt.v68i6.2582 (WoS)

2. Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. *International Journal of Computer Network and Information Security*. 2024. Vol. 16. №. 1. P. 24-34. DOI: <https://doi.org/10.5815/ijcnis.2024.01.02> (Scopus Q3)

3. Korystin O., Demediuk S., Sviridyuk N., Mitina O., Aleksander M., Yuriy Kardashevskyy. Risk Forecasting of Information-content-security. *Cyber Hygiene & Conflict Management in Global Information Networks*: Proceedings of the Third

International Conference on Cyber Hygiene & Conflict Management in Global Information Networks. 2025. Vol. 3925. P. 273–280. (Scopus Q4)

4. Korystin O., Demediuk S., Likhovitsky Y., Kardashevsky Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns. *International Journal of Information Technology and Computer Science*. 2025. Vol. 17. No. 2. P. 24-35. DOI: <https://doi.org/10.5815/ijitcs.2025.02.03> (Scopus Q3)

5. Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*. (2025). Vol. 17. Is. 19. P. 8757. <https://doi.org/10.3390/su17198757> (Scopus Q1)

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

6. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона*. 2023. № 1(59). С.77-85. DOI: [https://doi.org/10.36486/np.2023.1\(59\).8](https://doi.org/10.36486/np.2023.1(59).8)

7. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона*. 2023. № 2(60). С.78-85. DOI: [https://doi.org/10.36486/np.2023.2\(60\).8](https://doi.org/10.36486/np.2023.2(60).8)

8. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59. DOI: <https://doi.org/10.32850/sulj.2023.3.10>

9. Демедюк С.В. Захист критично важливих послуг у цифрову епоху. *Наука і правоохорона*. 2023. № 3(61). С.26-34 DOI (Issue): [https://doi.org/10.36486/np.2023.3\(61\).3](https://doi.org/10.36486/np.2023.3(61).3)

10. Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету*

ДВНЗ «Ужгородський національний університет». 2023. №06. С. 708-713.

DOI: <https://doi.org/10.24144/2788-6018.2023.06.122>

11. Демедюк С.В. Інституціоналізація кіберстійкості. *Наука і правоохорона*. 2023. № 4(62). С.31-41.

DOI: [https://doi.org/10.36486/np.2023.4\(62\).4](https://doi.org/10.36486/np.2023.4(62).4)

12. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. *Наука і правоохорона*. 2024. № 1(63). С.133-141.

DOI: [https://doi.org/10.36486/np.2024.1\(63\).13](https://doi.org/10.36486/np.2024.1(63).13)

13. Демедюк С.В. OSINT в контексті кібербезпеки. *Юридичний бюлетень*. 2024. № 34. С.200-207. DOI:10.32850/LB2414-4207.2024.34.26

14. Демедюк С.В. OSINT в контексті виявлення та запобігання кіберзлочинам. *Південноукраїнський правничий часопис*. 2024. № 4. С. 38-41.

DOI: <https://doi.org/10.32850/sulj.2024.4.7>

15. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154. DOI: [https://doi.org/10.36486/np.2024.3\(65\).12](https://doi.org/10.36486/np.2024.3(65).12)

16. Демедюк С.В. Зміст та особливості експертної вибірки в оцінюванні кіберризиків. *Морська безпека та оборона*. 2025. №1. С.17-24.

DOI: <https://doi.org/10.32782/msd/2025.1/03>

17. Демедюк С.В. Сучасні тенденції on-line шахрайства в Україні. *Право і суспільство*. 2025. №4. Т. 2. С. 186-194. DOI: <https://doi.org/10.32842/2078-3736/2025.4.2.28>

18. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. *Правові новели*. 2025. № 26. 157-166.

DOI: <https://doi.org/10.32782/ln.2025.26.18>

Наукові праці, які засвідчують апробацію матеріалів дисертації

1. Демедюк С.В. Стійкість системи кібербезпеки та її правове забезпечення в Україні. *Закарпатські правові читання: збірник тез за*

матеріалами XV міжнародної науково-практичної конференції (Ужгород, 27 квітня 2023 р.). Ужгород: УжНУ, 2023. С. 5-7.

2. Демедюк С.В. Захист критично важливої інформаційної інфраструктури в системі кібербезпеки. *Стратегії безпеки підприємництва в умовах воєнного стану*: Збірник тез за матеріалами XIV міжнародної науково-практичної конференції «Безпекотворення: питання теорії, практики та правові аспекти» (Київ, 06 квітня 2023 р.) / за ред. Тимошенко О.І., Київ: Видавництво Європейського університету», 2023. С. 26-27.

3. Демедюк С.В. Розбудова кіберстійкості на національному рівні. *Актуальність та особливості наукових досліджень в умовах воєнного стану*: збірник матеріалів III Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки – 2023 в Україні (Київ, 23 травня 2023 р.). Київ: ДНДІ МВС України, 2023. С. 133-134.

4. Демедюк С.В. Актуалізація сучасних методологій аналізу кіберзлочинності. *Стан та перспективи розвитку адміністративного права України*: матеріали X міжнародної науково-практичної інтернет-конференції (Одеса, 20 жовтня 2023 р.). Одеса: ОДУВС. С. 63-66.

5. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення*: матеріали науково-практичного круглого столу (Київ, 26 вересня 2023 р.) / [Редкол.: Вербенський М. Г., Опришко І. В., Кулик О. Г. та ін.]. Київ : ДНДІ МВС України, 2023. С. 168-170.

6. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції. (Київ, 17 листопада 2023 р.). Київ: НАВС. С.40-44.

7. Демедюк С.В. Захист критично важливих кібер-активів. *Кібербезпека в Україні: правові та організаційні питання*: збірник матеріалів міжнародної науково-практичної конференції (Одеса, 17 листопада 2023 р.). Одеса: ОДУВС. С.55-57.

8. Демедюк С.В. Показники кіберстійкості. *Актуальні питання забезпечення безпекового середовища в Україні: збірник тез наукових доповідей Всеукраїнської науково-практичної конференції* (Київ, 19 квітня 2024 р.). Київ: ДНДІ МВС України, 2024. С.38-41.

9. Демедюк С.В. Щодо питань розвитку кіберстійкості. *Актуальність та особливості наукових досліджень в умовах воєнного стану: збірник матеріалів IV Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки-2024 в Україні* (Київ, 22 травня 2024 р.). Київ: ДНДІ МВС України, 2024. С.19-21.

10. Демедюк С.В. Використання злочинцями комп'ютерних систем та мереж. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки: збірник матеріалів всеукраїнської науково-практичної конференції* (Київ, 27 вересня 2024 р.). Київ: ДНДІ. С. 203-207.

11. Демедюк С.В. Особливості онлайн шахрайства в Україні. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України: матеріали міжвідомчої науково-практичної конференції* (Київ, 01 листопада 2024 р.). Київ: НАВС, 2024. С. 35-38.

12. Демедюк С.В. Поширення та характерні складові кіберзалежних злочинів. *Протидія організованим злочинності і корупції в умовах збройного конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ: збірник матеріалів Міжнародної науково-практичної конференції* (Кропивницький, 04 жовтня 2024 року). Кропивницький: ДонДУВС, 2024. С. 268-273.

13. Демедюк С.В. Інтеграція OSINT в систему кібербезпеки держави: стратегічні та прикладні аспекти. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України: матеріали круглого столу* (Львів, 07 травня 2025 р.). Львів: ЛьвДУВС, 2025. С. 58-61.

Додаток Б

Акти впровадження



НАРОДНИЙ ДЕПУТАТ УКРАЇНИ

вул. М. Грушевського, 5, м. Київ, 01008, www.rada.gov.ua**ДОВІДКА
про впровадження результатів дисертаційної роботи
Демедюка Сергія Васильовича**

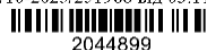
Довідка дана про те, що теоретичні висновки та практичні рекомендації, що містяться в дисертаційній роботі Демедюка Сергія Васильовича за темою «Організаційно-правові та кримінологічні засади кіберстійкості в Україні», використані при розробленні законопроекту № 12207 «Проект Закону про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки».

**народний депутат України,
Голова підкомітету з питань безпеки у
кіберпросторі, урядового зв'язку,
криптографічного захисту інформації Комітету
Верховної Ради України з питань національної
безпеки, оборони та розвідки**

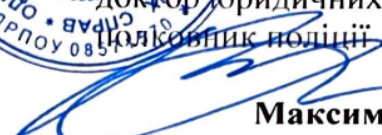
Олександр ФЕДІЄНКО

ЕАС ВЕРХОВНОЇ РАДИ УКРАЇНИ
Підписувач: Федієнко Олександр Павлович
Сертифікат: 3FAA92883581EC00304000000F8032F00709D0C00
Дійсний до: 12.12.2026 0:00:00

Апарат Верховної Ради України
89д9/10-2025/251968 від 03.11.2025



2044899


ЗАТВЕРДЖУЮ
 Перший проректор Одеського державного університету внутрішніх справ
 доктор юридичних наук, професор
 полковник поліції

Максим КОРНІЄНКО
 «15» 01 2026р.

АКТ
впровадження в наукову діяльність Одеського державного університету
внутрішніх справ результатів дисертаційного дослідження
Демедюка Сергія Васильовича на тему: «Організаційно-правові та
кримінологічні засади кіберстійкості в Україні»

«15» 01 2026 року

м. Одеса

Комісія у складі:

- 1) начальника відділу організації наукової діяльності ОДУВС, кандидата юридичних наук, доцента Домброван Наталії;
- 2) ученого секретаря секретаріату Вченої ради ОДУВС, кандидата педагогічних наук Ісаєнка Максима;
- 3) начальника відділу аспірантури (ад'юнктури) і докторантури ОДУВС, кандидата юридичних наук Теслюк Ірини

склала цей акт з приводу того, що комісією розглянуто матеріали дисертаційного дослідження Демедюка Сергія Васильовича на тему: «Організаційно-правові та кримінологічні засади кіберстійкості в Україні», які, зокрема, відображені у наукових публікаціях:

1. Демедюк С.В. Розділ 26. Кібервійна та форсайт кіберстійкості. Реалізація філософії ІЛР в системі кримінального аналізу Національної поліції України: монографія / О.Є. Користін, Б.А. Денисенко, С.В. Демедюк та ін. ; за заг. ред. д-ра юрид. наук, проф. О.Є. Користіна. Київ: ВАЙТЕ, 2024. С. 343-357. DOI: <https://doi.org/10.36486/978-966-2310-66-5-26>.
2. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Львів. 304 с.
3. Демедюк С.В. Розділ 1. Стратегічний ландшафт застосування OSINT в секторі національної безпеки. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Львів. С. 21-36.
4. Demedyuk, Serhii V. and Demedyuk, Tetyana S. (2018). Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. Vol. 68 № 6. Pp.278-290. DOI: 10.33407/itlt.v68i6.2582.

5. Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. (2024). Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Set Theory. *International Journal of Computer Network and Information Security*, Vol. 16. №. 1. P. 24-34. DOI: <https://doi.org/10.5815/ijcnis.2024.01.02>.
6. Oleksandr Korystin, Serhii Demediuk, Nataliia Sviridyuk, Olena Mitina, Marek Aleksander, Yuriy Kardashevskyy (2025). Risk Forecasting of Information-content-security. Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks. CEUR Workshop Proceedings (January 24–27, 2024) (CEUR-WS.org ISSN 16130073). Vol. 3925. P. 273–280. <https://ceur-ws.org/Vol-3925/short02.pdf>.
7. Oleksandr Korystin, Serhii Demediuk, Yaroslav Likhovitskyy, Yuriy Kardashevskyy, Olena Mitina (2025). Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns. *International Journal of Information Technology and Computer Science*. Vol. 17. No. 2. Pp.24-35. DOI: <https://doi.org/10.5815/ijitcs.2025.02.03>.
8. Korchenko, O.; Korystin, O.; Shulha, V.; Kazmirchuk, S.; Demediuk, S.; Zybin, S. (2025). Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*. 17(19), 8757. <https://doi.org/10.3390/su17198757>.
9. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона*. 2023. № 1(59). С.77-85. DOI: [https://doi.org/10.36486/np.2023.1\(59\).8](https://doi.org/10.36486/np.2023.1(59).8).
10. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона*. 2023. № 2(60). С.78-85. DOI: [https://doi.org/10.36486/np.2023.2\(60\).8](https://doi.org/10.36486/np.2023.2(60).8).
11. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59. DOI <https://doi.org/10.32850/sulj.2023.3.10>.
12. Демедюк С.В. Захист критично важливих послуг у цифрову епоху. *Наука і правоохорона*. 2023. № 3(61). С.26-34 DOI (Issue): [https://doi.org/10.36486/np.2023.3\(61\).3](https://doi.org/10.36486/np.2023.3(61).3).
13. Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет»*. 2023. № 06. С. 708-713. DOI: <https://doi.org/10.24144/2788-6018.2023.06.122>.
14. Демедюк С.В. Інституціоналізація кіберстійкості. *Наука і правоохорона*. 2023. № 4 (62). С.31-41. DOI: [https://doi.org/10.36486/np.2023.4\(62\).4](https://doi.org/10.36486/np.2023.4(62).4).
15. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. *Наука і правоохорона*. 2024. № 1 (63). С.133-141. DOI: [https://doi.org/10.36486/np.2024.1\(63\).13](https://doi.org/10.36486/np.2024.1(63).13).
16. Демедюк С.В. OSINT в контексті кібербезпеки. *Юридичний бюлетень*. № 34. 2024. С.200-2007. DOI:10.32850/LB2414-4207.2024.34.26
17. Демедюк С.В. OSINT в контексті виявлення та запобігання кіберзлочинам. *Південноукраїнський правничий часопис*. 2024. № 4. С. 38-41. DOI: <https://doi.org/10.32850/sulj.2024.4.7>.
18. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154. DOI: [https://doi.org/10.36486/np.2024.3\(65\).12](https://doi.org/10.36486/np.2024.3(65).12).

19. Демедюк С.В. Зміст та особливості експертної вибірки в оцінюванні кіберризиків. *Морська безпека та оборона*. 2025. №1. С.17-24. DOI: <https://doi.org/10.32782/msd/2025.1/03>.

20. Демедюк С.В. Сучасні тенденції on-line шахрайства в Україні. *Право і суспільство*. 2025. №4. Т. 2 С. 186-194. <https://doi.org/10.32842/2078-3736/2025.4.2.28>.

21. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. *Правові новели*. 2025. № 26. 2663-5631. <https://doi.org/10.32782/ln.2025.26.18>.

Комісія вважає, що представлені матеріали, отримані на основі проведеного самостійного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, можуть бути використані в науковій діяльності Одеського державного університету внутрішніх справ, зокрема, під час реалізації теми науково-дослідних і дослідно-конструкторських робіт Одеського державного університету внутрішніх справ «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі», № 0123U103538, а також теми науково-дослідної роботи кафедри кримінально-правових дисциплін інституту права та безпеки «Забезпечення кримінально-правової діяльності суб'єктів запобігання кримінальним правопорушенням в інтересах кримінального судочинства» (№ 0124U004215), теми науково-дослідної роботи кафедри кримінального аналізу та інформаційних технологій «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період» (№0123U103748).

Члени комісії:

**Начальник відділу організації
наукової діяльності ОДУВС**
кандидат юридичних наук, доцент
підполковник поліції



Наталія ДОМБРОВАН

**Учений секретар секретаріату
Вченої ради ОДУВС**
кандидат педагогічних наук



Максим ІСАЄНКО

**Начальник відділу аспірантури
(ад'юнктури) і докторантури ОДУВС,**
кандидат юридичних наук



Ірина ТЕСЛЮК

ЗАТВЕРДЖУЮ

Перший проректор Одеського державного університету
внутрішніх справ
доктор юридичних наук, професор
підполковник поліції

Максим КОРНІЄНКО

«15» 01 2026р.

АКТ

**впровадження в освітній процес Одеського державного університету
внутрішніх справ результатів дисертаційного дослідження
Демедюка Сергія Васильовича на тему: «Організаційно-правові та
кримінологічні засади кіберстійкості в Україні»**

«15» 01 2026р.

м. Одеса

Комісія у складі:

- 1) начальника відділу забезпечення якості освіти ОДУВС, кандидата історичних наук, доцента Камінської Олени;
- 2) завідувача кафедри кримінально-правових дисциплін інституту права та безпеки ОДУВС, доктора юридичних наук, професора Бабенка Андрія,
- 3) завідувача кафедри кримінального аналізу та інформаційних технологій ОДУВС, кандидата юридичних наук, доцента підполковника поліції Форос Ганни

склала цей акт з приводу того, що комісією розглянуто матеріали дисертаційного дослідження Демедюка Сергія Васильовича на тему: «Організаційно-правові та кримінологічні засади кіберстійкості в Україні», які, зокрема, відображені у наукових публікаціях:

1. Демедюк С.В. Розділ 26. Кібервійна та форсайт кіберстійкості. Реалізація філософії ІЛР в системі кримінального аналізу Національної поліції України: монографія / О.Є. Користін, Б.А. Денисенко, С.В. Демедюк та ін. ; за заг. ред. д-ра юрид. наук, проф. О.Є. Користіна. Київ: ВАЙТЕ, 2024. С. 343-357. DOI: <https://doi.org/10.36486/978-966-2310-66-5-26>.

2. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Львів. 304 с.

3. Демедюк С.В. Розділ 1. Стратегічний ландшафт застосування OSINT в секторі національної безпеки. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Львів. С. 21-36.

4. Demedyuk, Serhii V. and Demedyuk, Tetyana S. (2018). Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. Vol. 68 № 6. Pp.278-290. DOI: 10.33407/itlt.v68i6.2582.
5. Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. (2024). Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Set Theory. *International Journal of Computer Network and Information Security*, Vol. 16. №. 1. P. 24-34. DOI: <https://doi.org/10.5815/ijcnis.2024.01.02>.
6. Oleksandr Korystin, Serhii Demediuk, Nataliia Sviridyuk, Olena Mitina, Marek Aleksander, Yuriy Kardashevskyy (2025). Risk Forecasting of Information-content-security. Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks. CEUR Workshop Proceedings (January 24–27, 2024) (CEUR-WS.org ISSN 16130073). Vol. 3925. P. 273–280. <https://ceur-ws.org/Vol-3925/short02.pdf>.
7. Oleksandr Korystin, Serhii Demediuk, Yaroslav Likhovitsky, Yuriy Kardashevskyy, Olena Mitina (2025). Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns. *International Journal of Information Technology and Computer Science*. Vol. 17. No. 2. Pp.24-35. DOI: <https://doi.org/10.5815/ijitcs.2025.02.03>.
8. Korchenko, O.; Korystin, O.; Shulha, V.; Kazmirchuk, S.; Demediuk, S.; Zybin, S. (2025). Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*. 17(19), 8757. <https://doi.org/10.3390/su17198757>.
9. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона*. 2023. № 1(59). С.77-85. DOI: [https://doi.org/10.36486/np.2023.1\(59\).8](https://doi.org/10.36486/np.2023.1(59).8).
10. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона*. 2023. № 2(60). С.78-85. DOI: [https://doi.org/10.36486/np.2023.2\(60\).8](https://doi.org/10.36486/np.2023.2(60).8).
11. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59. DOI <https://doi.org/10.32850/sulj.2023.3.10>.
12. Демедюк С.В. Захист критично важливих послуг у цифрову епоху. *Наука і правоохорона*. 2023. № 3(61). С.26-34 DOI (Issue): [https://doi.org/10.36486/np.2023.3\(61\).3](https://doi.org/10.36486/np.2023.3(61).3).
13. Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет»*. 2023. № 06. С. 708-713. DOI: <https://doi.org/10.24144/2788-6018.2023.06.122>.
14. Демедюк С.В. Інституціоналізація кіберстійкості. *Наука і правоохорона*. 2023. № 4 (62). С.31-41. DOI: [https://doi.org/10.36486/np.2023.4\(62\).4](https://doi.org/10.36486/np.2023.4(62).4).

15. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. *Наука і правоохорона*. 2024. № 1 (63). С.133-141. DOI: [https://doi.org/10.36486/np.2024.1\(63\).13](https://doi.org/10.36486/np.2024.1(63).13).

16. Демедюк С.В. OSINT в контексті кібербезпеки. *Юридичний бюлетень*. № 34. 2024. С.200-2007. DOI:10.32850/LB2414-4207.2024.34.26

17. Демедюк С.В. OSINT в контексті виявлення та запобігання кіберзлочинам. *Південноукраїнський правничий часопис*. 2024. № 4. С. 38-41. DOI: <https://doi.org/10.32850/sulj.2024.4.7>.

18. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154. DOI: [https://doi.org/10.36486/np.2024.3\(65\).12](https://doi.org/10.36486/np.2024.3(65).12).

19. Демедюк С.В. Зміст та особливості експертної вибірки в оцінюванні кіберризиків. *Морська безпека та оборона*. 2025. №1. С.17-24. DOI: <https://doi.org/10.32782/msd/2025.1/03>.

20. Демедюк С.В. Сучасні тенденції on-line шахрайства в Україні. *Право і суспільство*. 2025. №4. Т. 2 С. 186-194. <https://doi.org/10.32842/2078-3736/2025.4.2.28>.

21. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. *Правові новели*. 2025. № 26. 2663-5631. <https://doi.org/10.32782/ln.2025.26.18>.

Комісія вважає, що представлені матеріали, отримані на основі проведеного самостійного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, можуть бути використані в освітньому процесі Одеського державного університету внутрішніх справ, зокрема, під час викладання навчальних дисциплін «Кримінально-правова та кримінологічна характеристика кіберзлочинності», «Інформаційна та кібернетична безпека», «Кримінальний аналіз», «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції», «Протидія кіберзлочинності», при підготовці відповідних розділів підручників, навчальних посібників, програм, проведенні занять з професійної підготовки працівників оперативних підрозділів Національної поліції України.

Члени комісії:

**Начальник відділу
забезпечення якості освіти
кандидат історичних наук, доцент**



Олена КАМІНСЬКА

**Завідувач кафедри кримінально-правових
дисциплін інституту права та безпеки
доктор юридичних наук, професор**



Андрій БАБЕНКО

**Завідувач кафедри кримінального аналізу
та інформаційних технологій
кандидат юридичних наук, доцент
підполковник поліції**



Ганна ФОРОС

Додаток В

Система кіберстійкості в Україні

Опитувальник складено з метою проведення стратегічного аналізу кіберстійкості в Україні на основі оцінки ризиків поширення кіберзагроз, спроможностей щодо протидії їм, а також формування системи кіберстійкості в Україні.

Відповіді на запитання є **виключно конфіденційними** і не потребують розкриття персональних даних опитуваних.

При оцінюванні важливим є *відображення власного досвіду* та обізнаності опитуваного *із акцентом на специфіці регіону, сектору діяльності, місця роботи* тощо.

Дякуємо за вашу участь в опитуванні! Ваша експертна оцінка є важливою!

№ З/П	ЗАГАЛЬНА ІНФОРМАЦІЯ	
1.	Який суб'єкт (орган) Ви представляєте	Державний орган - рівень: - центральний, - обласний, - районний Установа (підприємство, організація) - форма власності: - державна - приватна - змішана (державна присутня частково) <u>інтерактивний вибір суб'єкта</u> • Національний координаційний центр кібербезпеки (РНБО) • Кабінет міністрів України • міністерство або інший центральний орган виконавчої влади • Державна служба спеціального зв'язку та захисту інформації України • обласна військова адміністрація • районна військова адміністрація • правоохоронний орган • розвідувальний орган • контррозвідувальний орган • постачальник ІКТ послуг • критична інфраструктура • громадська організація • освітня (наукова) установа • інше (зазначити)
2.	Регіон	<u>інтерактивний вибір регіону</u> • АР Крим • Вінницька область • Волинська область • Донецька область • Дніпропетровська область

		• Житомирська область • Закарпатська область • Запорізька область • Івано-Франківська область • м. Київ • Київська область • Кіровоградська область • Луганська область • Львівська область • Миколаївська область • Одеська область • Полтавська область • Рівненська область • Сумська область • Тернопільська область • Харківська область • Херсонська область • Хмельницька область • Черкаська область • Чернівецька область • Чернігівська область
3.	Стать	<i>чоловік, жінка</i>
	Галузь вашої діяльності	державне управління енергетичний комплекс фінанси/банки/страхування інфраструктура/транспортна система телекомунікаційні послуги цифрові послуги оборонно-промисловий комплекс правоохоронна сфера держбезпека освіта/наука інші
4.	За посадою:	<u>інтерактивний вибір</u> • керівник, заступник керівника (департамент, управління, відділ, сектор тощо) • фахівець (радник, інспектор тощо) • оперативний співробітник (слідчий, детектив) • аналітик • інше (зазначити)
5.	Досвід діяльності за фахом кібербезпеки:	до 1 року 1-3 3-10 10-20 понад 20
6.	Рівень обізнаності у питаннях кібербезпеки (на власну думку):	високий середній

		низький
7.	Освіта	<u>інтерактивний вибір</u> технічна юридична економічна державна безпека державне управління інша (зазначити)

Індикатори, що характеризують кіберзагрози

№ З/П	КІБЕРЗАГРОЗИ – наявні та потенційно можливі явища (дії), що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. <i>За кожним індикатором оцінюється ймовірність його прояву в Україні у теперішній час та можливі наслідки</i>	ЙМОВІР НІСТЬ			МОЖЛИВІ НАСЛІДКИ			
		висока	середня	низька	катастрофа	критичний стан	тяжкий стан	незначні наслідки
1.	Кіберзагрози класифіковані за порушенням базових характеристик захищеності (безпеки):	x	x	x	x	x	x	x
1.1.	порушення конфіденційності (розголошення даних)							
1.2.	порушення цілісності (неавторизована модифікація)							
1.3.	порушення доступності (недоступні сервіси)							
1.4.	порушення достовірності (не істинні / не коректні дані)							
1.5.	порушення надійності (система не може виконувати функцію / функції)							
1.6.	порушення спостережуваності (не можливо визначити поточний стан системи)							
1.7.	відмова від авторства (не достовірні дані щодо користувача / автора)							
2.	Я вважаю, що можу бути експертом (певного рівня) щодо аналізу кіберзагроз	ТАК			НІ			
3.	Кібератаки за видами:	x	x	x	x	x	x	x
3.1.	Шкідливе програмне забезпечення (Malware)							
3.2.	Веб-атаки (Web-based Attacks)							
3.3.	Фішинг (Phishing)							
3.4.	Атаки на веб-додатки (Web application attacks)							
3.5.	Спам (Spam)							
3.6.	Атака на відмову в обслуговуванні (Denial of service)							
3.7.	Крадіжки особистих даних (Identity theft)							
3.8.	Злом (порушення) даних (Data breaches)							
3.9.	Інсайдерська загроза (Insider threat)							
3.10.	Ботнети (Botnets)							

3.11.	Фізичне втручання, пошкодження, крадіжки та втрати (Physical manipulation, damage, theft and loss)								
3.12.	Витік інформації (Information leakage)								
3.12.	Програма вимагач (Ransomware)								
3.14.	Кібершпигунство (Cyberespionage)								
3.15.	Криптоджекінг (шкідливий майнінг) (Cryptojacking)								
4.	Кібератаки								
4.1.1.	4.1. на об'єкти	телекомунікаційних послуг							
4.1.2.		транспортної системи							
4.1.3.		енергетичного комплексу							
4.1.4.		забезпечення питною водою							
4.1.5.		суспільно важливих інформаційних ресурсів							
4.1.6.		системи управління технологічними процесами							
4.1.7.		органів державної влади							
4.1.8.		фінансового та банківського сектору							
4.1.9.		оборонно-промислового комплексу							
4.1.10.		державної безпеки							
4.1.11.		правоохоронних органів							
4.2.	Територія походження кібератак:		x	x	x	x	x	x	x
4.2.1.	російська федерація								
4.2.2.	ТОТ АР Крим								
4.2.3.	ТОТ Донецької області								
4.2.4.	ТОТ Луганської області								
4.2.5.	ТОТ Запорізької області								
4.2.6.	ТОТ Херсонської області								
4.2.7.	республіка білорусь								
4.2.8.	Європа								
4.2.9.	Азія								
4.2.10.	Африка								
4.2.11.	інші (вказати)								
4.3.	Суб'єкти, які здійснюють (ініціюють) кібератаки:		x	x	x	x	x	x	x
4.3.1.	держава-спонсор								
4.3.2.	кіберзлочинці								
4.3.3.	хакери-найманці								
4.3.4.	хакери, що входять до міжнародних злочинних угруповань								
4.3.5.	хактивісти								
4.3.6.	інші (зазначити)								
5.	Я маю достатній фаховий рівень щодо суджень про кіберзагрози		НІ			ТАК			
6.	Використання кібератак як елементу гібридної війни проти України з метою:								
6.1	з метою:		x	x	x	x	x	x	x
6.1.1.	зниження світової підтримки України								
6.1.2.	дискредитації військово-політичного керівництва України								

6.1.3.	інспірування міжнародних конфліктів на кордонах України								
6.1.4.	інспірування міжнародного тиску на Україну								
6.1.5.	інспірування розколу в українській владі								
6.1.7.	поширення в світі ідей т.зв. «руського світу»								
7.	Використання кібератак у якості деструктивних інформаційно-психологічних операцій (ІПСО) з метою:								
7.1.	з метою:		x	x	x	x	x	x	x
7.1.1	дискредитації органів влади та підриву владних повноважень								
7.1.2	соціально-політичної поляризації суспільства								
7.1.3	інспірування суспільної недовіри до органів влади								
7.1.4	негативного впливу на настрої в українському суспільстві								
7.1.5	підбурювання до акцій громадянської непокорі (демонстрації, мітинги)								
7.1.6	дискредитації СОУ								
7.1.7	деморалізації о/с СОУ								
7.1.8	поширення антиукраїнських настроїв								
7.1.9	розпалювання міжнаціональної ворожнечі								
7.1.10	розпалювання міжрелігійної ворожнечі								
7.1.11	розповсюдження проросійського наративу								
7.1.12	нагнітання соціально-економічної напруги через економічні інструменти								
7.1.13.	провокації порушення громадського порядку								
8.	Я вважаю, що маю достатній експертний рівень, щодо характеристики кібертероризму проти України		ТАК			НІ			
9.	Кібертероризм росії проти України								
9.1.1.	9.1. з метою	завдання шкоди інформаційним системам, комп'ютерним та телекомунікаційним мережам							
9.1.2.		створення надзвичайної ситуації техногенного характеру							
9.1.3.		блокування роботи систем життєзабезпечення							
9.1.4.		створення кризових явищ у певних галузях або сферах							
9.1.5.		масової загибелі людей							
9.1.6.		порушення стабільності в суспільстві							
9.1.7.		викликання широкого суспільного резонансу та розголосу							

9.1.8.		викликання соціального невдоволення							
9.1.9.		злякування населення, створення атмосфери незахищеності та загрози повторення акту кібертероризму							
10.	Поширення кіберзлочинності								
10.1.	у сфері комп'ютерних систем								
10.2.	у сфері обігу протиправного контенту і телекомунікацій								
10.3.	у банківській сфері								
10.4.	у сфері шахрайств								
10.5.	Шахрайства з платежами: без використання банківської картки								
10.6.	Шахрайства з платежами: з використанням банківської картки								
10.7.	Відмивання коштів з використанням ІТ технологій та кіберпростору								
10.8.	Фінансування тероризму з використанням ІТ технологій та кіберпростору								
11.	Кіберзагрози навмисного характеру (майбутній тренд)		x	x	x	x	x	x	x
11.1.	компрометація ланцюжка поставок програмних засобів (збільшення інтеграції компонентів і сервісів, об'єднаних у нові продукти)								
11.2.	просунуті кампанії з дезінформації / операцій впливу								
11.3.	зростання авторитаризму цифрового нагляду / втрата приватності (розпізнавання обличчя у публічній сфері, посилення цифрового нагляду на інтернет-платформах або запровадження цифрової ідентичності, індивідуальні свободи можуть бути обмежені заради безпеки та захисту)								
11.4.	людські помилки та застарілі системи в кіберфізичних екосистемах (швидке впровадження IoT і постійний дефіцит навичок)								
11.5.	цілеспрямовані атаки (наприклад, програми-вимагачі), посилені даними зі смарт-пристроїв								
11.6.	гібридизація загроз (використання одночасної комбінації методів для отримання початкового доступу, включаючи збір великих даних для адаптації своїх фішингових кампаній, машинне навчання для інтерпретації даних, розробку нових інструментів для обходу захисних механізмів і поєднання фізичного й віртуального для здійснення атак)								
11.7.	дефіцит навичок (зловмисники аналізують організаційні навички та недоліки, щоб отримати уявлення про слабкі місця в захисті, потенційні вразливості та можливості для використання їхніх систем і мереж)								

11.8.	транскордонні постачальники послуг ІКТ як єдина точка відмови (провайдери ІКТ-послуг та їхня інфраструктура, включаючи супутникові технології, є основою суспільства і тому можуть стати мішенню для терористів і злочинних угруповань)							
11.9.	зловживання штучним інтелектом (ШІ може бути використаний для посилення багатьох нечесних дій, таких як створення дезінформації та фейкового контенту, використання упереджень, збір біометричних та інших конфіденційних даних, створення військових роботів, отруєння даних тощо)							

Індикатори, що характеризують інституційну спроможність кіберсистеми та кіберстійкість в Україні

№ 3/П	Спроможності - індикатори, що характеризують здатність протидії кіберзагрозам, ефективність системи кібербезпеки в Україні та впливають на зниження ризиків поширення кіберзагроз. Кіберстійкість - розглядається як суспільно-культурний феномен, який полягає у спроможності суспільства досягати та в надзвичайних ситуаціях демонструвати високий рівень культури безпеки у кіберпросторі. Це здатність системи до прогнозування кіберризиків, запобігання кіберзагрозам, адекватного реагування на загрозу вразі неочікуваного впливу та швидкого відновлення або регенерації продуктивності. Оцінювання відносно нинішнього фактичного стану органу (регіону, установи, підприємства тощо), де працює. За умови відсутності активності, визначеної по суті індикатором, «Рівень оцінювання» визначається як «Дуже низький»	РІВЕНЬ ОЦІНЮВАННЯ					ВПЛИВ на загрози		
		дуже високий	високий	середній	низький	дуже низький	сильний	помірний	незначний
1.	Ефективність формування/реалізації державної політики у сфері кібербезпеки на рівні:	x	x	x	x	x	x	x	x
1.1.	на рівні:	x	x	x	x	x	x	x	x
1.1.1	загальнодержавному								
1.1.2	регіональному (область)								
1.1.3	місцевому								
1.1.4	діяльності Уряду								
1.1.5	діяльності ЦОВВ								
1.1.6	законодавчої (нормотворчої) діяльності								
1.1.7	правоохоронної діяльності								
1.1.8	державної регуляторної діяльності								
1.1.9	ініціативної діяльності постачальників ІКТ послуг								
1.1.10	ініціативної діяльності об'єктів критичної інфраструктури								

1.2.	Рівень захисту цифрового середовища (мереж) в Україні в частині:								
1.2.1	на національному рівні								
1.2.2	на місцевому рівні								
1.2.3	на рівні окремих підприємств								
1.2.4	на індивідуальному рівні								
	в частині:	X	X	X	X	X	X	X	X
1.2.5	запобігання кібератакам								
1.2.6	створення базової безпеки в продуктах і послугах								
1.2.7	допомоги приватним особам, малим підприємствам та організаціям з базовими заходами для покращення кібербезпеки								
1.2.8	подолання державними установами системних кібер-ризиків								
1.2.9	формування державними установами системної підтримки через рекомендації, інструменти, розвиток навичок та акредитацію на ринку								
1.3.	Рівень захисту інформації в Україні								
1.3.1	на національному рівні								
1.3.2	на місцевому рівні								
1.3.3	на рівні окремих підприємств								
1.3.4	на індивідуальному рівні								
1.4.	Здатність суб'єктів вітчизняної системи кібербезпеки:	X	X	X	X	X	X	X	X
1.4.1	розбудовувати національну систему кіберстійкості								
1.4.2	забезпечувати захист держави і суспільства від кібератак								
1.4.3	забезпечувати захист громадян від кібератак								
1.4.4	забезпечувати кіберзахист об'єктів критичної інфраструктури								
1.4.5	оцінювати власні спроможності кіберзахисту								
1.4.6	нарощувати сучасні технологічні можливості, приймати на озброєння новітні системи, сучасні технології та спеціальні засоби								
1.4.7	забезпечувати своєчасний обмін інформацією								
1.4.8	забезпечувати чітку координацію дій з іншими суб'єктами кібербезпеки								
1.4.9	організовувати заходи щодо інформування та підготовки населення до дій в умовах кібератак								
1.4.10	розробляти нові методи кіберзахисту								
1.5.	Інші спроможності	X	X	X	X	X	X	X	X
1.5.1	Стан ознайомлення із передовим зарубіжним досвідом у сфері кібербезпеки щодо:	X	X	X	X	X	X	X	X
1.5.1.1	професійної освіти								
1.5.1.2	практичної діяльності								
1.5.1.3	технічного оснащення								
1.5.1.4	аналітичного забезпечення								
1.5.1.5	оцінки ризиків								
1.5.1.6	прийняття управлінських рішень								
1.5.1.7	управління ризиками								
1.5.1.8	залучення та використання ресурсів								

1.5.1.9	<i>дотримання принципів демократичного суспільства</i>							
1.5.2	Рівень науково-методичного забезпечення у сфері кібербезпеки							
1.5.3	Рівень взаємозв'язку науки і практики у сфері кібербезпеки							
1.5.4	Рівень відповідних компетентностей і кваліфікацій науково-педагогічних працівників в закладах вищої освіти за спеціальністю «Кібербезпека»							
1.5.5	Рівень фахової освіти за спеціальністю «Кібербезпека» у закладах вищої освіти							
1.5.6	Рівень навчання на основі інцидентів інформаційної безпеки							
1.5.7	Рівень фінансового забезпечення наукової та дослідницької діяльності у сфері кібербезпеки							
1.5.8	Рівень спроможностей навчальних та наукових установ щодо стратегічних досліджень у сфері кібербезпеки							
1.5.9	Рівень пріоритетності фінансування прикладних і теоретичних досліджень в галузі інформатики.							
1.5.10	Рівень заохочення міждисциплінарних кібердосліджень для підготовки наступного покоління осіб, які приймають рішення, і аналітиків.							
2.	Ефективність щодо досягнення кіберстійкості (прогнозування, запобігання, адекватного реагування та швидкого відновлення) в Україні:	x	x	x	x	x	x	x
2.1	на рівні:	x	x	x	x	x	x	x
2.1.1	<i>загальнодержавному</i>							
2.1.2	<i>регіональному (область)</i>							
2.1.3	<i>місцевому</i>							
2.1.4	<i>окремих підприємств</i>							
2.1.5	<i>індивідуальному</i>							
2.2.	Ефективність реагування на кіберінциденти на рівні:							
	на рівні:	x	x	x	x	x	x	x
2.2.1	<i>загальнодержавному</i>							
2.2.2	<i>регіональному (область)</i>							
2.2.3	<i>місцевому</i>							
2.2.4	<i>правоохоронних, розвідувальних органів та безпеки</i>							
2.2.5	<i>окремих підприємств-постачальників ІКТ послуг</i>							
2.2.6	<i>окремих об'єктів критичної інфраструктури</i>							
2.2.7	<i>індивідуальному</i>							
2.3.	Ефективність боротьби з кіберзлочинністю на рівні:							
	на рівні:	x	x	x	x	x	x	x
2.3.1	<i>загальнодержавному</i>							
2.3.2	<i>регіональному (область)</i>							
2.3.3	<i>місцевому</i>							
2.3.4	<i>правоохоронних органів</i>							
2.4.	Ефективність захисту критичної інформаційної інфраструктури в частині:							
	на рівні:	x	x	x	x	x	x	x
2.4.1	<i>загальнодержавному</i>							

2.4.2	регіональному (область)								
2.4.3	місцевому								
2.4.4	окремих об'єктів критичної інфраструктури								
	в частині:	X	X	X	X	X	X	X	X
2.4.5	розуміння природи кіберризиків								
2.4.6	стратегічного бачення та відповідного планування								
2.4.7	ідентифікації загроз та оцінювання ризиків								
2.4.8	прогнозування ризиків								
2.4.9	адаптації до загроз і умов, які швидко змінюються (у т.ч. криз/руйнувань)								
2.4.10	визначення вразливостей								
2.4.11	витримування неочікуваних ударів								
2.4.12	визначеності дій щодо захисту систем, запобігання кібератакам і протистояння їм								
2.4.13	прийняття обґрунтованих (на основі попередніх аналітичних висновків) управлінських рішень								
2.4.14	готовності до мінімізації впливу кібератак								
2.4.15	здатності до відновлення після кібератак								
2.4.16	здатності до швидкої мобілізації зусиль в умовах загроз/кризи								
2.4.17	відновлювання після руйнівних наслідків								
2.4.18	можливості застосування творчих/інноваційних рішень								
2.4.19	доступності консультацій, рекомендацій та інших інструментів щодо кіберзахисту та кіберстійкості								
2.4.20	цілісності загальносуспільних зусиль, спрямованих на підвищення кіберстійкості України								
2.4.21	визначеності загального підходу до національної кіберстійкості								
2.4.22	використання досвіду країн-лідерів у сфері кібербезпеки								
2.4.23	використання найкращих світових практик у сфері кібербезпеки								
3.	Розуміння кібер-ризиків для забезпечення більш ефективних дій у сфері кібербезпеки та стійкості до кіберзагроз на рівні:	X	X	X	X	X	X	X	X
3.1.	на рівні:	X	X	X	X	X	X	X	X
3.1.1	загальнодержавному								
3.1.2	регіональному (область)								
3.1.3	місцевому								
3.1.4	правоохоронних, розвідувальних органів та безпеки								
3.1.5	окремих підприємств-постачальників ІКТ послуг								
3.1.6	окремих об'єктів критичної інфраструктури								
3.1.7	індивідуальному								
3.2.	Здатність державних органів виявляти кібер-ризиків								

3.3.	Рівень зв'язку оцінки кібер-ризиків, заходів кібербезпеки та кіберстійкості (Ваша особиста точка зору)							
3.4.	Рівень розуміння обов'язків щодо управління кібер-ризиками							
3.5.	Ефективність партнерства між урядом, бізнесом і організаціями задля колективного розуміння ризиків, визначення пріоритетних та формування обґрунтування необхідності дій							
3.6.	Рівень підтримки громадян державними органами у взаємодії з бізнесом та організаціями, які надають ІКТ послуги споживачам							
3.7.	Стратегічне розуміння кібер-ризиків для країни та використання цього розуміння для визначення системних ризиків, пріоритетів, формування стратегії та її реалізації							
3.8.	Підтримка залучення значних інвестицій у контексті «розуміння кіберзагроз» на основі попередньо визначеної Національної стратегії кібербезпеки, спираючись на відповідні зусилля щодо розуміння кібер-ризиків							
3.9.	Системність використання методики (рамкової, відомої, визнаної, рекомендованої) щодо оцінки кібер-ризиків							
3.10.	Системність, методична визначеність (порівнювання існуючих систем) аналізу кібербезпеки							
3.11.	Системність (регулярність, постійність) виявлення вразливостей та звітування про них							
3.12.	Рівень відносин (налагодженість, довіра) зі спільнотою дослідників кібербезпеки							
3.13.	Рівень використання аналізу критичності ланцюгів постачання ІКТ							
3.14.	Рівень партнерських відносин держави (органів, установ) з власниками та операторами ІКТ послуг щодо доступу до інформації про загрози та ризики							
3.15.	Рівень співпраці щодо розумінням нових ризиків, що з'являються внаслідок діджиталізації та нових технологій							
3.16.	Рівень зв'язку між українською і глобальною кіберстійкістю (Ваша особиста точка зору)							
3.17.	Рівень допомоги суб'єктам (організаціям, постачальниками послуг) щодо кращого зрозуміння кібер-ризиків для їхніх клієнтів							
3.18.	Рівень впровадження підприємствами кібербезпеки як важливої та провідної частини належного ведення бізнесу							
3.19.	Доступність та відкритість результатів досліджень і даних про поширеність і вплив кібератак							
3.20.	Доступність та відкритість результатів досліджень і даних щодо прогресу, якого досягають сектори у підвищенні кібербезпеки							

3.21.	Рівень розроблення показників кібер-ризиків підприємствами за участю представників страхових компаній та керівництва галузі							
3.22.	Рівень мотивації державою зусиль щодо аналізу потенційного позитивного впливу страхових практик на плани кіберзахисту							
3.23.	Застосування форсайту у сфері кібербезпеки							
4.	Ефективність запобігання кібератакам та протистояння їм шляхом покращання управління кібер-ризики в організаціях та забезпечення більшого захисту громадян	x	x	x	x	x	x	x
4.1.	Рівень відповідальності в установах, підприємствах, організаціях за вжиті заходи щодо управління власними кібер-ризики							
4.2.	Рівень відповідальності державних органів (підприємств, установ, організацій) та операторів критично важливої національної інфраструктури щодо підвищення своїх стандартів та більш проактивного управління своїми кібер-ризики							
4.3.	Рівень відповідальності великого бізнесу та організацій-постачальників цифрових послуг щодо ставлення до захисту своїх систем, послуг і клієнтів як до основної частини ведення бізнесу							
4.4.	Рівень пріоритетності впровадження більш ефективних систем звітності та належного управління кібер-ризики							
4.5.	Рівень впровадження більш ефективних систем звітності та належного управління кібер-ризики на рівні вищого керівництва							
4.6.	Роль уряду (державних органів, установ) у співпраці з суб'єктами системи кібербезпеки щодо безпосереднього зниження кіберризиків в сегментах унікальних державних можливостей							
4.7.	Ефективність системи стимулів, підтримки та регулювання щодо перенесення тягаря ризиків кібербезпеки від кінцевих користувачів до тих, хто має найкращі можливості для управління ними							
4.8.	Рівень підтримки та допомоги фізичним особам, приватним підприємцям, малим підприємствам та організаціям в управлінні своїми кібер-ризики							
4.9.	Рівень державних заходів активного кіберзахисту для підтримки ширшого кола секторів, включаючи благодійні організації, наукові кола, малий і середній бізнес та громадян							
4.10.	Рівень взаємодії та обміну інформацією з суб'єктами системи кібербезпеки (бізнесом) щодо посилення захисту онлайн-сервісів							
4.11.	Рівень правового забезпечення безпеки громадян в Інтернеті та протидії шахрайству							
4.12.	Рівень співпраці з провайдерами онлайн-послуг, телекомунікаційних технологій, банківським сектором і							

	роздрібною торгівлею щодо кращого захисту українських інтернет-користувачів								
	щодо:	x	x	x	x	x	x	x	x
4.12.1	ускладнення реєстрації веб-сайтів для незаконних цілей								
4.12.2	посилення видалення та блокування шкідливого контенту в Інтернеті								
4.12.3	покращення відновлення та повернення викрадених облікових даних								
4.12.4	підвищення безпеки телекомунікаційної інфраструктури								
4.13.	Рівень подолання системних ризиків, пов'язаних з ланцюгом постачання цифрових технологій (диверсифікації ланцюгів постачання)								
4.14.	Рівень обміну інформацією щодо надійності та прозорості відбору прямих іноземних інвестицій у критично важливих секторах та загальних постачальників для уряду (державних органів)								
4.15.	Рівень стійкості до поширених нових методів кібератак								
4.16.	Рівень визначеності регуляторними органами базового стандарту кібербезпеки за окремими секторами								
4.17.	Рівень упровадження стандартизації, акредитації, сертифікації у сфері кібербезпеки								
4.18.	Рівень мотивованості операторів ІКТ щодо інвестування в кібербезпеку критично важливих систем, підвищення ефективності управління своїми ризиками, зокрема щодо ланцюгів постачання ІКТ								
4.19.	Рівень юридичної відповідальності операторів ІКТ щодо неналежного інвестування в кібербезпеку критично важливих систем, підвищення ефективності управління своїми ризиками, зокрема щодо ланцюгів постачання ІКТ								
4.20.	Рівень необхідності розбудови національної системи кіберстійкості (Ваша особиста точка зору)								
4.21. 1	Рівень законодавчого забезпечення ефективного управління кібер-ризиками тими, хто несе за це найбільшу відповідальність								
4.21. 2	Рівень законодавчого забезпечення ефективного управління кібер-ризиками тими, хто несе за це найбільшу відповідальність, у світлі еволюції ризиків і технологій у майбутньому								
4.22.	Рівень консультаційних заходів щодо законодавчого забезпечення кібербезпеки та кіберстійкості, зокрема провайдерів ІКТ, пропорційно майбутнім викликам								
4.23.	Спроможність регуляторних органів, операторів ІКТ послуг інших суб'єктів щодо інвестування в розвиток навичок та утримання кіберпрофесіоналів								
4.24.	Спроможність регуляторних органів, операторів ІКТ послуг інших суб'єктів щодо інвестування в розвиток партнерства між урядом, науковими колами та промисловістю								

4.25.	Рівень інвестиційного скринінгу посилення системи управління кібер-ризиками, забезпечення вищих стандартів безпеки та стійкості економічної інфраструктури							
4.26.	Здатність підприємств та організацій проактивно управляти своїми кібер-ризиками та впроваджувати заходи для підвищення своєї кіберстійкості.							
4.27.	Рівень розвитку ринкових стимулів, що заохочують підприємства та організації проактивно управляти своїми кібер-ризиками та впроваджувати заходи для підвищення своєї кіберстійкості							
4.28.	Рівень співпраці держави (її представників) з тими, хто впливає на ринок (замовниками, фінансовими установами, інвесторами, аудиторам та страховиками) з метою стимулювання належних практик кібербезпеки по всій економіці							
4.29.	Рівень використання корпоративної звітності про стійкість до кібер-ризиків							
4.30.	Рівень розуміння інвесторами та акціонерами компаній щодо управління та пом'якшення суттєвих кібер-ризиків для свого бізнесу							
4.31.	Рівень цільового законодавчого забезпечення секторів, де потенційний вплив кібератак є найбільшим, включаючи постачальників певних основних та цифрових послуг, захист даних в економіці в цілому, та для великого бізнесу							
4.32.	Розробленість та доступність стимулів, технічних порад, інструментів самопомоги, а також гарантованих продуктів та послуг, для підвищення кіберстійкості громадян, фізичних осіб-підприємців та малих підприємств.							
4.33.	Організаційне, фінансове забезпечення та доступність формування цифрових навичок громадянами усіх вікових груп							
4.34.	Рівень допомоги підприємствам та організаціям в орієнтуванні на складному ринку кібербезпеки, розширюючи рамки гарантованих продуктів і послуг та полегшуючи малим підприємствам доступ до базових консультацій							
4.35.	Рівень розуміння суб'єктами системи кібербезпеки необхідності розбудови національної системи кіберстійкості							
5.	Посилення стійкості на національному та організаційному рівнях, реагування на кібератаки та відновлення після них	x	x	x	x	x	x	x
5.1.	Рівень можливостей для управління інцидентами та реагування на них в усіх організаціях (підприємствах, установах), мінімізації завданої шкоди та надання максимальної підтримки жертвам							
5.2.	Рівень Вашого особистого розуміння необхідності спільних зусиль між урядом, всіма частинами економіки та суспільства у розбудові кіберстійкості							

5.3.	Рівень ефективності стратегічного управління в державі та координації реагування на національно значущі кіберінциденти							
5.4.	Рівень гарантій використання для покращення політик та процесів, набутого досвіду урядом (державними органами) щодо реагування на значні кіберінциденти							
5.5.	Рівень визначення найкращих зарубіжних (міжнародних) практик кризового управління для підвищення готовності та процесів							
5.6.	Рівень забезпеченості спеціальних органів щодо управління кібер-ризиками, набуття необхідного досвіду й використання відповідного інструментарію реагування на весь спектр кіберінцидентів та координації національного реагування на пріоритетні кібер загрози							
5.7.	Доступність повідомлень про кіберінциденти							
5.8.	Рівень підтримки жертв кіберзлочинів							
5.9.	Рівень узагальнення, аналізу та використання інформації для запобігання майбутнім кібер-інцидентам та підтримки правоохоронних органів щодо розслідування, припинення злочинів та переслідування кіберзлочинців							
5.10.	Достатність узагальнення інформації про шахрайство і кіберзлочинність та поширення у суспільстві з метою запобігання та реагування у майбутньому							
5.11.	Рівень мотивації розвитку оповіщення не традиційними способами про кіберінциденти							
5.12.	Можливості регуляторів вимагати звітність про ширший спектр кіберінцидентів, включно з «прорахунками»							
5.13.	Рівень планування та проведення регулярних навчань щодо реагування на випадок інцидентів та відновлення після них							
5.14.	Рівень включення кібер-аспектів у національні навчання з врегулювання кризових ситуацій							
5.15.	Рівень проведення національних командно-штабних навчань із включенням різних відомств, відповідальних за надання критично важливих послуг, представників приватного сектору і ключовий персонал органів державного управління							
5.16.	Рівень поєднання технічних аспектів кібернавчань, які проводяться в лабораторіях лише серед технічного персоналу, із стратегічними щодо прийняття рішень							
5.17.	Наявність на ринку акредитованих освітніх послуг щодо реагування та управління кіберінцидентами, а також вивчення новітніх методів та алгоритмів							
5.18.	Рівень моніторингу та виявлення кіберінцидентів в державній цифровій інфраструктурі							
5.19.	Рівень компетентності фахівців державних органів щодо управління кіберінцидентами, наявності відповідного потенціалу та можливостей реагування							

	ними на весь спектр кіберінцидентів, із врахуванням майбутніх змін							
5.20.	Наявність чітких вимог до навчання і випробовування усіх операторів ІКТ, враховуючи симуляції кіберінцидентів							
5.21.	Рівень мотивації щодо інновацій та співробітництва в реагуванні на кіберінциденти і навчання							
5.21.	Рівень використання передового досвіду для тестування, тренувань і навчання з критично важливих інформаційних технологій для розбудови потенціалу в цій галузі, у співпраці з бізнесом, науковими колами та міжнародними партнерами							
5.22.	Рівень розуміння підприємствами та організаціями того, що робити у випадку кіберінциденту, кому телефонувати, хто може допомогти та як відновитися							
5.23.	Рівень розгортання національної програми правоохоронної підтримки жертв кіберзлочинів							
5.24.	Ефективність діяльності регіональних центрів кіберстійкості (за їх відсутності рівень оцінюється як «дуже низький»)							
5.25.	Рівень мотивації використання малими підприємствами та організаціям місцевої підтримки щодо кіберстійкості							
6.	Рівень реалізації спроможності суб'єктів системи кібербезпеки (планувати/готуватися, поглинати, відновлюватися, адаптуватися) до кіберподії в сферах: фізичній, інформаційній, когнітивній, соціальній	x	x	x	x	x	x	x
6.1.	Здатність планування/підготовки: закладення основи для забезпечення доступності послуг та функціонування активів під час руйнівної події (несправності або атаки) у сферах							
	у сферах	x	x	x	x	x	x	x
6.1.1	фізичній: фізичні ресурси, можливості і структура цих ресурсів							
6.1.2	інформаційній: інформація та розвиток інформації про фізичну сферу							
6.1.3	когнітивній: використання інформаційного та фізичного доменів для ухвалення рішень							
6.1.4	соціальній: організаційна структура та комунікація для ухвалення когнітивних рішень							
6.2.	Здатність поглинання: підтримки найбільш важливих функцій активів та доступність послуг під час відбиття або ізоляції збоїв у роботі у сферах							
	у сферах	x	x	x	x	x	x	x
6.2.1	фізичній: фізичні ресурси, можливості і структура цих ресурсів							
6.2.2	інформаційній: інформація та розвиток інформації про фізичну сферу							
6.2.3	когнітивній: використання інформаційного та фізичного доменів для ухвалення рішень							
6.2.4	соціальній: організаційна структура та комунікація для ухвалення когнітивних рішень							

6.3.	Здатність до відновлення: відновлення всіх функцій активів, доступність сервісів та їх функціональність як до події у сферах								
	у сферах	x	x	x	x	x	x	x	x
6.3.1	фізичний: фізичні ресурси, можливості і структура цих ресурсів								
6.3.2	інформаційний: інформація та розвиток інформації про фізичну сферу								
6.3.3	когнітивний: використання інформаційного та фізичного доменів для ухвалення рішень								
6.3.4	соціальний: організаційна структура та комунікація для ухвалення когнітивних рішень								
6.4.	Здатність до адаптації: використовуючи знання, отримані під час події, зміна протоколу, конфігурації системи, навчання персоналу або інші аспекти для досягнення більшої стійкості у сферах								
	у сферах	x	x	x	x	x	x	x	x
6.4.1	фізичний: фізичні ресурси, можливості і структура цих ресурсів								
6.4.2	інформаційний: інформація та розвиток інформації про фізичну сферу								
6.4.3	когнітивний: використання інформаційного та фізичного доменів для ухвалення рішень								
6.4.4	соціальний: організаційна структура та комунікація для ухвалення когнітивних рішень								

Додаток Г

Опитувальник складено з метою проведення аналізу кіберзлочинності.

Опитування є анонімним. При заповненні опитувальника забороняється вносити будь-які реєстраційні дані матеріалів та персональні дані осіб.

№ З/П	ЗАГАЛЬНІ ДАНІ	КАТЕГОРІЇ				
1.	Ваш номер за списком реєстрації у даному опитуванні	цифри				
2.	Регіон	1.	Вінницька область			
		2.	Волинська область			
		3.				
		4.				
		5.				
		6.				
		7.				
		8.				
		9.				
		10.				
		11.				
		12.				
		13.				
		14.				
		15.				
		16.				
		17.				
		18.				
		19.				
		20.				
		21.				
		22.				
		23.				
		24.				
		xx.	Центральний апарат			
		5.	Досвід діяльності за фаховою сферою	Більше 15 років	10 – 15 років	5 – 10 років
						Менше 1 р
3.	Посада Категорія посади	Інспектор, ст.інспектор		Керівник оперативного підрозділу		Керівник аналітичного підрозділу
		Слідчий		Оперативний працівник		Аналітик
4.	Джерело інформації - оберіть із можливих варіантів:	кримінальне провадження, оперативно-розшукова справа, довідково-аналітичні матеріали				
	Стать					

Індикатори загроз

1.	Сфера злочинної діяльності ОЗУ: Ви можете обрати декілька сфер.
1.1	Вкажіть причетність до вчинення кримінального правопорушення у розрізі видів (ККУ) Так/ні
	у сфері комп'ютерних систем – 1833 (425):
1.1.1	361
1.1.2	361-1
1.1.3	361-2
	362
1.1.4	363
	363-1
	у сфері протидії обігу протиправного контенту і телекомунікацій – 1637 (163): - ст. 120 КК України – 0 (0); - ст. 149 КК України – 1 (1); - ст.ст. 156, 156-1 КК України – 4 (3); - ст. 176 КК України – 3 (2); - ст. 203-1 КК України – 4 (0); - ст. 229 КК України – 2 (0); - ч. 3, 4, 5 ст. 301 КК України – 71 (12); - ст.ст. 301-1, 301-2 КК України – 152 (139); - ст. 307 КК України – 1399 (5); - ст.ст. 321, 321-1 КК України – 1 (1).
	у сфері протидії злочинам у банківській сфері – 2538 (414): - ст. 185 КК України – 482 (80); - ст. 200 КК України – 531 (143); - ст. 209 ККУ - ст. 231 КК України – 2 (1); - ст. 362 КК України – 1523 (190).
	у сфері протидії різновидам онлайн шахрайств – 6113 (1006): - чч. 1, 2 ст. 190 КК України – 1107 (335); - чч. 3, 4 ст. 190 КК України – 5006 (671).
	в інших сферах – 222 (156): - ст. 357 КК України – 21 (15); - ст. 358 КК України – 201 (141).
1.1.5.	
1.2	Які сфери в суспільстві зазнали шкоди внаслідок вчинення (готування) злочину Вкажіть причетність до вчинення злочинів у розрізі сфер в суспільстві: Так/ні
1.2.1	Управління (адміністрування)
1.2.3	Економіка
1.2.4	Фінанси / банки / страхування
1.2.5	Інфраструктура
1.2.6	Виробництво
1.2.7	Юридична
1.2.8	Інформаційна та комунікації
1.2.9	Цифрові послуги
1.2.10	Військова

1.2.11	Оборонна
1.2.12	Безпекова
1.2.13	Аналітична
1.2.14	Освітня
1.2.15	Соціальна
1.2.16	Культура
1.3.	Шляхи реалізації злочинного наміру один Приєднати до шахрайства
1.3.1	Виготовлення дублікату картки
1.3.2	Купівля в Інтернет
1.3.3.	Використання підробленої картки в магазині
1.3.4	Продаж скомпрометованих даних
1.3.5	Використання викрадених карток
1.3.6	Отримання готівки
1.3.7	Інше (коментувати)
	Невідомо
	Мотивація злочинців Так/ні
	Матеріальне збагачення
	Складова гібридної війни
	Співпраця з агресором
	Хуліганські дії
	Суспільний протест
	Невідомо
	Інше
2.2.	Кількість осіб причетних до вчинення кримінального правопорушення: один
2.1	ОЗУ має більш ніж 9 членів
2.2	ОЗУ має від 5 до 9 членів
2.3	ОЗУ має від 3 до 5 членів
2.4	Менше 3-х осіб
2.5	Невідомо
2.1.	Кримінальне правопорушення визнається вчиненим організованою групою, якщо в його готуванні або вчиненні брали участь. Будь ласка оберіть:
	декілька осіб (дві або більше)
	декілька осіб (три і більше)
	Наявні ознаки кваліфікації ОГ або ЗО
	так
	ні
	Не відомо
3.	Термін кримінальної діяльності: один
	Більше 15 років
	Від 10 до 15 років
	Від 5 до 10 років
	Від 3 до 5 років
	Від 1 до 5 років
	До 1 року
	Невідомо
	Не застосовується
4.	Зв'язок з країною-агресором: один
4.1	Цілеспрямована діяльність в інтересах країни-агресора
4.2	Діяльність з тимчасово непідконтрольних (анексованих) територій
4.3	Із зазначеними ознаками не пов'язано

4.4	Невідомо
5.	Географічне поширення
5.1.	Оберіть географічний вимір злочинної діяльності: один
5.1.1	на транснаціональному рівні
5.1.2	На національному рівні
5.1.4	На регіональному рівні
5.1.5	На місцевому рівні (район, місто)
5.1.6	Невідомо
5.2.	З якої країни надходить ГОЛОВНА загроза Список Bootstrap dropdown
	З якої країни надходить ДОДАТКОВА загроза Список Bootstrap dropdown
	З якої країни надходить ДОДАТКОВА загроза Список Bootstrap dropdown
	На яку країну поширюється загроза: Список Bootstrap dropdown
	На яку країну ДОДАТКОВО поширюється загроза: Список Bootstrap dropdown
	На яку країну ДОДАТКОВО поширюється загроза: Список Bootstrap dropdown
	Уточніть, з якою тимчасово окупованою (анексованою) територією пов'язана злочинна діяльність?
	Профіль правопорушника (у випадку вчинення кримінального правопорушення у складі ОЗУ профіль може вказувати на різні ознаки одночасно)
	Стать Множинний вибір
	Чоловік/ Жінка
	Вік Множинний вибір
	Менше 15 років, 15 – 18 років, 18 – 25 років, ,, Більше 60 років
	Соціальний статус Множинний вибір
	учень, Студент, Працюючий, Непрацюючий, Пенсіонер
	Невідомо
6.	Будь ласка, вкажіть основні загрози, пов'язані з діяльністю цієї ОЗУ, та їх тенденції
6.2	Шахрайство з платежами: без використання банківської картки
	Шахрайство, пов'язане з транспортом – авіаквитки
	Шахрайство, пов'язане з транспортом – квитки на поїзд або автобус
	Шахрайство, пов'язане з транспортом - оренда автомобілів
	Шахрайство, пов'язане з позику (послугою, орендою приміщення тощо)
	Шахрайство, пов'язане з веб-сайтами азартних ігор
	Шахрайство, пов'язане з роздрібною торгівлею – фізичні товари
	Шахрайство, пов'язане з роздрібною торгівлею – віртуальні товари (програмне забезпечення, послуги тощо)
	Шахрайство, пов'язане з конвертацією валют (криптовалют та електронних грошей тощо)
	Шахрайство з використанням паливних карток
	Шахрайство з використанням карток у роздрібній торгівлі продуктами
	Шахрайство з використанням клубних карток
	Шахрайство з використанням подарункових карток
	Шахрайство з використанням ігрових карток
	Шахрайство на ринку мобільного зв'язку
	Шахрайство в сфері комп'ютерних ігор (внутрішньоігрові перекази)
	Шахрайство пов'язане з букмекірськими послугами
	Шахрайство пов'язане з «move to»
	Інше - надайте деталі >>
6.3	Шахрайство з платежами: з використанням банківської картки
	Зняття готівки з банківських карт UA за межами UA
	Зняття готівки з банківських карт UA в межах UA

	<i>Зняття готівки з іноземних банківських карток у межах UA</i>
	<i>RoS-покупки з використанням скомпрометованої платіжної картки</i>
	<i>Шахрайство з платіжними картками: треїлінг</i>
	<i>Шахрайство з платіжними картками: фармінг</i>
	<i>Шахрайство з платіжними картками: фішинг</i>
	<i>Шахрайство з банкоматом: скімінг</i>
	<i>Шахрайство з банкоматом: траппінг</i>
	<i>Шахрайство з банкоматом: фантом</i>
	<i>Шахрайство з банкоматом: jackpotting</i>
	<i>Шахрайство з телефоном та інтернетом: вішинг</i>
	<i>Шахрайство з телефоном та інтернетом: смішинг</i>
	<i>Інше - надайте деталі >></i>
6.3	Шахрайство з платежами_інше
	<i>Attacks on ATMs - cash traps Атаки на банкомати - пастки для готівки</i> <i>Attacks on ATMs - Malware (e.g. jackpotting) Зловмисне програмне забезпечення (наприклад, джекпотинг)</i> <i>Attacks on ATMs - Інше - надайте деталі >></i> <i>Mobile / Contactless Payment Fraud Шахрайство з використанням мобільних/безконтактних платежів</i> <i>Продаж скомпрометованих даних картки онлайн (кардшопи тощо)</i> <i>Інше - надайте деталі >></i>
7.	Кримінальні комунікації
	<i>Комунікації між злочинцями - форуми Deep Web/Darknet</i> <i>Комунікації між злочинцями - Email</i> <i>Комунікації між злочинцями - відкриті форуми, соціальні мережі</i> <i>Комунікації між злочинцями - ICQ</i> <i>Комунікації між злочинцями - IRC</i> <i>Комунікації між злочинцями - Jabber</i> <i>Комунікації між злочинцями - веб-чат</i> <i>Комунікації між злочинцями – інше – надайте деталі >></i> <i>Спілкування між злочинцями та жертвами - Email</i> <i>Спілкування між злочинцями та жертвами - FaceTime</i> <i>Спілкування між злочинцями та жертвами - Messenger</i> <i>Спілкування між злочинцями та жертвами - Skype</i> <i>Спілкування між злочинцями та жертвами - Viber</i> <i>Спілкування між злочинцями та жертвами - Web-based chatroom</i> <i>Спілкування між злочинцями та жертвами - WhatsApp</i> <i>Спілкування між злочинцями та жертвами - Telegram,</i> <i>Спілкування між злочинцями та жертвами - IMO,</i> <i>Спілкування між злочинцями та жертвами - Signal</i> <i>Спілкування між злочинцями та жертвами - веб-чат</i> <i>Спілкування між злочинцями та жертвами - WeChat</i> <i>Спілкування між злочинцями та жертвами - QQ</i> <i>Спілкування між злочинцями та жертвами - Snapchat</i> <i>Спілкування між злочинцями та жертвами - Riot</i> <i>Спілкування між злочинцями та жертвами - Threema</i> <i>Спілкування між злочинцями та жертвами - LINE</i> <i>Спілкування між злочинцями та жертвами - Wire</i> <i>Спілкування між злочинцями та жертвами - Voxer</i> <i>Спілкування між злочинцями та жертвами - Slack</i> <i>Спілкування між злочинцями та жертвами - GroupMe</i> <i>Спілкування між злочинцями та жертвами - IM+</i>

	Спілкування між злочинцями та жертвами - інше – надайте деталі >> Використання рішень анонімізації - I2P Використання рішень анонімізації - Proxies Використання рішень анонімізації - Tor Використання рішень анонімізації - VPNs Використання рішень анонімізації - Other - please give details >> Інше – надайте деталі >>
6.	Кримінальні фінанси
6.4	Грошові мули (дропи) Racket Mules Платежі між злочинцями Платежі між злочинцями - банківські перекази Платежі між злочинцями - банківська картка Платежі між злочинцями - Системи оплати ваучерами (наприклад, paysafecard) Платежі між злочинцями – електронні гроші: Webmoney Платежі між злочинцями – електронні гроші: PerfectMoney Платежі між злочинцями – електронні гроші: Юmoney Платежі між злочинцями – електронні гроші: Qiwi Платежі між злочинцями – електронні гроші: PayPal Платежі між злочинцями – електронні гроші: Advanced Cash Платежі між злочинцями – електронні гроші: Payeer Платежі між злочинцями – електронні гроші: Skrill Платежі між злочинцями – електронні гроші: EasyPay Платежі між злочинцями – електронні гроші: Інші Платежі між злочинцями – криптовалюти: Bitcoin Платежі між злочинцями – криптовалюти: Ethereum Платежі між злочинцями – криптовалюти: Ripple Платежі між злочинцями – криптовалюти: Monero Платежі між злочинцями – криптовалюти: BNB Платежі між злочинцями – криптовалюти: USDT Платежі між злочинцями – криптовалюти: USDC Платежі між злочинцями – криптовалюти: Zcash Платежі між злочинцями – криптовалюти: Dash Платежі між злочинцями – криптовалюти: Litecoin Платежі між злочинцями - Інші криптовалюти Платежі між злочинцями - інше – надайте деталі >> 6.5 Платежі від жертв до злочинців: Платежі від жертв до злочинців - Банківські перекази Платежі від жертв до злочинців - Платіжна картка Платежі від жертв до злочинців - Шляхом поповнення мобільного рахунку Платежі від жертв до злочинців - Шляхом покупки якогось предмету, речі Платежі від жертв до злочинців - Системи оплати ваучерами (наприклад, paysafecard) Платежі від жертв до злочинців: електронні гроші Платежі від жертв до злочинців – електронні гроші: Webmoney Платежі від жертв до злочинців – електронні гроші: PerfectMoney Платежі від жертв до злочинців – електронні гроші: Юmoney Платежі від жертв до злочинців – електронні гроші: Qiwi Платежі від жертв до злочинців – електронні гроші: PayPal Платежі від жертв до злочинців – електронні гроші: Advanced Cash Платежі від жертв до злочинців – електронні гроші: Payeer Платежі від жертв до злочинців – електронні гроші: Skrill

	Платежі від жертв до злочинців – електронні гроші: EasyPay Платежі від жертв до злочинців – електронні гроші: Інші Платежі від жертв до злочинців: криптовалюта Платежі від жертв до злочинців – криптовалюти: Bitcoin Платежі від жертв до злочинців – криптовалюти: Ethereum Платежі від жертв до злочинців – криптовалюти: Ripple Платежі від жертв до злочинців – криптовалюти: Monero Платежі від жертв до злочинців – криптовалюти: BNB Платежі від жертв до злочинців – криптовалюти: USDT Платежі від жертв до злочинців – криптовалюти: USDC Платежі від жертв до злочинців – криптовалюти: Zcash Платежі від жертв до злочинців – криптовалюти: Dash Платежі від жертв до злочинців – криптовалюти: Litecoin Платежі від жертв до злочинців - Інші криптовалюти інше – надайте деталі >>
6.1	Фінансова активність пов'язана з: Шахрайство з платежами Платежі між злочинцями Платежі від жертв до злочинців Відмиванням коштів Фінансуванням тероризму Інше
6.6	Відмивання коштів здійснюється через: Банківські перекази За допомогою платіжних карток Через рахунки мобільних телефонів Шляхом покупки якогось предмету, речі, послуги Систему оплати ваучерами Електронні гроші Криптовалюти Інше
6.7	Фінансування тероризму здійснюється через: Банківські перекази За допомогою платіжних карток Через рахунки мобільних телефонів Шляхом покупки якогось предмету, речі, послуги Систему оплати ваучерами Електронні гроші Криптовалюти Інше
8	Активність в Даркнет Криптопрограми (для шифрування шкідливих файлів для невиявлення їх антівірусами) Програми, в які навмисно вбудована вразливість розробниками Відомості про банківські рахунки Матеріали про насильство над дітьми Контрафактні товари Наркотики Відмивання коштів Торгівля людьми Шкідливе програмне забезпечення Відомості про платіжні картки

	Зброя Персональні дані осіб Послуги хостингу, які не зберігають дані про клієнта В інтересах агресора (РФ) Фінансування тероризму Надання іншого сервісу кіберзлочинності – надайте деталі >>
9	Способи шифрування
	Використання рішень анонімізації - I2P Використання рішень анонімізації - Tor Використання рішень анонімізації - VPN сервісний Використання рішень анонімізації - VPN власноналаштований Використання рішень анонімізації - Проксі-сервір Використання шифрування для захисту даних: BitLocker Використання шифрування для захисту даних: VeraCrypt Використання шифрування для захисту даних: TrueCrypt інше – надайте деталі >>
10	Інтернет речей
	Свідчення щодо нетипових смарт-пристроїв Відомості на нетипових смарт-пристроях Пристрої IoT використовуються як частина ботнету Пристрої IoT використовуються як проксі-сервіси Шкідливе програмне забезпечення націлене на IoT пристрої IoT інше – надайте деталі >>
11	Соціальна інженерія
	Фішинг (через електронну пошту) Вішинг (по телефону) Smishing (через SMS) CEO Fraud Шахрайство з авансовими платежами Романтична афера Шахрайство типу "підтримка Microsoft". Вербування грошових мулів інше – надайте деталі >> Advanced fee fraud Romance Scam "Microsoft support" type scams Recruiting of money mules
12	Специфічні інструменти (послуги), що використовуються при вчиненні злочинів
	За видом використання операційних систем злочинцями
	Kali Linux
	BlackArch Linux
	BackBox Linux
	Parrot Security OS
	Невідомо інші
	За видом використання спеціального програмного забезпечення
	DoS-атака

	спамінг	
	брутфорс	
	пентестинг	
	Невідомо інші	
	За джерелом отримання програмного забезпечення злочинцями	
	даркнет	
	форуми	
	соціальні мережі	
	інші	
	За видом спеціальних технічних засобів	
	скіммер	
	код-граббер	
	спеціальні технічні засоби негласного отримання інформації	
	Невідомо інші	
13	Способи вчинення злочинів	
	За способом отримання доступу одночасно	
	Шляхом перехоплення інформації при її передачі телекомунікаційними каналами і комп'ютерними мережами	
	Шляхом проникнення до приміщення, в якому знаходиться ПК	
	Шляхом відкритого доступу до ПК	
	Невідомо інше	
	За способом віддаленого отримання доступу одночасно	
	Шляхом використання зловмисниками реальних паролів користувачів, отриманих в мережі	
	Отримання паролів, ключів шляхом перебору за допомогою спеціальних програм	
	Невідомо інше	
	За способом отримання потерпілими посилання на шкідливе програмне забезпечення одночасно	
	Месенджери	
	Соціальні мережі	
	Електронна пошта	
	Sms-повідомлення	
	Сайт	
	Невідомо інші	
	За способом перехоплення трафіку одночасно	

	Людина посередині (man in the middle)	
	Отруйний DNS (poison DNS)	
	Паралельна сесія	
	За допомогою шкідливого ПЗ, яке отримує авторизаційні дані з браузера (Stiller)	
	Невідомо інше	

Індикатори вразливості національної системи кібербезпеки

№ З/П	ВРАЗЛИВОСТІ (порушення захищеності ІКТ і даних) – фактори, що характеризують нездатність (системи або її частини) витримувати впливи кіберзагроз; міра чутливості до уражень, пошкоджень. При відсутності зазначеного фактору рівень прояву визначається як «нульовий», а вплив як можлива ймовірність.	Рівень прояву					Вплив на кібербезпеку		
		дуже високий	високий	середній	низький	нульовий	сильний	помірний	незначний
1.	Технологічна відсталість в Україні:								
1.1.	Щодо сучасних інформаційно-комунікаційних технологій								
1.2.	Щодо перспективних новітніх технологій:								
1.2.1.	Наступного покоління мобільного зв'язку або 5G								
1.2.2.	Інтернет речей (IoT)								
1.2.3.	Smart cars								
1.2.4.	Віртуальних фінансових активів (криптовалют)								
1.2.5.	Штучного інтелекту (автоматизованого фішингу, вішингу та пошуку уразливостей комп'ютерних систем, автономної зброї)								
2.	Низький технічний рівень:								
2.1.	Комп'ютерних систем								
2.2.	Комунікаційних систем								
2.3.	Інформаційних систем								
2.4.	Платіжних систем								
	Захисту банкоматів								
3.	Невідповідність програмного забезпечення:								
3.1.	Неліцензійне програмне забезпечення								
3.2.	Помилки програмування								
3.3.	Застарілі (неактивні) спеціальні програми кіберзахисту (антивірус, firewall тощо)								
	У зв'язку із впровадженням високотехнологічних інформаційних систем								
4.	Недостатність юридичного забезпечення:								
4.1.	Невідповідність міжнародним стандартам у сфері кібербезпеки								
4.2.	Незабезпечення кібербезпеки на рівні законів України								

4.3.	Незабезпечення кібербезпеки на рівні підзаконних нормативних актів								
4.4.	Невідповідність державним та галузевим стандартам								
4.5.	Недостатність юридичної відповідальності за порушення законодавства у сфері кібербезпеки								
	Надмірність та неузгодженість правового регулювання у сфері кібербезпеки								
5.	Недостатність фінансового забезпечення:								
5.1.	Недостатній рівень фінансування кібербезпеки								
5.2.	Недостатній рівень інвестування у технологічний та безпековий розвиток НСКБ								
6.	Недостатність інституційного забезпечення:								
6.1.	Недостатній рівень регуляторного забезпечення кібербезпеки								
6.2.	Недостатній рівень правоохоронного забезпечення кібербезпеки								
7.	Організаційні недоліки:								
7.1.	Недостатній рівень міжвідомчих стратегічних комунікацій у сфері кібербезпеки								
7.2.	Недостатній відомчий моніторинговий рівень кібербезпеки								
7.3.	Недостатній рівень державно-приватної взаємодії у сфері кібербезпеки								
8.	Соціальні (персонал) недоліки:								
8.1.	Недостатній рівень кібергігієни громадян								
8.2.	Недостатній рівень кібергігієни персоналу державних органів								
8.3.	Недостатній рівень кібергігієни персоналу об'єктів критичної інформаційної інфраструктури								
8.4.	Недостатній рівень компетентностей фахівців з кібербезпеки								

Індикатори спроможності

№ з/П	СПРОМОЖНОСТІ – внутрішні фактори, що стосуються різних сторін діяльності КІБЕРПОЛІЦІЇ й характеризуються рівнем прояву (застосування, поширення, ефективності) та рівнем впливу на зниження кіберзагроз (оцінюється нинішній фактичний стан). При відсутності зазначеного фактору рівень прояву визначається як «нульовий», а вплив як можлива ймовірність.	Рівень прояву					Вплив на кіберзагрози		
		дуже високий	високий	середній	низький	нульовий	сильний	помірний	незначний
1.	Рівень політичної підтримки розвитку кіберполіції								
2.	Рівень нормативно-правового забезпечення								

	діяльності кіберполіції								
3.	Рівень нормативно-правового забезпечення технічного регулювання у сфері захисту інформації								
4.	Повнота імплементації міжнародних стандартів кібербезпеки								
5.	Рівень економічної підтримки діяльності та розвитку кіберполіції								
6.	Рівень реагування органів влади на потреби кіберполіції								
7.	Рівень співробітництва кіберполіції із зарубіжними партнерами								
8.	Рівень поширення позитивного зарубіжного досвіду щодо розвитку кіберполіції								
9.	Рівень залучення іноземних експертів щодо розвитку кіберполіції								
10.	Рівень міжвідомчих комунікацій кіберполіції з:	X	X	X	X	X	X	X	X
10.1.	державними органами								
10.2.	об'єктами критичної інформаційної інфраструктури								
10.3.	іншими правоохоронними органами								
10.4.	органами державної безпеки								
10.5.	фінансовими установами								
10.6.	громадськими та приватними ініціативами								
11.	Ефективність реагування кіберполіції на нові виклики (техногенні, глобалізаційні, гібридні загрози тощо)								
12.	Ефективність кіберполіції щодо моніторингу кіберзагроз								
13.	Ефективність кіберполіції щодо протидії кібератакам (загалом)								
14.	Ефективність кіберполіції щодо реагування на кіберінциденти								
15.	Рівень культури в кіберполіції щодо забезпечення конфіденційності службових та приватних комунікацій через електронні засоби								
16.	Рівень дотримання кібергігієни персоналом кіберполіції								
17.	Рівень використання ліцензійного програмного забезпечення в кіберполіції								
18.	Рівень використання програм захисту (антивірус, firewall тощо) в кіберполіції								
19.	Рівень діджиталізації управлінських комунікацій кіберполіції								
	Рівень діджиталізації досудового розслідування у сфері кібербезпеки								
20.	Рівень фінансового забезпечення розвитку наукової та дослідницької діяльності у сфері кібербезпеки								
21.	Рівень спроможності (компетентності) закладів вищої освіти МВС щодо:								
21.1	освітньої підготовки персоналу кіберполіції								
21.2	підвищення кваліфікації персоналу кіберполіції								

21.3	наукових досліджень у сфері кібербезпеки								
21.4	стратегічного аналізу у сфері кібербезпеки								
22.	Рівень методологічного забезпечення кіберполіції								
23.	Рівень аналітичного забезпечення кіберполіції								
24.	Рівень впровадження кіберполіцією превентивних заходів щодо протидії кіберзагрозам								
25.	Рівень прогнозування персоналом кіберполіції наслідків поширення кіберзагроз								
26.	Рівень обізнаності кіберполіції щодо видів та рівня кіберзагроз								
27.	Рівень обізнаності кіберполіції щодо вразливості у сфері кібербезпеки								
28.	Рівень обізнаності кіберполіції з ризик-орієнтованим підходом								
29.	Рівень використання кіберполіцією підходів з управління ризиками: загалом								
29.1.	на стратегічному рівні								
29.2.	на оперативному (тактичному) рівні								
30.	Рівень особистісної стійкості персоналу кіберполіції до:	X	X	X	X	X	X	X	X
30.1.	проявів корупції								
30.2.	зловживання посадовим станом								
30.3.	дезінформації								
31.	Професійна компетентність персоналу кіберполіції								
31.1.	управлінського рівня								
31.2.	виконавського рівня								
32.	Рівень забезпечення професійної підготовки персоналу в підрозділах кіберполіції								