НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Кваліфікаційна наукова праця на правах рукопису

КОТУХ Євген Володимирович

УДК 35.085:316.344.42

ДИСЕРТАЦІЯ
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПУБЛІЧНОМУ СЕКТОРІ

25.00.02 – механізми державного управління

галузь знань – публічне управління та адміністрування

Подається на здобуття наукового ступеня
доктора наук з державного управління

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

(підпис, ініціали та прізвище здобувача)

Харків – 2022

АНОТАЦІЯ

Котух Є.В. Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 «Механізми державного управління». – Національний університет цивільного захисту України, Харків, 2022.

Забезпечення кібербезпеки на даний час є важливою проблемою на всіх рівнях публічного управління: від місцевих органів влади, що займаються онлайн-транзакціями, до центральних органів влади, що займаються питаннями національної безпеки. Кібербезпека – це динамічна мета, яка змінюється з такою швидкістю, що дуже важко отримати абсолютно актуальне уявлення про неї. Нові кіберзагрози або варіації старих виникають майже щодня, як і стратегії захисту від них. Однак існують і деякі загальні підходи до забезпечення кібербезпеки, які слід визначати та адаптувати до специфіки конкретних держав і конкретних органів публічної влади.

У *першому розділі* дисертаційної роботи розкриваються зміст і особливості електронного врядування як парадигми публічного управління, визначається поняття і сутність кібербезпеки у публічному секторі, розглядаються особливості впровадження систем кібербезпеки в органах публічної влади. Обґрунтовується, що кібербезпеку слід розглядати як суспільне благо, оскільки кібербезпека, маючи три основні складові (інформаційно-комунікаційні системи, які є надійними і можуть протистояти атакам; методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; забезпечення системної реактивності на кібератаки), забезпечує задоволення публічних інтересів інформаційного суспільства щодо можливості належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології.

Визначаються основні виклики для публічного сектора у контексті забезпечення кібербезпеки в сучасних умовах.

У межах *другого розділу* здійснюється аналіз сучасних тенденцій і підходів до забезпечення кібербезпеки у публічному секторі крізь призму зарубіжного досвіду. Докладно розглядаються та аналізуються національні стратегії кібербезпеки, визначаються основні підходи до забезпечення кібербезпеки у публічному секторі. Наголошується на тому, що сфера кібербезпеки вже включена до порядку денного з питань безпеки всіх досліджених держав, але дана сфера у різних державах відрізняється за тим, як держави, по-перше, визначають референтний об'єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики; відповідно до цих відмінностей держави можна поділити на дві категорії: держави, що мілітаризують питання кібербезпеки, та держави, що криміналізують питання кібербезпеки.

У *третьому розділі* розглядаються практичні аспекти забезпечення кібербезпеки у публічному секторі, обґрунтовується необхідність формування глобального підходу до забезпечення кібербезпеки. Ключовою ідеєю при цьому виступає забезпечення кібербезпеки у середовищі Gov 2.0. Визначено, що вона має ґрунтуватись на реалізації таких заходів: модерування контенту публічних аккаунтів; запобігання несанкціонованому використанню і передачі конфіденційної інформації; використання браузерів з обмеженими привілеями; впровадження систем виявлення / запобігання вторгнень; використання сервісів Web-репутації; фільтрація універсального локатора ресурсів (URL) та Інтернет-протоколу (IP); фільтрація шкідливих програм по периметру мережі; використання інструментів попереднього перегляду скорочення URL.

Четвертий розділ присвячено аналізу сучасного стану і проблем запобігання та протидії кіберзагрозам у публічному секторі України. Доводиться, що головними кіберзагрозами для сучасної України є крадіжка інформації, фінансове шахрайство і хакерські атаки. При цьому держава в

цілому і органи публічного управління, зокрема, є не готовими сьогодні до адекватного реагування на ці загрози. Рівень кіберзахисту у публічному секторі значно поступається приватному, публічний сектор взагалі виявився найбільш незахищеним з точки зору протистояння кібератакам та витоку даних в Україні. Це зумовлено як недостатньою захищеністю інформаційних мереж, недосконалістю існуючого обладнання і програмного забезпечення, так і відсутністю кваліфікованих фахівців в сфері кіберзахисту. Виходячи з цього, держава не виступає суб‘єктом, якому громадяни довіряють в питаннях кіберзахисту, зокрема, стосовно захисту персональної інформації.

Зміст *п’ятого розділу* містить пропозиції автора щодо удосконалення забезпечення кібербезпеки в публічному секторі. Розроблено модель інституційної кібербезпеки, відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість. Обґрунтовано теоретико-методологічну модель розробки національної стратегії кібербезпеки, яка використовує підходи неореалізму, соціального конструктивізму, інтерсекційності, кібервестфалізму. Визначено основні принципи публічно-приватного партнерства у сфері забезпечення кібербезпеки, до яких віднесено: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства.

Ключові слова: публічний сектор, публічне управління, кібербезпека, кіберзагрози, формування та реалізація державної політики, органи публічної влади, електронне врядування, владні відносини, публічно-приватне

партнерство у сфері забезпечення кібербезпеки.

ANNOTATION

Kotuch Ye.V. «Theoretical and methodological principles of ensuring cybersecurity in the public sector». – Qualifying scientific paper as the manuscript.

Dissertation for obtaining the scientific degree of doctor of sciences of public administration specialty 25.00.02 – Mechanisms of Public Administration. – National University of Civil Defence of Ukraine, Kharkiv, 2022.

Ensuring cybersecurity is currently an important issue at all levels of public administration: from local authorities dealing with online transactions to central authorities dealing with national security issues. Cybersecurity is a dynamic goal that changes at such a rate that it is very difficult to get a completely up-to-date view of it. New cybersecurity or variations of old ones emerge almost daily, as do strategies to protect against them. However, there are also some general approaches to ensuring cybersecurity, which should be defined and adapted to the specifics of specific states and specific public authorities.

The *first chapter* of the dissertation reveals the content and features of e-governance as a paradigm of public management, defines the concept and essence of cybersecurity in the public sector, considers the features of the implementation of cybersecurity systems in public authorities. It is justified that cybersecurity should be considered as a public good, since cybersecurity, having three main components (information and communication systems that are reliable and can withstand attacks; methods and systems for detecting threats and anomalies to ensure the stability of information and communication systems; ensuring system reactivity on cyberattacks), ensures the satisfaction of the public interests of the information society regarding the possibility of proper functioning of critical national infrastructures, and allows citizens to carry out their routine activities, relying on safe technologies. The main challenges for the public sector in the context of ensuring cybersecurity in modern conditions are identified.

The *second chapter* analyzes modern trends and approaches to ensuring cybersecurity in the public sector through the prism of foreign experience. National cybersecurity strategies are considered and analyzed in detail, the main approaches to ensuring cybersecurity in the public sector are determined. It is emphasized that the sphere of cybersecurity is already included in the security agenda of all the studied states, but this sphere differs in different states according to how states, firstly, define the reference object (what needs to be protected), secondly , perceive the main threats and risks and, thirdly, identify the sources of threats and risks; according to these differences, states can be divided into two categories: states that militarize cybersecurity issues and states that criminalize cybersecurity issues.

In the *third chapter*, the practical aspects of ensuring cybersecurity in the public sector are considered, the necessity of forming a global approach to ensuring cybersecurity is substantiated. The key idea here is to ensure cybersecurity in the Gov 2.0 environment. It was determined that it should be based on the implementation of the following measures: moderation of the content of public accounts; prevention of unauthorized use and transfer of confidential information; using browsers with limited privileges; implementation of intrusion detection / prevention systems; use of Web-reputation services; Universal Resource Locator (URL) and Internet Protocol (IP) filtering; filtering of malicious programs along the network perimeter; using URL shortening preview tools.

The *fourth chapter* is devoted to the analysis of the current state and problems of preventing and countering cybersecurity in the public sector of Ukraine. It is proven that the main cybersecurity for modern Ukraine are information theft, financial fraud and hacker attacks. At the same time, the state as a whole and public administration bodies, in particular, are not ready today to respond adequately to these threats. The level of cyber protection in the public sector is significantly inferior to the private sector, the public sector in general turned out to be the most unprotected from the point of view of countering cyber attacks and data leakage in Ukraine. This is due to the insufficient security of information networks, the imperfection of existing equipment and software, and

the lack of qualified specialists in the field of cyber protection. Based on this, the state does not act as an entity that citizens trust in matters of cyber protection, in particular, in relation to the protection of personal information.

The *fifth chapter* contains the author's proposals for improving cybersecurity in the public sector. A model of institutional cybersecurity has been developed, according to which institutional cybersecurity should have the following main components: cybersecurity policy, strategy and standards; cyber risk management; vulnerability and threat management; centralized management of incidents; cybersecurity awareness and education; log management and correlation; secure architecture; legal norms; technical tools; business continuity; permanent audit and monitoring; cooperation; cyber resilience.

The theoretical and methodological model of the development of the national cybersecurity strategy, which uses the approaches of neorealism, social constructivism, intersectionality, and cyber Westphalia, is substantiated.

The main principles of public-private partnership in the field of cybersecurity are defined, which include: transition from "classic" partnership to mutually beneficial cooperation; defining the roles of partnership members using risk management approaches; introduction of joint responsibility of partnership members regarding threats and vulnerabilities; implementation of the partnership evaluation system.

Keywords: public sector, public administration, cybersecurity, cybersecurity, formation and implementation of state policy, public authorities, e-governance, power relations, public-private partnership in the field of cybersecurity.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

монографічні видання:

1. Котух Є.В. Кібербезпека у публічному секторі : монографія / Є.В. Котух. – Харків : Колегіум, 2021. – 272 с.

в яких опубліковані основні наукові результати дисертації:

2. Котух Є.В. Особливості національної та регіональної політики у сфері кібербезпеки / Є.В. Котух // Теорія та практика державного управління. – 2019. – № 4(67). – С. 40-47.

3. Котух Є.В. Проблеми кібербезпеки в сучасному світі // Актуальні проблеми державного управління. – 2019. – №2(56). – С. 33-38.

4. Котух Є.В. Особливості забезпечення кібербезпеки в публічному секторі в умовах глобалізації / Є.В. Котух // Державне будівництво. – 2019. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/view/65/60.

5. Котух Є.В. Формування систем кібербезпеки в органах публічної влади / Є.В. Котух // Державне управління: удосконалення та розвиток. – 2020. – № 3, березень. – Режим доступу: http://www.dy.nayka.com.ua/pdf/3_2020/32.pdf.

6. Котух Є.В. Електронне урядування як нова парадигма публічного управління / Є.В. Котух // Інвестиції: практика та досвід. – 2020. – № 3, лютий. – С. 122-127.

7. Котух Є.В. Електронний уряд і кібербезпека у соціальних мережах: особливості реалізації // Вісник НУЦЗ України. Серія: Державне управління. – 2020. – № 2. – С. 564-572.

8. Котух Є.В. Основні виклики врядування у сфері кібербезпеки / Є. Котух, В. Ободяк // Теорія та практика державного управління. – 2020. – № 4 (71). – С. 38-46.

Особистий внесок здобувача: визначено характеристики врядування у сфері кібербезпеки та ресурси кіберпростору.

9. Котух Є.В. Кібербезпека як один з пріоритетів національної політики / В.Б. Дзюндзюк, Є.В. Котух // Державне будівництво. – 2020. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/download/90/85.

Особистий внесок здобувача: визначено пріоритетні напрями реалізації стратегій кібербезпеки.

10. Котух Є.В. Сучасний стан та проблеми «цифровізації» в Україні / Є.В. Котух, А.С. Довбиш // Актуальні проблеми державного управління. – 2020. – № 2. – С. 25-31.

Особистий внесок здобувача: визначено основні проблеми процесу цифровізації в Україні.

11. Котух Є.В. Реалізація національних стратегій кібербезпеки: силовий аспект // Наукові перспективи. – 2021. – № 2(8). – С. 125-136.

12. Котух Є. В. Основні підходи до забезпечення кібербезпеки: досвід країн вишеградської четвірки // Інвестиції: практика та досвід. – 2021. – № 3. – С. 68-74.

13. Котух Є.В. Проблема кібершахрайства та фактори стримування її вирішення органами публічного управління / Є.В. Котух. // Вісник НУЦЗ України. Серія: Державне управління. – 2021. – Випуск 1 (14). – С. 185-191.

14. Котух Є.В. Національні стратегії кібербезпеки: порівняльний аналіз / Є.В. Котух // Актуальні проблеми державного управління. – 2021. – № 1. – С. 48-57.

15. Котух Є.В. Оцінка рівня захисту кіберпростору в публічному управлінні: національний та організаційний виміри / Є.В. Котух // Теорія та практика державного управління. – 2021. – № 1. – С. 31-39.

16. Котух Є.В. Реалізація стратегій кібербезпеки: економіко-політичний аспект / Є.В. Котух // Теорія та практика державного управління. – 2021. – № 2. – С. 171-175.

17. Котух Є.В. та ін. Аудит інформаційної безпеки як необхідна складова управління в державних установах / Є.В. Котух, О.М. Кучма, Д.М. Нехороших, Г.В. Пліс, Г.З. Халімов // Державне будівництво. – 2021. – № 1. – Режим доступу: https://db.kh.ua/index.php/db/article/view/117/110.

Особистий внесок здобувача: визначення особливнстей аудиту інформаційної безпеки.

18. Котух Є.В. Типи владних відносин у стратегії кібербезпеки / Є.В. Котух // Інвестиції: практика та досвід. – 2021. – № 11. – С. 98-102.

19. Котух Є.В. Теоретико-методологічна модель розробки національної стратегії кібербезпеки / Є.В. Котух // Наукові перспективи. – 2021. – № 6 (12). – С. 39-52.

20. Котух Є.В. Розвиток публічно-приватного партнерства у сфері кібербезпеки // Інвестиції: практика та досвід. – 2021. – № 13. – С. 76-84.

21. Kotukh Ye.V. Public value management and new public governance as modern approaches to the development of public administration / Oleksandr O. Bryhinets, Ivo Svoboda, Oksana R. Shevchuk, Yevgen V. Kotukh, Valentyna Yu. Radich // Revista San Gregorio (Web of Science Core Collection). – Núm. 42 (2020). Pp. 205-213. http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1568/20-OLAKSANDR

Особистий внесок здобувача: визначення особливостей концепції «Public value», що має значення для розвитку концепції електронного врядування.

22. Kotukh Ye.V. Spread of virtual communities as a potential threat to state security and sustainable well-being / Viacheslav B. Dziundziuk, Oleksandr A. Kotukov, Dmytro V. Hryn, Eugene V. Kotukh // Rivista Di Studi Sulla Sostenibilita (Scopus). – 2020. – Issue 2. – Pp. 7-18.

Особистий внесок здобувача: визначено основні напрями негативного впливу розвитку віртуальних співтовариств як акторів кіберпростору на національну безпеку.

23. Kotukh Y.V. State Information Security Policy (Comparative Legal Aspect) / Y. V. Kotukh, V. B. Dziundziuk, O. M. Krutii, V. P. Solovykh, O. A. Kotukov // Cuestiones Políticas. – 2021. – 39(71). – Pp. 166-186.

Особистий внесок здобувача: визначено принципи, на яких має грунтуватись державна політика кібербезпеки.

24. Kotukh, Y. V. Cybercrime and subculture of cybercriminals / Y. V. Kotukh, D. V. Kislov, T. S. Yarovoi, R. O. Kotsiuba, O. H. Bondarenko // Linguistics and Culture Review. –2021 – 5(S4). – Pp. 858-869.

які засвідчують апробацію матеріалів дисертації:

25. Котух Є.В. Ризики зростання відкритості публічного сектору та засоби боротьби з ними / Котух Є.В. // Збірник тез XX Міжнародного наукового конгресу «Публічне управління XXI століття: портал можливостей» (м. Харків, 23 квітня 2020 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2020. – С. 103-106.

26. Котух Є.В. Кіберзагрози у сучасному світі / В.Б. Дзюндзюк, Є.В. Котух // International Scientific Integration ‘2020 (Seattle, Washington, USA, November 10, 2020). – Pp. 103-106.

27. Котух Є.В. Проблеми урядування у сфері кібербезпеки / В.Б. Дзюндзюк, Є.В. Котух // Abstracts of scientific papers of IV International Scientific Conference «Science and Global Studies» (Prague, November 30, 2020). – Pp. 25-28.

28. Kotukh Ye. Encryption scheme based on the automorphism group of the Ree function field / Gennady Khalimov, Yevgeniy Kotukh, Svitlana Khalimova // 7th International Conference on Internet of Things: Systems, Management and Security (Paris, France. December 14-16, 2020). – Pp. 1-8.

29. Котух Є.В. Щодо питання реалізації національних стратегій кібербезпеки / Котух Є.В. // Збірник тез XXI Міжнародного наукового конгресу «Публічне управління XXI століття: погляд у майбутнє» (м. Харків, 21 квітня 2021 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2021. – С. 161–165.

30. Котух Є.В. Національні стратегії кібербезпеки: економіко-політичний аспект / Є.В. Котух // Multidisziplinare Forschung: Perspektiven, Probleme und Muster (Wien, 09.04.2021). – Pp. 49-50.

31. Котух Є. Боротьба з кіберзлочинністю в країнах ЄС / Є. Котух // Матеріали 18-ї регіональної науково-практичної конференції «Актуальні проблеми європейської та євроатлантичної інтеграції України» (м. Дніпро, 13 травня 2021 р.). – Дніпро : ДРІДУ НАДУ. – С. 114-117.

ЗМІСТ

ВСТУП

Актуальність теми. Забезпечення кібербезпеки на даний час є важливою проблемою на всіх рівнях публічного управління: від місцевих органів влади, що займаються онлайн-транзакціями, до центральних органів влади, що займаються питаннями національної безпеки. Кібербезпека – це динамічна мета, яка змінюється з такою швидкістю, що дуже важко отримати абсолютно актуальне уявлення про неї. Нові кіберзагрози або варіації старих виникають майже щодня, як і стратегії захисту від них. Однак існують і деякі загальні підходи до забезпечення кібербезпеки, які слід визначати та адаптувати до специфіки конкретних держав і конкретних органів публічної влади.

Забезпечення кібербезпеки занадто часто віддають ІТ-фахівцям, які погано розбираються в більших організаційних проблемах або виробленні політики, в той час як вище керівництво публічних організацій не розуміє пов’язаних з цим технічних питань. Тому важливим завданням є переведення новітніх технічних термінів і загроз у поняття, зрозумілі для вищого керівництва, співробітників і суспільства в цілому. Усунення розриву між ІТ-фахівцями і керівниками публічного сектора й особами, що визначають політику, має фундаментальне значення для підвищення кібербезпеки.

Крім того, організації публічного сектора можуть створити більш сильний кіберзахист, налагоджуючи більш тісні відносини і співпрацюючи з іншими для обміну досвідом, помилками, отриманими уроками та іншою інформацією і дослідженнями. Готовність збирати, аналізувати й обмінюватися інформацією, в тому числі про кіберінциденти, має вирішальне значення для підвищення загального рівня кібербезпеки. А це потребує налагодження співпраці з вітчизняними та міжнародними акторами з усіх трьох секторів: публічного, приватного, неурядового, що, зокрема, дозволить підвищити суспільну обізнаність щодо кіберзагроз, їх небезпек і методів запобігання.

Зовнішня і внутрішня ефективність публічного сектора може значно підвищитися за рахунок використання нових інформаційно-комунікаційних технологій, проте сучасні тенденції в цій сфері можуть також призвести до появи нових викликів та нових проблем. Очевидно, що частота і масштаби кібератак будуть збільшуватися, в тому числі й на публічний сектор. Шкідливе програмне забезпечення, інсайдерська інформація, бот-мережі, DDoS-атаки, кібершпіонаж і кібертероризм ставатимуть все більш витонченими і, як і раніше, наноситимуть фінансову, репутаційну та інші види шкоди, а також створювати загрозу національній безпеці. Тому у даний час кібербезпека – це глобальна проблема, яка потребує глобальної відповіді, але це також локальна проблема, що вимагає локального реагування. Відтак, кожна сучасна публічна організація зобов'язана проявляти ініціативу і реалізовувати політики, що підвищують рівень кібербезпеки. Від цього залежить не тільки її власна безпека, але і безпека всього публічного сектора, держави і суспільства в цілому.

Теоретико-методологічні засади публічного управління в сучасних умовах висвітлюються в працях таких науковців, як В. Бакуменко [8; 9], Д. Белл [12; 13], Т. Бове [252], Е. Гідденс [35], В. Дзюндзюк [54 – 57], М. Дрепо [299], М. Кастельс [72 – 75], В. Князєв [79], Ю. Куц [121], М. Лахижа [123], Е. Лоффлер [252], М. Маклюен [132], Дж. Най [427], С. Попов [157], К. Торнхілл [491], П. Уілбі [214], Р. Хікс [351], В. Шамрай [226] та ін.

Питання формування та реалізації державної політики щодо забезпечення кібербезпеки розглянуто у працях таких зарубіжних дослідників, як М. Данн [301; 302; 303], К. Зеттер [529; 530], Дж. Карр [270], С. Кемпбелл [267], Р. Кларк [278], Е. Клімбург [383; 384; 385], Р. Кнейк [278], М. Лібіцкі [396; 397], Т. Мур [419], П. Розенцвейг [454], Т. Стівенс [471; 472], Дж. Хілі [350; 383], Р. Хьюс [359] та ін.

Серед вітчизняних науковців проблеми забезпечення інформаційної та кібербезпеки у публічному секторі досліджували такі науковці як М. Бутко

[20], С. Гончар [37], Ю. Даник [39], П. Воробієнко [39], Б. Дзюндзюк [48; 49], Д. Дубов [59], В. Карпенко [71], Б. Корнієнко [86], О. Курбан [120], В. Лизанчук [126], Ю. Лісовська [129], Р. Лук'янчук [130], О. Орлов [149], Г. Почепцов [158], О. Рижук [190], А. Семенченко [61; 192], Т. Станіславський [203], В. Степанов [205] та ін.

Проте проблема забезпечення кібербезпеки у публічному секторі залишається недостатньо розробленою. Насамперед це стосується напрацювань, присвячених методологічним підходам до практичної реалізації теоретичних моделей і концепцій у даній сфері. Також бракує праць, присвячених адаптації вже наявного позитивного досвіду як до специфіки конкретних країн, так і з урахуванням нових викликів, що постійно виникають у кіберпросторі. Усе це зумовлює актуальність теми дисертації, визначає її мету й завдання.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційної роботи пов'язана з науково-дослідними роботами «Публічне управління в умовах глобалізації» (державний реєстраційний номер 0220U104528) та «Євроінтеграційний вектор розвитку України та реалізація національних інтересів в умовах глобальних викликів» (державний реєстраційний номер 0120U105649), що виконувались кафедрою політології та філософії Харківського регіонального інституту державного управління Національної академії державного управління при Президентові України. У межах першої теми автором визначено особливості забезпечення кібербезпеки у середовищі Gov 2.0, другої – основні виклики для публічного сектора у контексті забезпечення кібербезпеки.

Мета і завдання дослідження. Метою дослідження є теоретико-методологічне обґрунтування забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Досягнення визначеної мети зумовило необхідність вирішення таких *завдань*:

– розкрити зміст і особливості електронного врядування як

парадигми публічного управління;

– з’ясувати основні виклики для публічного сектора у контексті забезпечення кібербезпеки;

– обґрунтувати концептуальні засади забезпечення кібербезпеки в органах публічної влади;

– визначити основні принципи інституційної кібербезпеки в публічному секторі;

– узагальнити зарубіжні практики щодо забезпечення кібербезпеки у публічному секторі;

– з’ясувати особливості запобігання та протидії кіберзагрозам у публічному секторі України;

– обґрунтувати методологічний підхід до забезпечення кібербезпеки у середовищі Gov 2.0;

– з’ясувати використання різних типів владних відносин у забезпеченні кібербезпеки;

– розробити модель інституційної кібербезпеки, визначити її основні компоненти;

– обґрунтувати теоретико-методологічну модель розробки національної стратегії кібербезпеки;

– розглянути особливості публічно-приватного партнерства у сфері забезпечення кібербезпеки.

Об’єкт дослідження – формування та реалізація державної політики у сфері кібербезпеки.

Предмет дослідження – забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Методи дослідження. Методологічною основою дослідження є системний підхід, що дозволяє представити державну політику стосовно забезпечення кібербезпеки як складну структурно-організовану систему, яка потребує удосконалення та розвитку. Для досягнення мети й завдань дисертаційного дослідження використовувався комплекс загальнонаукових і

спеціальних методів, зокрема:

– історико-генетичний, логіко-семантичний, аналіз, узагальнення, ідеалізація (розкриття змісту й особливостей електронного врядування як парадигми публічного управління);

– історико-генетичний, логіко-семантичний, узагальнення, абстрагування, порівняння (з'ясування основних викликів для публічного сектора у контексті забезпечення кібербезпеки);

– системний, абстрагування, порівняння, формалізація, історико-генетичний, інституціональний аналіз, (обґрунтування концептуальних засад забезпечення кібербезпеки в органах публічної влади);

– історико-генетичний, логіко-семантичний, класифікації, узагальнення, аналіз, формалізація, порівняння (визначення основних принципів інституційної кібербезпеки в публічному секторі);

– емпіричний, абстрагування, порівняльний аналіз, узагальнення, описово-індуктивний, спостереження (узагальнення зарубіжних практик щодо забезпечення кібербезпеки у публічному секторі);

– емпіричний, індукція, узагальнення, синтез, діалектичний, прогностичний (з'ясування особливостей запобігання та протидії кіберзагрозам у публічному секторі України);

– діалектичний, індукція, узагальнення, формалізація, прогностичний (обґрунтування методологічного підходу до забезпечення кібербезпеки у середовищі Gov 2.0);

– системний, діалектичний, інституціональний аналіз, факторний аналіз (з'ясування використання різних типів владних відносин у забезпеченні кібербезпеки);

– моделювання, системний, інституціональний аналіз, узагальнення, формалізація, синтез (розробка моделі інституційної кібербезпеки);

– моделювання, системний, діалектичний, узагальнення, формалізація, синтез (обґрунтування теоретико-методологічної моделі розробки національної стратегії кібербезпеки);

– системний, індукція, узагальнення, порівняння, інституціональний аналіз, структурно-функціональний аналіз (розгляд особливостей публічно-приватного партнерства у сфері забезпечення кібербезпеки).

Крім зазначених методів дослідження у дисертації широко використовувалися такі методи дослідження як аналіз статистичних даних і офіційних документів, а також порівняльно-правовий та компаративний методи, використання яких мало суцільний характер.

Теоретичну основу роботи складають наукові праці фахівців у галузі науки державного управління, соціології, політології, юридичних наук. Особливе місце у дисертації приділено аналізу спеціальної літератури з тематики дослідження: статей у спеціалізованих наукових виданнях, монографій, енциклопедій, словників.

У дисертації широко використана нормативно-правова база України та інших країн, які регулюють різні аспекти формування та реалізації державної політики щодо забезпечення кібербезпеки у публічному секторі. При написанні роботи використано вітчизняні та зарубіжні джерела (довідкові видання, статистичні матеріали тощо), які послужили інформаційною та емпіричною основою для вирішення визначених завдань дослідження.

Наукова новизна одержаних результатів полягає в обґрунтуванні теоретико-методологічних положень і визначенні практичних заходів щодо забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Найважливіші наукові результати дисертаційного дослідження розкриваються в таких положеннях:

уперше:

– обґрунтовано концептуальні засади забезпечення кібербезпеки в органах публічної влади, які поділяються на дві групи: виміри кібербезпеки (людський, організаційний, інфраструктурний, технологічний, нормативний) та дії, необхідні для забезпечення кібербезпеки (побудова онлайн-довіри; розвиток координації, співпраця та кооперація; профілювання кіберстану; сприяння впровадженню систем кібербезпеки; перегляд; створення правового

середовища; встановлення стандартів);

– розроблено модель інституційної кібербезпеки, відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість;

– обґрунтовано теоретико-методологічну модель розробки національної стратегії кібербезпеки, яка використовує підходи неореалізму, соціального конструктивізму, інтерсекційності, кібервестфалізму та враховує, що актори у кіберпросторі (державні актори, недержавні актори, кінцеві користувачі та кіберзлочинці) здійснюють дії (проводять політику, слідують політиці, атакують, захищаються від нападів, отримують і передають інформацію, здійснюють комунікацію, використовують інформаційно-комунікаційні технології для роботи й у побуті тощо), які перетинаються з різними аспектами кіберпростору та кібербезпеки (політичними, соціальними, культурними, технологічними) та породжують явища кібербезпеки, такі як вразливості, цілісність системи, шкідлива поведінка, ідентичність, мотивація тощо;

удосконалено:

– методологічний підхід до забезпечення кібербезпеки у середовищі Gov 2.0, визначено, що вона має ґрунтуватись на реалізації таких заходів: модерування контенту публічних аккаунтів; запобігання несанкціонованому використанню і передачі конфіденційної інформації; використання браузерів з обмеженими привілеями; впровадження систем виявлення / запобігання вторгнень; використання сервісів Web-репутації; фільтрація універсального локатора ресурсів (URL) та Інтернет-протоколу (IP); фільтрація шкідливих програм по периметру мережі; використання інструментів попереднього

перегляду скорочення URL;

– перелік основних принципів інституційної кібербезпеки, до яких віднесено такі: запровадження холістичного підходу до кібербезпеки; використання гнучкого стилю управління у сфері кібербезпеки; впровадження методів постійного вдосконалення діяльності, орієнтованих на управління ризиками; віднесення до базису забезпечення кібербезпеки координації діяльності публічних, приватних, академічних та неурядових організацій разом з міжнародною співпрацею та обміном інформацією; заохочення прозорості, підзвітності, етичних цінностей, свободи слова у кіберпросторі; встановлення балансу між безпекою та застосовністю IT-продуктів і технологій;

– обґрунтування основних принципів публічно-приватного партнерства у сфері забезпечення кібербезпеки, до яких віднесено такі: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства;

дістали подальшого розвитку:

– концептуальні положення щодо трактування кібербезпеки як суспільного блага; було визначено, що кібербезпека, маючи три основні складові (інформаційно-комунікаційні системи, які є надійними і можуть протистояти атакам; методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; забезпечення системної реактивності на кібератаки), забезпечує задоволення публічних інтересів інформаційного суспільства щодо можливості належного функціонування критично важливих національних інфраструктур і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології;

– визначення основних викликів для публічного сектора у контексті забезпечення кібербезпеки, до яких віднесено такі: 1) велика ступінь

оперативної незалежності та «ізольованості» між різними частинами публічного сектора, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного; 2) важливі загальнодоступні дані створюються, зберігаються та застосовуються відповідними суб'єктами поза органами публічної влади; 3) працівники організацій публічного сектора далеко не завжди демонструють безпечну поведінку у кіберпросторі, хоча саме поведінка людини є стрижнем кібербезпеки; 4) зворотна залежність між використанням інформаційно-комунікаційних технологій і кібербезпекою; 5) відсутність або неефективність публічно-приватного партнерства щодо забезпечення кібербезпеки;

– узагальнення зарубіжних практик щодо забезпечення кібербезпеки у публічному секторі, зокрема, з'ясовано, що сфера кібербезпеки вже включена до порядку денного з питань безпеки всіх досліджених держав, але дана сфера у різних державах відрізняється за тим, як держави, по-перше, визначають референтний об'єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики; відповідно до цих відмінностей держави можна поділити на дві категорії: держави, що мілітаризують питання кібербезпеки, та держави, що криміналізують питання кібербезпеки;

– методологічний підхід до використання різних типів владних відносин у забезпеченні кібербезпеки; визначено, що примусова влада стосовно кібербезпеки надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кіберпростором;

– визначення особливостей запобігання та протидії кіберзагрозам у

публічному секторі України, зокрема, визначено комплекс взаємопов'язаних заходів, які передбачають збільшення рівня кібербезпеки в публічному секторі, що включають: організаційну (створення в органах публічної влади спеціальних підрозділів), матеріально-технічну (установка сучасного обладнання і програмного забезпечення), кадрову (підвищення кваліфікації управлінських кадрів з питань кібербезпеки) і бюджетно-фінансову складову (виділення в державному і місцевому бюджетах обов'язкового цільового фінансування зазначених заходів).

Практичне значення одержаних результатів полягає в можливості їх використання в діяльності органів влади, що сприятиме підвищенню ефективності діяльності як окремих органів влади, так і системи публічного управління в цілому.

Розроблені автором рекомендації щодо підвищення кібербезпеки впроваджено в діяльність:

– Міністерства фінансів України (довідка від 20 серпня 2021 р. № 20040-03-73/26056);

– Міністерства молоді та спорту України (довідка від 13 липня 2021 р. № 6090/1);

– Державної аудиторської служби України (довідка від 13 липня 2021 р. № 001400-16/8764-2021).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею. Усі сформульовані в ній висновки, теоретичні положення та пропозиції ґрунтуються на особистих дослідженнях. У дисертації не використовувалися ідеї співвиконавців науково-дослідних робіт.

Апробація результатів дослідження. Основні положення та результати дисертаційної роботи викладено в наукових повідомленнях на комунікативних заходах: XX Міжнародний науковий конгрес «Публічне управління XXI століття: портал можливостей» (м. Харків, 2020 р.), XXI Міжнародний науковий конгрес «Публічне управління XXI століття: погляд у майбутнє» (м. Харків 2021 р.), International Scientific Integration '2020

(Seattle, Washington, USA, 2020), IV International Scientific Conference «Science and Global Studies» (Prague, 2020), 7th International Conference on Internet of Things: Systems, Management and Security (Paris, France, 2020), Multidisziplinare Forschung: Perspektiven, Probleme und Muster (Wien, 2021), 18-та регіональна науково-практична конференції «Актуальні проблеми європейської та євроатлантичної інтеграції України» (м. Дніпро, 2021 р.) та ін.

Публікації. Основні положення дисертаційного дослідження висвітлено у 31 публікації, з них 1 – одноосібна монографія, 4 – статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та Scopus, 19 – статті у наукових фахових виданнях у галузі науки «Державне управління».

Структура і обсяг роботи. Дисертаційна робота складається зі вступу, п’яти розділів, висновків, списку використаних джерел і додатку. Її повний обсяг становить 479 сторінок, у тому числі: рисунків – 80 (на 35 сторінках), таблиць – 13 (на 17 сторінках), додатків – 1 (на 3 сторінках). Список використаних джерел налічує 531 найменування (на 56 сторінках), у тому числі іноземною мовою – 302.

РОЗДІЛ 1
ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА, ЩО ВПЛИВАЮТЬ НА КІБЕРБЕЗПЕКУ

1.1. Електронне урядування як нова парадигма публічного управління

У Звіті про глобальні ризики Світового економічного форуму за 2019 рік було віднесено кібератаки до десятки найбільших глобальних ризиків. У звіті, опублікованому в 2019 році Інститутом Понемон, зазначено, що 90% установ, що підтримують національні критичні інфраструктури, – енергетичні, охорони здоров'я, промисловості і виробництва, транспортні, зазнали принаймні одну кібератаку у період 2017-2019 рр., що призвело до порушення даних або значних зривів операційної діяльності [449]. Ці звіти є лише двома з тривалої серії досліджень, проведених за останнє десятиліття щодо стану кібербезпеки. З року на рік дані про кібератаки та їх вплив продовжують зростати, що свідчить про те, що кібератаки становлять постійно зростаючу загрозу для інформаційних суспільств, особливо у публічному секторі.

З цих даних можна дізнатися два уроки. Перший досить очевидний і говорить про те, що цифрові інфраструктури – *пористі*. Ми повинні думати про них як про рухливу, гнучку, але крихку систему. Ця крихкість дає перевагу нападу над обороною, частково пояснюючи тривале зростання кіберзагроз та ескалацію їх негативних наслідків. Чим більше цифрових технологій стає все більш розповсюдженими, тим ширше стає поверхня атак, а разом з цим зростає і кількість успішних атак. Візьмемо, наприклад, поширення Інтернету речей (IoT). У 2018 році дослідження Symantec повідомило в середньому про 5200 атак на місяць на пристрої IoT, ця цифра майже вдвічі перевищує 3650 атак, що відбулись у 2016 році.

Другий урок може бути важче засвоїти, оскільки йдеться про неадекватність способів, якими створилась та керується кібербезпека. Це

зрозуміло, якщо подивитись на дані про ескалацію кількості та наслідків кібератак, незважаючи на зростаючу цінність ринку кібербезпеки та посилення зусиль приватних та державних акторів покращити безпеку інформаційних систем та інфраструктури [479].

Відсутність ефективних заходів з кібербезпеки може потенційно вплинути на інформаційну революцію та розвиток інформаційних суспільств по всьому світу [328]. Без відповідних заходів безпеки кіберзагрози можуть підірвати стабільність інформаційних суспільств, зробивши цифрові технології джерелом ризиків, а не лише джерелом розвитку. Крім того, відсутність безпеки цифрових технологій зруйнує довіру користувачів до них, а це, у свою чергу, завадить впровадженню інновацій, насамперед, у публічному секторі.

Вивчення другого уроку тягне за собою перегляд рамок, що лежать в основі управління кібербезпекою. У цьому відношенні вже склався стійкий консенсус щодо трактування кібербезпеки як *суспільного блага*, яким слід керувати в інтересах суспільства [459; 514]. Ми повністю поділяємо цю точку зору, вважаючи при цьому, що головний наголос у забезпеченні кібербезпеки має робитись на публічному секторі як такому, що забезпечує функціонування всіх суспільних сфер.

«Кібер» є складовим елементом інформаційного суспільства, який переплітається з фізичними, економічними, соціальними та політичними елементами, і його безпека має важливе значення для розвитку суспільства, технологічного прогресу, а також для використання потенціалу цифрових технології для досягнення суспільно значущих результатів [476]. Тому кібербезпека охоплює широкий набір практик: оцінка ризиків і тестування проникнення; аварійне відновлення; криптографія; контроль та спостереження за доступом; мережева архітектура, програмне забезпечення та безпека; безпекові операції; фізична безпека тощо. При цьому кібербезпека має три основні складові: 1) інформаційно-комунікаційні системи, які є *надійними* і можуть протистояти атакам; 2) методи та системи

виявлення загрози та аномалій для забезпечення *стійкості* інформаційно-комунікаційних систем; 3) забезпечення системної *реактивності* на кібератаки.

Так, надійність вимірює розбіжність між фактичною і очікуваною поведінкою системи, коли спостерігаються помилки на вході або коли є помилки у виконанні. Система є більш або менш надійною залежно від величини розбіжності між реальною та очікуваною поведінкою. Надійність є важливою (хоча й недостатньою) для пом'якшення наслідків кібератак та забезпечення безперервності функціонування системи. У той же час, підвищення надійності системи є коштовним процесом: він вимагає точного проектування, а також верифікації та валідації коду, тестування та зондування на вразливості. Тому побудова надійності цифрових пристроїв може настільки впливати на їх вартість, що виробники можуть пожертвувати стійкістю в пошуку комерційної конкурентоспроможності. Це часто трапляється, наприклад, з IoT-технологіями, що може призвести до розповсюдження в глобальному масштабі пристроїв, стійкість яких є ефемерною.

Створення надійних інформаційно-комунікаційних систем має прямі та непрямі наслідки для публічних інтересів інформаційного суспільства, оскільки це дає можливість належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології. Це підкріплює висловлену вище думку, що кібербезпека є саме суспільним благом.

Надійність систем не обов'язково має бути безкоштовною для кінцевих користувачів, але дуже важливо, щоб її вартість не була дискримінаційним фактором, що визначає доступ до неї. Ключовим моментом тут є те, щоб гарантувати, щоб всі користувачі мали доступ до цифрових технологій, чия надійність адекватна цілям і контексту їх використання. За такого підходу публічний сектор повинен взяти на себе частину витрат на забезпечення кібербезпеки, які можуть включати в себе, наприклад, витрати, пов'язані з

встановленням стандартів і процедур сертифікації, а також витрати, пов’язані з тестуванням технологій, в той час як також забезпечуючи, щоб цифрові пристрої, наявні на ринку, відповідали необхідному рівню надійності.

Три важливі переваги випливають із управління кібербезпекою як суспільним благам: системний підхід до безпеки; спільна відповідальність між різними стейкхолдерами; розвиток співпраці у сфері кібербезпеки.

Системний підхід. Управління суспільним благом вимагає розгляду як прямих, так і непрямих зовнішніх чинників, а також середньо- і довгострокових наслідків. Це сприяє використанню підходів, спрямованих на визначення та аналіз взаємозалежностей щодо безпеки різних, але пов’язаних, технології та їх впливу на різні суспільні сфери.

Спільна відповідальність. Управління суспільним благом вимагає співробітництва між приватним і публічним сектором в цілях забезпечення високого рівня надійності відповідних систем та інфраструктур. Публічний сектор насамперед повинен встановлювати стандарти, здійснювати сертифікацію та тестування, процедури нагляду, щоб забезпечити підтримання достатнього рівня кібербезпеки для захисту та сприяння суспільним інтересам, а також вживати відповідних заходів, коли кібербезпека не забезпечується належним чином. У той же час, приватний сектор несе відповідальність за розробку надійних систем, розробку та вдосконалення методів забезпечення надійності послуг та продуктів, які вони пропонують, та співпрацює з публічним сектором для здійснення відповідного контролю. Визначення кібербезпеки як суспільного блага також покладає на користувачів певні обов’язки щодо їх кібергігієни.

Розподіл відповідальності між різними акторами, а також необхідність врахування прямих та непрямих зовнішніх ефектів сприяє *співпраці та обміну інформацією*. Обмін інформацією про уразливість різних систем, наприклад, є важливим для приватного сектора для гарантування надійності інформаційно-комунікаційних системи. У той же час, публічний сектор може підтримувати цю практику, включаючи обмін інформацією та співпрацю як

частину ініціатив та процедур щодо підвищення власної спроможності.

У загальному випадку «суспільне благо» є економічним, а не нормативним поняттям. Однак суспільства можуть вирішити розглядати щось як суспільне благо і на нормативному ґрунті, наприклад, для підтримки суспільних інтересів. Кібербезпека сама по собі не є суспільним благам, але через її важливу роль для наших суспільств, її слід розглядати як таке. При цьому, слід зазначити, що поняття кібербезпеки у цілому та в публічному секторі зокрема безпосередньо пов'язане з феноменом інформаційного суспільства та електронного врядування, що з'явилось внаслідок розвитку інформаційного суспільства. Тому нижче зупинимось на розгляді електронного врядування, але саме електронного *врядування* (e-governance), а не електронного *уряду* (e-government). І хоча про електронний уряд і електронне врядування написано багато, але ми хочемо розглянути останнє під дещо іншим кутом – як нову парадигму публічного управління що прийшла/приходить на зміну іншим у цій сфері.

Сфера публічного управління протягом своєї історії зазнала різноманітних змін, що можна, зокрема, побачити у п'яти парадигмах, визначених Генрі [353], до яких слід додати новітні парадигми, такі як Новий публічний менеджмент та належне врядування. Перебуваючи в інформаційному столітті, можна стверджувати, що впровадження ІКТ призвело до перетворення різних аспектів публічного управління, до виникнення та впровадження концепцій електронного уряду та електронного врядування.

Англомовний термін «e-governance» складається з двох частин: відповідно «електронний» і «врядування», тому слід визначати обидві ці частини для визначення «електронного врядування». «Електронний», представлений префіксом «е», стосується конвергенції комп'ютерів та комунікаційних технологій [422]. Що стосується другої частини, то низка авторів, зокрема, Пальвія та Шарма [377], Торнхілл [491] та Місурака [416] відзначаючи складність поняття врядування, стверджують, що врядування

стосується процесів та інституцій, як формальних, так і неформальних, які керують колективними цілями груп. Як наслідок, хоча уряди і можуть бути авторитетними для суспільства, але вони є лише одними із стейкхолдерів у врядуванні. Іншими стейкхолдерами є представники приватного сектору та неурядові організації, які в деяких випадках діють без державних повноважень. Чадвік [274, с. 31] стверджує, що врядування стосується всього кола відносин та інститутів, що беруть участь у процесі публічного управління, і основне питання тут полягає у тому, як влада взаємодіє із суспільством для прийняття взаємно прийнятних рішень і чи суспільство здійснює самокерування, а не чекає настанов від уряду.

Цікаво, що різні міжнародні органи визначають електронне врядування відповідно до їх поглядів на врядування у цілому. Наприклад, трактування врядування Світовим Банком пов’язане виключно з тим внеском, який воно робить у соціально-економічний розвиток шляхом економічної та структурної лібералізації. Тому для Світового Банку електронне врядування передбачає використання засобів ІКТ, щоб змінити спосіб взаємодії громадян та бізнесу з владою для того, щоб забезпечити залучення громадян до прийняття рішень, розширення доступу до інформації, більшу прозорість органів влади та зміцнення громадянського суспільства [290].

Бетнагар зауважує, що Світовий банк ставиться до електронного врядування як до використання інформаційно-комунікаційних технологій урядовими установами. Іншими словами, електронне врядування може бути визначене як надання публічних послуг та інформації населенню за допомогою електронних засобів. Ці технології дозволяють органам влади трансформувати відносини один з одним, громадянами, бізнесом, призводячи до кращого надання публічних послуг громадянам, поліпшення взаємодії з бізнесом, розширення можливостей громадян через доступ до інформації та, врешті-решт, до більш ефективного управління державою. Отримані переваги включать зменшення корупції, підвищення прозорості, більшу зручність в отриманні послуг, зростання публічних доходів та / або зниження

публічних витрат [244].

ПРООН пов’язує концепцію врядування з концепцією сталого людського розвитку, а електронне врядування розглядає як процес створення суспільної цінності із застосуванням сучасних ІКТ. Суспільна цінність при цьому визначається як поняття, укорінені в уподобаннях людей. З такої точки зори, електронний уряд є виправданим, якщо він розширює можливості публічного управління щодо збільшення пропозиції суспільної цінності, що у результаті має призводити до підвищення якості життя. Зосереджуючись більше на можливостях врядування, ПРООН вважає, що електронне врядування може «оснастити» людей для справжньої участі в політичному процесі, наслідком чого має стати поінформована суспільна згода, що стає все більш поширеною основою для легітимності влади. При цьому визначаються п’ять головних цілей електронного врядування: 1) створення послуг на основі вибору громадян; 2) підвищення рівня доступу до влади та публічних послуг 3) соціальна інклюзія; 4) відповідальне надання інформації; 5) ефективне використання ІТ та людських ресурсів [445].

Група публічного управління (PUMA) Організації економічного співробітництва та розвитку (OECD) фокусується на трьох основних компонентах електронного врядування: 1) інформація; 2) активна участь; та 3) суспільні консультації [453].

Уряди деяких країн, зокрема, Великої Британії та Індії, взяли за основу концепцію SMART для свого трактування електронного врядування. На їхню думку, електронне врядування є застосуванням ІТ у процесі функціонування органів влади для запровадження *простого, морального, відповідального, чуйного* та *прозорого управління* [290].

Узагальнюючи різні трактування електронного врядування, Торсон і Рагланд [492] з Maxwell School зазначають: «Термін «електронний уряд» охоплює широкий спектр діяльності, що передбачає вдосконалення операцій та послуг уряду, а також сприяє більший співпраці та змістовним відносинам з громадянами та іншими недержавними суб’єктами. Е-урядові ініціативи,

проте, в основному спрямовані на зміну урядової діяльності, структури і послуг, а не на визначення нової ролі і кола обов'язків для громадян».

Хікс [351] зауважує, що електронне врядування повинно охоплювати всі ІКТ, але ключовими є комп'ютерні мережі, – від інтрамереж до Інтернету, – що створюють широкий спектр нових цифрових зв'язків, а саме:

– зв'язки всередині влади: дозволяють досягти «об'єднаного мислення»;

– зв'язки між органами влади та неурядовими організаціями / громадянами: забезпечують посилення підзвітності;

– зв'язки між владою та бізнесом / громадянами: трансформують надання послуг;

– зв'язки всередині та між неурядовими організаціями: підтримують навчання та узгоджені дії;

– зв'язки всередині та між громадами: сприяють забезпеченню соціально-економічного розвитку.

Один з важливих наслідків використання нових технологій у врядуванні полягає в тому, що воно розширюється за межи внутрішньої операційної діяльності органів влади, включаючи надання електронних послуг громадськості та подальшу взаємодію між громадянином та владою. Цей потенціал інтерактивності можна визначити як один із найважливіших аспектів електронного врядування стосовно зміни характеру публічного управління у цілому.

Браун в одній зі своїх праць, на наш погляд, досить влучно визначив сутність електронного врядування. Він пише: «Більш широкий погляд на електронне врядування полягає в тому, що воно стосується всього спектру ролей та діяльності органів влади, що формуються та використовують інформаційно-комунікаційні технології (ІКТ). Електронне врядування дозволяє створити уряд, заснований на знаннях, в суспільстві, заснованому на знаннях. Тобто електронне врядування об'єднує два елементи, які раніше природним чином не були об'єднані. Перший – це середовище системи

публічного управління та суспільства у цілому, створене за допомогою електронних технологій, таких як електронна пошта, всесвітня мережа Інтернет, бездротові та інші ІКТ у поєднанні з моделями управління, такими як орієнтація на клієнта / громадянина та єдине вікно. Другий – це основна модель держави та публічного управління, що поєднує демократію, врядування та державний менеджмент» [256, с. 243].

Виходячи з цього визначення, електронне врядування має величезний потенціал для того, щоб громадяни перестали бути просто пасивними споживачами послуг, що пропонуються їм; електронне врядування дає можливість громадянам відігравати більш активну роль у визначенні тих послуг, які вони хочуть отримувати, і структури, завдяки якій ці послуги можна найкраще надати.

У свою чергу вже згадані Пальвія та Шарма стверджують, що «Електронне врядування - це використання інформаційних і комунікаційних технологій у публічному секторі з метою покращення надання інформації та послуг, заохочення участі громадян у процесі прийняття рішень та підвищення рівня відповідальності, прозорості й ефективності діяльності органів влади. Електронне урядування включає в себе нові стилі керівництва, нові способи обговорення і прийняття рішень, нові способи доступу до знань, нові способи з’ясування думки громадян і нові способи організації і надання інформації та послуг. Електронне урядування є як правило, розглядають як більш широке поняття, ніж електронний уряд, оскільки воно може призвести до зміни способу взаємодії громадян з органами влади та один з одним. Електронне врядування може сприяти виникненню нових концепцій громадянства, як з точки зору потреб громадян, так і їхніх обов’язків. Його мета – залучити громадянина до публічного управління, та розширити його можливості у цій сфері» [377, с. 3].

Можна бачити, що дане визначення стосується широкого спектру аспектів управління публічним сектором з акцентом на те, як використання ІКТ сприяє належному врядуванню. Однак, визначення акцентує і на тому,

що електронне врядування призвело до серйозних змін у способі надання публічних послуг. Як зауважували Мухаммед та Абу Момтаз [422, с. 33], впровадження ІКТ у врядуванні призвело до заміни таких двох відомих елементів як праця та капітал інформацією та знаннями. І у цьому сенсі Інтернет створив той же самий прорив, який створив друкарський верстат у п’ятнадцятому столітті. Ми повністю погоджуємось з авторами з цього приводу, хоча і не погоджуємось з тим, що вони у своїй роботі «Розуміння електронного врядування: теоретичний підхід» [422] використовують поняття електронного врядування та електронного уряду взаємозамінно, так, ніби вони означають одне й те саме.

Масерумюле [404, с. 77] визначає електронний уряд як прагматичне використання інноваційної інформації, комунікацій та технологій, таких як Інтернет, для надання ефективних послуг, інформації та знань. З цього визначення, електронний уряд, як правило, зосереджується на операційній діяльності органів влади, з особливим наголосом на питаннях ефективності та результативності. Але це позбавляє громадян від усього процесу прийняття рішень і тим самим робить їх пасивними отримувачами рішень з боку органів влади і публічних послуг.

Суттєва різниця між електронним врядуванням та електронним урядом полягає в тому, що перше виходить за рамки другого. Електронне врядування не стосується лише веб-сайтів та електронної пошти, воно змінює по суті відносини між державними установами та середовищем, що включає бізнес та громадянське суспільство. Тому електронний уряд слід розглядати лише як складову електронного врядування.

Деякі автори також опосередковано ототожнюють електронне врядування з електронною демократією, що також, на наш погляд, є хибним. Хоча немає загального консенсусу щодо визначення поняття «електронна демократія», узагальнюючи різні погляди та думки її можна визначити як використання ІКТ та стратегій «демократичних секторів» у політичних процесах на рівні місцевих громад, регіонів, націй та на світовій арені. І у

цьому сенсі електронну демократію слід розглядати як розширення електронного уряду.

Здається, немає загальної думки щодо того, звідки і коли дійсно розпочалося електронне врядування, так само, як і науковці не чітко визначають появу електронного уряду, що з'явився до електронного врядування. Як показав аналіз відповідної літератури, автори мають тенденцію показувати ретроспективні події в галузі електронного врядування або електронного уряду в контексті окремих країн або регіонів. Також часто стверджується, що витоки електронного управління в усьому світі тісно пов'язані з концепцією «Інформаційна супермагістраль» («Information Super Highway»), яка приписується колишньому віце-президенту Сполучених Штатів Америки Ал Гору у 1990-х роках. Інформаційна супермагістраль як поняття визначалась значною мірою з точки зору інформаційної інфраструктури на національному рівні такими країнами, як Канада, Сполучені Штати Америки, Великобританія, Австралія та Індія.

Як стверджує Пабру [444, с. 5], в цей період акцент робився на розвитку компонентів інфраструктури, таких як волоконно-оптичні мережі, як усередині різних держав, так і між державами. З часом інтерес перейшов до соціально-економічних аспектів, що було пов'язано з розвитком концепції інформаційного суспільства або суспільства знань, яка, серед іншого, охоплювала електронне управління. Спочатку було зосереджено увагу на впровадженні інформаційних систем у державних відомствах та державних установах. Однак, як зазначав Пабру [там само], такі ранні спроби електронного врядування не отримали широкого схвалення урядів, і, отже, у більшості випадків не вдались.

У свою чергу Мухаммед та Абу Момтаз [422, с. 34] стверджують, що основна ідея електронного врядування пов'язана з мантрою «розміщення уряду в Інтернеті», яка вперше з'явилася в технологічно розвинених західних країнах у 1990-х роках. На цих ранніх стадіях акцент робився на зменшенні публічних витрат за рахунок підвищення ефективності, і мало згадувалося

про участь громадян в управлінні.

Ще одним важливим моментом, який слід зазначити в еволюції електронного врядування, є те, що адаптація ІКТ в публічному секторі, як правило, відстає від такої у приватному секторі. У 1980-х та 1990-х роках комерційні організації все більше приймали та використовували ІКТ для підвищення якості своїх послуг для клієнтів, що сприяло підвищенню ефективності, швидкості та зручності послуг приватного сектору. Впровадження ІКТ у бізнесі називалося електронною комерцією, що включало використання банкоматів, електронних покупок, інтеграції кабельного телебачення з Інтернетом та багато іншого. Таким чином, діяльність в галузі електронної комерції включала функціонування інформаційних систем у бек-офісах, а також таких, що забезпечували взаємодію з клієнтами. Тим часом усі ці заходи не стосувались операційної діяльності органів влади, які лише пізніше приєднались до спроб використання ІКТ у своїй діяльності. Причому початкові розробки електронного врядування призвели лише до часткової автоматизації діяльності органів влади, зокрема, щодо надання публічних послуг.

На думку дослідників, (див., напр., [1]) електронне врядування у будь-якій країні розвивається відповідно до чотирьох етапів: інформування, взаємодія, трансакція, трансформація. Але на наш погляд, до цих чотирьох етапів слід додати ще п’ятий – інституціоналізацію (рис. 1.1).

1. На *першому етапі* електронне врядування означає бути присутнім у мережі Інтернет, надаючи громадськості та бізнесу (G2C та G2B) відповідну інформацію. Формат веб-сайтів органів влади на даному етапі подібний до формату брошури чи листівки. Цінність для громадськості полягає в тому, що багато інформації про діяльність органів влади стає загальнодоступною, що підвищує їх прозорість і відкритість. Внутрішньо (G2G) органи влади також можуть поширювати інформацію один для одного електронними засобами, такими як Інтернет.

2. На *другому етапі* взаємодія між владою та громадськістю, між

владою та бізнесом (G2C і G2B) стимулюється різними програмами. Є можливість задавати питання електронною поштою, користуватися пошуковими системами та завантажувати форми та документи. Все це заощаджує час і надає можливість доступу 24 години на добу. Внутрішньо (G2G) органи влади використовують локальні мережі, інтранет та електронну пошту для спілкування та обміну даними.

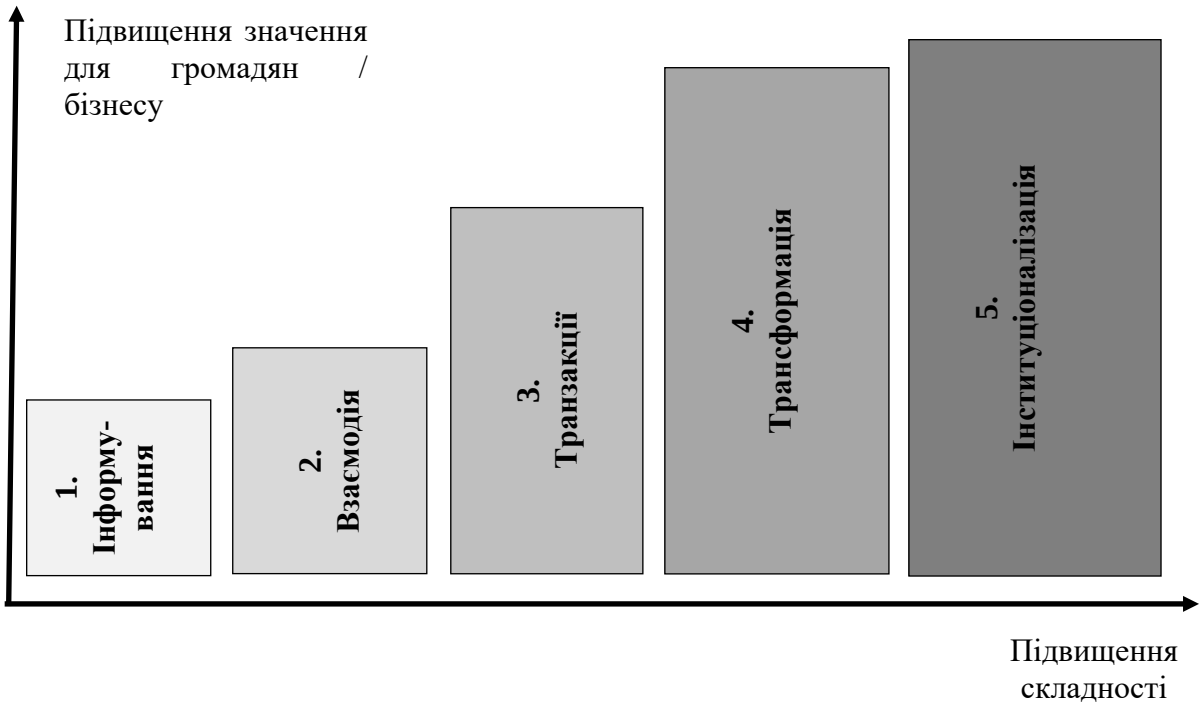

Рис. 1.1. Етапи розвитку електронного врядування

3. На *третьому етапі* складність технологій зростає, але зростає й їхня цінність для клієнтів (G2C і G2B). Можна здійснити певні повні операції, не відвідуючи органи влади. Прикладами таких онлайн-сервісів є подання податку на прибуток, подання податку на майно, продовження / поновлення ліцензій, отримання паспортів і віз та онлайн-голосування. У відносинах з бізнесом органи влади впроваджують заявки на електронні закупівлі. Внутрішні процеси (G2G) повинні бути перебудовані, щоб забезпечити якісне обслуговування. Третій етап складний через проблеми безпеки та

персоналізації. Так, для забезпечення легальної передачі послуг знадобляться цифрові (електронні) підписи, що може потребувати внесення змін до законодавства.

4. *Четвертий етап* – це досягнення такого стану, коли всі інформаційні системи інтегровані і громадськість може отримати послуги G2C та G2B за одним (віртуальним) аккаунтом. Кінцевою метою цього етапу є створення єдиної точки контакту для всіх служб. Складність у досягненні цієї мети має головним чином внутрішнє походження, адже виникає необхідність кардинальної зміни культури, процесів та відповідальності в рамках системи органів влади (G2G). Зокрема, публічні службовці в різних органах і відомствах повинні спільно працювати плавно і безперешкодно. На цьому етапі економія витрат, ефективність та задоволеність клієнтів досягають найвищих можливих рівнів.

5. *П'ятий етап* – це перехід до інтерактивної демократії. На додаток до інтегрованих та повністю виконуваних онлайн-сервісів, пропонується можливість персоналізації веб-сайтів. Завдяки цим та іншим додатковим функціям відвідувачі можуть персоналізувати веб-сайти, надавати відгуки, коментарі та користуватися безліччю складних функцій, розроблених для підвищення демократичної чуйності та відповідальності керівництва органів влади.

Після спроби простежити походження електронного врядування, доцільно стисло окреслити різні парадигми в публічному управлінні з метою обґрунтування, чому електронне врядування насправді має розглядатися як окрема парадигма у цій сфері.

На думку Сомеха та Левіна [468, с. 207], парадигма – це «світогляд, загальна перспектива, спосіб розбиття складності реального світу...». Надалі автори підкреслюють складність розуміння цього терміну, наводячи як приклад Куна, який у 1970 р. першим використав цей термін у своїй роботі, але згодом застосував його більше двадцяти разів у різних значеннях [там само]. У свою чергу, Генрі [353, с. 378], хоча визнаючи, що термін

«парадигма» є дещо перевантаженим, вказує на те, що немає іншого кращого терміну, який би передав концепцію самоідентичності певної сфери та визначення її динаміки. Поділяючи цю думку Генрі, ми використовуємо нижче поняття «парадигма» саме для позначення самоідентичності публічного управління та визначення динаміки його розвитку.

Парадигма 1: Політико-адміністративна дихотомія (1900 – 1926 рр.).

Ключовим аспектом цієї парадигми було відмежування публічного управління від політики. За словами Генрі, один з відомих науковців того часу, Гудноу, стверджував, що політика, яка стосується «стратегічних речей» у вигляді публічних політик у різних сферах, повинна бути відокремлена від публічного управління, що пов'язане з реалізацією цих політик [353, с. 379]. Поділ влади на три гілки розглядався як ще одне підтвердження цього поділу політичних і адміністративних функцій уряду. Суттєва увага в цій парадигмі також приділялась місцю публічного управління серед інших соціальних наук. З цього приводу існували дві думки. Перша, якої дотримувався, зокрема, Гудноу, наголошувала на тому, що публічне управління є самостійною академічною дисципліною і науковою галуззю; у той час, як з точки зору другої публічне управління є частиною політології.

Парадигма 2: Наукове публічне управління (1927 – 1940-ві рр.).

Ця парадигма пов'язана з формулюванням перших засадничих наукових принципів публічного управління. У цей період (1930-ті та 1940-ві роки) також відчувався високий попит на державних адміністраторів як у публічному, так і у приватному секторі, що було пов'язано з їхнім управлінським досвідом.

Ф. Віллоубі у своїй праці «Принципи публічної адміністрації», яка вийшла у 1927 р., стверджує, що якщо державні адміністратори повинні бути експертами в своїй роботі, їм доведеться засвоїти певні принципи у цій галузі [353, с. 379]. Інші автори, Л. Х. Гулік та Л. Урвік у 1937 р. теж висловили думку про важливість формулювання та дотримання науково обґрунтованих принципів у публічному управлінні. Одним із важливих аспектів

аргументації цих авторів було їх наполягання на тому, що адміністративні навички не мають меж, інакше кажучи, адміністрація в приватному та державному секторі є подібною [491, с. 795].

Парадигма 3: Державне управління як політична наука (1950-ті – 1970-ті рр.).

У цей період науковці активно переглядали місце публічного управління як наукової галуззі, переважно вважаючи його як одну з політичних наук. Також дещо знизився інтерес до публічного управління як науки, особливо у США. Уолдо відзначив ворожнечу, яку проявляли політологи до своїх колег у публічному управлінні; він заявив, що науковці з публічного управління відчували себе поза мейнстрімом тодішньої науки [353]. Крім того, науковці того часу суттєво критикували ідею Вільсона щодо дихотомії політики та управління, вважаючи її нездійсненою на практиці.

Парадигма 4: Публічне управління як адміністративна наука (1956 – 1970-ті рр.).

Ця парадигма виникла головним чином внаслідок зневаги, яку виявили до публічного управління політологи. На думку прибічників цієї парадигми, публічне управління є саме адміністративною наукою, адже адміністрування є адмініструванням незалежно від того, де воно здійснюється. Також акцентувалось на тому, що в основу публічного управління має бути покладена організаційна теорія. Але поряд з цим на відміну від попередньої дана парадигма прагнула відкинути «публічність», вважаючи, що немає різниці між адмініструванням у публічному, приватному або третьому секторі. Це певним чином «розмивало» межу між приватною та публічною сферами.

Парадигма 5: Публічне управління як міждисциплінарна наука (1970-ті – ?)

За словами Генрі [353, с. 383], на початку 1970-х років приділення уваги місцю публічного управління серед інших соціальних наук зменшується, адже публічне управління починає вважатися самостійною, але

міждисциплінарною наукою. Міждисциплінарний характер публічного управління став усвідомлюватися все більше, коли науковці в цій галузі почали цікавитись суміжними галузями, такими як політологія, політична економія, соціологія та інші. Одним із важливих моментів є те, що, спираючись на організаційну теорію та науку про управління, науковці з публічного управління намагалися створити автономну навчальну програму з гносеологічною унікальністю. Це призвело до того, що в університетах публічне управління почало викладатись як самостійна галузь, а не частина політичних наук або менеджменту.

Парадигма 6: Публічне управління як новий публічний менеджмент (1991– ?)

У рамках даної парадигми увага акцентується на тому, як зробити владу більш економічною та ефективною у наданні послуг населенню. У цей період створюється багато моделей, що отримали загальну назву Нового публічного менеджменту (НПМ). За словами Міноуг, Полідано і Хулме [414], щоб НПМ був реалізованим необхідно зробити наступне:

1. Реструктуризацію публічного сектору, зокрема, шляхом приватизації.
2. Реструктуризацію та скорочення публічної служби, особливо на центральному рівні.
3. Запровадження змагальності, зокрема, через створення внутрішнього ринку публічних послуг та аутсорсингу щодо надання публічних послуг для приватного сектору.
4. Підвищення ефективності, особливо за допомогою аудиту та вимірювання ефективності.

Міноуг, Полідано та Хулме [там само] далі висловили думку, що вищезазначені реформи породжуватимуть публічне управління, яке характеризується :

1. Розмежуванням стратегічної політики від операційного управління.
2. Занепокоєнням результатами, а не процесами.

3. Орієнтацією на потреби клієнтів, а не на бюрократичні організації.

4. Зміною акценту з прямого надання публічних послуг на користь керівної ролі у цьому процесі.

5. Трансформованою бюрократичною культурою.

НПМ, який суттєво переосмислює відносини між державою та ринком, повинен був замінити «соціальну» модель держави. Тому невипадково, що НПМ користується популярністю серед домінуючих політичних еліт, оскільки, у певному сенсі, слугує їхнім інтересам більше, ніж інтересам широкої громадськості. І це згодом стало предметом критики з боку багатьох науковців. Також одним з найважливіших закидів до НПМ була його спрямованість на скорочення витрат та зниження податків, що було головним питанням «розвиненого світу» і не охоплювало питання розвитку потенціалу та проблем розвитку «світу, що розвивається».

Парадигма 7: Державне управління як врядування (1990-ті – ?)

Парадигма нового публічного менеджменту занадто дбала про те, як органи влади можуть досягати своїх цілей стати економічними й ефективними у наданні послуг населенню в ліберальному середовищі, де індивідуальні переваги домінують над колективними [414]. Для того, щоб уникнути недоліків НПМ була запропонована концепція врядування, а згодом належного врядування.

Бов'є і Лоффер [252, с. 9] зазначають, що концепція врядування, як вона використовується в публічному секторі, бере свій початок від приватного сектору, де концепція «корпоративного врядування» вперше була запропонована у відповідь на проблеми контролю та прийняття рішень у приватних структурах. За словами Торнхілла [491, с. 803], концепція врядування увійшла в сферу публічного управління ще у 1980-х роках як теоретична конструкція, але набула поширення лише у другій половині 1990-х років.

Парадигма врядування наголошує на переході від розгляду органів влади як єдиного драйвера суспільного розвитку до визначення та визнання у

цьому процесі інших стейкхолдерів, а саме громадян та бізнесу як однаково здатних формувати публічний дискурс та брати участь у керуючих процесах. Врядування, як поняття, хоч і відображає об'єднання суспільних стейкхолдерів в процесі управління, не має універсального значення. Бов'є і Лоффер [252] роблять спробу спростити це поняття, зазначаючи, що у врядуванні «важливо не те, що ми (в уряді) робимо, а як люди ставляться до того, що ми робимо». У свою чергу Міністерство міжнародного розвитку Великобританії, а також такі автори як Міноуг, Полідано та Хулме [414] стверджують, що врядування повинно охоплювати чотири основні аспекти. По-перше, це легітимність органів влади. По-друге, підзвітність, яка передбачає існування механізмів і систем, які забезпечують, що посадові особи та носії політичних посад нестимуть відповідальність перед людьми за свої дії чи бездіяльність та (не)використання публічних ресурсів. По-третє, компетентність публічних службовців та установ у здійсненні публічної політики, що призводить до ефективного надання послуг. По-четверте, у всій системі публічного управління повинно бути дотримання закону та захист прав людини.

В рамках парадигми врядування, публічне управління може розглядатися як складова частина «належного врядування». Пишучи про належне врядування, Масермюле [405, с. 558] робить висновок, що це концептуальна проблематика, яка досі потребує контекстуального теоретизування. Місурака [416, с. 13] намагається визначити належне врядування як процес, який стосується розподілу ресурсів для реагування на колективні проблеми. Далі автор з посиланням на ПРООН визначає наступні як ключові принципи належного врядування: прозорість, підзвітність, участь, верховенство права, ефективність та стратегічне бачення. У цілому, належне врядування можна зобразити таким чином (рис. 1.2).

Наведений рисунок показує, що різні автори розглядають як ключові компоненти для належного врядування: ефективний уряд, успішний приватний сектор плюс ефективне громадянське суспільство, які

використовують у взаємодії партисипативний підхід. У свою чергу, «неналежне врядування», на думку Місураки [416], характеризується персоніфікацією влади, корупцією, а також безвідповідальністю.

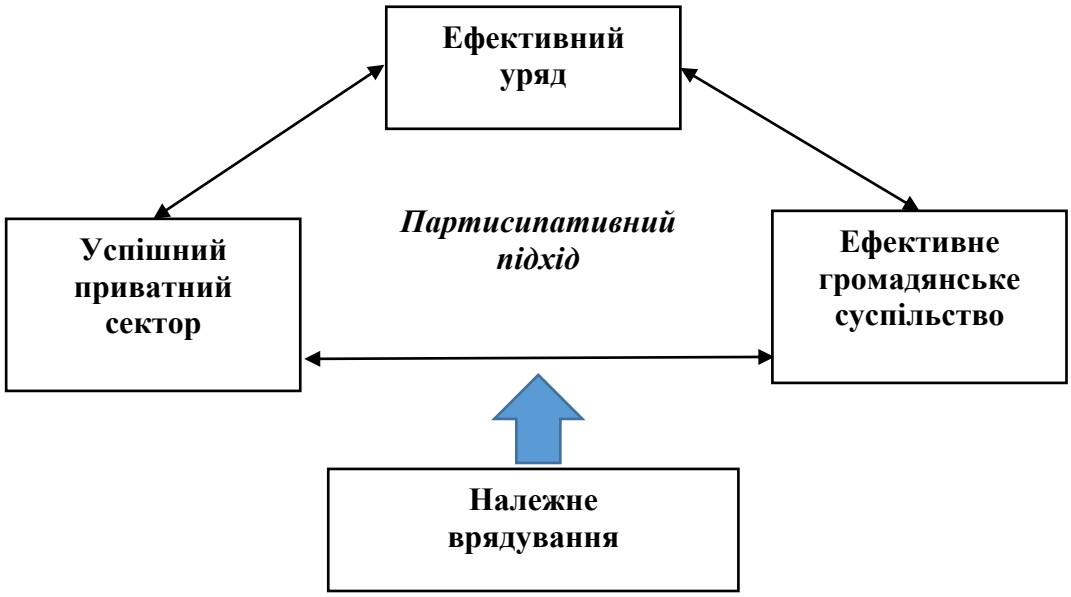

Рис. 1.2. Ключові компоненти належного врядування

Парадигма 8 (?). Публічне управління як електронне врядування.

З точки зору парадигм у сфері державного управління, електронне врядування можна розглядати з різних позицій. По-перше, якщо аргумент Чадвіка [274, с. 179] про те, що впровадження ІКТ в управлінні в основному сприяв тому, щоб уряд був ефективним у наданні послуг, буде висунутий на перший план, електронне врядування може розглядатись як складова нового публічного менеджменту, оскільки саме тут переважала тема ефективності та результативності влади. У цьому випадку впровадження ІКТ в уряді може розглядатися лише як інструмент, який покликаний забезпечити досягнення цілей НПМ. Однак ця думка ігнорує той факт, що у сфері електронного врядування ІКТ використовуються не лише в операційній діяльності органів влади, а радше використовуються для взаємодії органів влади і посадових осіб з іншими суспільними стейкхолдерами.

По-друге, можна стверджувати, що впровадження ІКТ в управлінні публічними справами посилило демократичні практики в суспільстві. Особливо це стосується покращення обміну інформацією між органами влади та іншими суспільними стейкхолдерами. Зокрема, ІКТ дають можливості як органам влади, так і громадянам взаємодіяти один з одним, тим самим покращуючи належне врядування. Оскільки впровадження ІКТ в публічному управлінні мають на меті покращити доступ, прозорість та підзвітність, то у цьому випадку електронне врядування можна розглядати як складову концепції врядування/належного врядування.

Проте, на наш погляд, електронне врядування слід розглядати як самостійну парадигму публічного управління, оскільки впровадження ІКТ *суттєво* змінило його характер. Це вірно, як з точки зору внутрішньої діяльності органів влади (G2G), так і з точки зору їх взаємодії з іншими стейкхолдерами (G2C та G2B). Слід визнати і те, що електронне врядування сильно впливає на розвиток і в інших галузях, таких як технології інформаційно-комунікаційні технології та електронна комерція, які у свою чергу впливають на електронне врядування. Нижче представлений рис. 1.3, що ілюструє взаємовплив електронного врядування та інших сфер і секторів.

Рисунок 1.3 ілюструє, що в той час як розвивалось публічне управління, відбувався розвиток і в інших сферах, що мало вплив на електронне врядування, як ми це знаємо сьогодні. Основний внесок, безумовно, стосується сфери ІКТ, оскільки будь-які події в цій сфері мали безпосередній вплив на впровадження та використання ІКТ в органах влади.

Як було зазначено раніше, впровадження корпоративного врядування в приватному секторі вплинуло на парадигму врядування в публічному управлінні, отже, на електронне врядування. Електронне врядування також значною мірою залежить від впровадження ІКТ інститутами громадянського суспільства.

Таким чином, хоча можна стверджувати, що електронне врядування може бути «вписаним» або в парадигму нового публічного менеджменту, або

у парадигму врядування, на наш погляд, електронне врядування є новою парадигмою публічного управління, оскільки електронне врядування не лише кардинально змінює і переосмислює взаємодію між органами влади та іншими суспільними стейкхолдерами, а й запроваджує новий спосіб координації, планування, формулювання та реалізації рішень й дій у публічному управлінні.

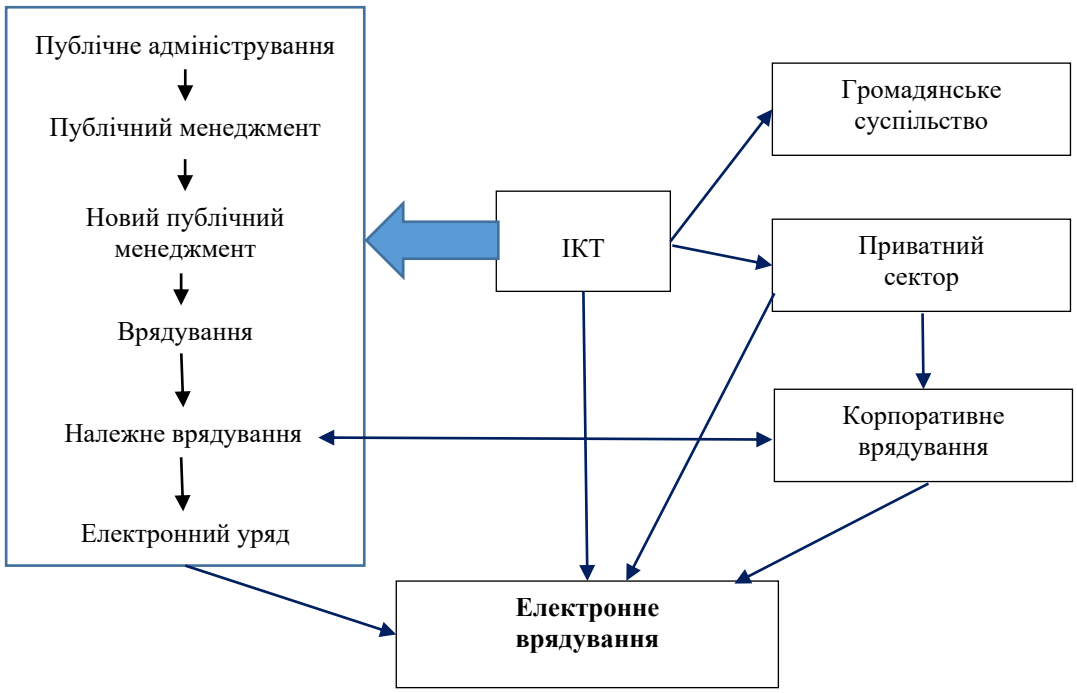

Рис. 1.3. Взаємовплив електронного врядування та інших сфер і секторів

Реформування публічного управління, частиною якого є впровадження електронного врядування, можна спостерігати як загальносвітову тенденцію, що простежується у багатьох країнах. І це не просто експерименти щодо впровадження нових режимів надання послуг, оскільки електронне врядування неминуче також охоплює (і керується) новими моделями формування політики, новими моделями участі громадян у публічному управлінні та політичних процесах, новими моделями відносин громадян і влади, новими варіантами соціально-економічного розвитку.

Швидкому впровадженню електронного врядування сприяють, як зазначалось, динамічні технологічні та телекомунікаційні інновації. Органи влади усього світу з метою перетворення структури управління та процесів управління з традиційної на електронну форму передають величезні масиви інформації в Інтернеті, автоматизуючи колись громіздкі процеси та взаємодіючи в електронному вигляді зі своїми громадянами. Але електронне врядування також представляє нові виклики довірі громадян до органів влади. Необхідно забезпечити безпеку цифрових транзакцій та комунікацій; конфіденційність повинна бути захищена, а громадяни повинні мати можливість контролювати особисті дані та того, хто має доступ до них. І це знов-таки підкріплює висловлену вище тезу про те, що кібербезпека є суспільним благом.

1.2. Кібербезпека у публічному секторі

Глобальна взаємопов’язаність невпинно зростає та поширюється. За оцінками Міжнародного союзу електрозв’язку (МСЕ), спеціалізованої агенції Організації Об’єднаних Націй (ООН), наприкінці 2010 року вже два мільярди людей були онлайн; очікується, що до 2015 ця кількість сягне п’яти мільярдів. Також МСЕ нараховує 143 країни, які вже пропонують послуги 3G, забезпечуючи можливість доступу в Інтернет через смартфони для дедалі більшої частини з приблизно 5,3 мільярдів осіб, що підписані на мобільні послуги. 3,8 мільярда з них знаходяться в країнах, що розвиваються.

Нажаль, що більше ми перебуваємо онлайн, то більше стаємо уразливими до кіберзагроз. У дисертаційній роботі ми досліджуємо тенденції та стратегії з усього світу, щоб підвищити рівень обізнаності та запропонувати комплекс пріоритетних заходів із забезпечення кібербезпеки в публічному секторі. У широкому сенсі це може бути визначено, як політика заходів зі зниження вразливості комп’ютерних систем, у тому числі й веб-

сайтів, та їх захисту від несанкціонованого доступу або нападу.

Щоб зрозуміти кібербезпеку в публічному секторі, слід усвідомити конвергенцію трьох основних чинників: глобалізації, ступеню підключення до мережі, та тенденції до надання послуг публічному сектора в Інтернеті, що зазвичай називають електронним урядом (е-урядом).

Інтернет пропонує загальну платформу, за допомогою якої кожен може віртуально взяти участь у глобалізації. Доступ до веб-сайту в одній країні так само простий, як і в іншій, й люди в усьому світі користуються такою можливостю. За даними сайту світової статистики Інтернету (https://www.internetworldstats.com) на початку 2019 року, кількість користувачів Інтернету за попередні 10 років збільшилася на 445% до рівня глобального поширення у 29%. Враховуючи переваги інформаційно-комунікаційних технологій (ІКТ), країни усього світу також наполегливо працюють над тим, щоб залучити решту своїх громадян до Інтернету. За даними доповіді консультаційної групи досліджень інституту McKinsey Global Institute станом на травень 2011 року, частка Інтернету у ВВП становить 3,4% у країнах великої вісімки (G8), у Південній Кореї, Швеції, Бразилії, Китаї та Індії. Серед країн зрілої економіки він оцінювався на рівні 21% приросту ВВП за останні п’ять років.

За даними Статистичної служби Європейського Союзу, у 2002 році 39% домогосподарств у 15 країнах ЄС мали доступ до Інтернету; на початок 2010 року відповідний показник становив вже 68%. У 2000 році 30% домогосподарств Південної Кореї мали широкосмуговий доступ до мережі; у 2009 році цей показник становив 96%. У Сполучених Штатах цей показник за той самий час збільшився з 4% до 64% [276]. Наведені показники відповідають й даним Організації економічного співробітництва та розвитку (ОЕСР), яка також повідомляє, що середня ціна щомісячної підписки на широкосмуговий доступ у 2010 році впала приблизно до 40 доларів США.

Час перебування людей в он-лайні також збільшується. У 2018 році, за даними компанії зі США з вимірювання та аналітики медіа ComScore

(https://www.comscore.com), середній громадянин США витрачав на Інтернет 32 години щомісяця, незважаючи на те, що приблизно п’ята частина населення залишається повністю непідключеною до мережі.

Наша довіра до Інтернету, ймовірно, зростатиме. Розробка технології радіочастотної ідентифікації (RFID) у поєднанні із впровадженням 6 версії протоколу Інтернету зробила можливим, наприклад, створення «Інтернету речей», що технічно надає можливість підключити до Інтернету будь що, включаючи повсякденні об’єкти, як от автомобілі. Чому б не мати можливість віддалено розблокувати автомобіль у разі надзвичайної ситуації, або не встановити у ньому бездротове обладнання для покращення можливостей комунікації?

З огляду на переваги Інтернету публічному сектор теж його використовує. Найчастіше згадуваний приклад підвищення ефективності – податки. У 2019 році шведський податковий орган очікував, що 65% людей подаватимуть інформацію про податки онлайн, що заощаджує час, зусилля та кошти уряду, та водночас полегшує життя виборців. Як чітко зазначено у Звіті ООН щодо світового публічному сектору 2013 року, «уряди усе більше усвідомлюють важливість використання електронного уряду для покращення надання громадянам послуг державного сектору» [500, с. 128]. Але Інтернет-середовище також виходить за рамки надання простих сервісів і надає урядам на всіх рівнях змогу покращити можливості обліку, розвиток, ефективність та прозорість.

Різноманітні міжнародні огляди показників електронних урядів демонструють великий прогрес за попередні десять років та підтверджують переконання у тому, що більшість країн світу вже «електронно-готові». Отже, у випадку ООН, вимірювання показників перейшло від «готовності» до фактичного «розвитку». Щоб підкреслити цю тенденцію, консалтингове агентство досліджень та аналізу Групи Economist (The Economist Intelligence Unit, EIU) навіть змінило назву свого рейтингу, який щорічно створювався вже протягом 10 років. Рейтинг «електронної готовності» у 2018 році

перетворився на рейтинг «цифрової економіки». Ілюстрацією того, наскільки швидко може відбуватися розвиток, можуть бути дані, що наведені у дев'ятому звіті про показники е-урядів Європи: середня доступність 20 важливих онлайн послуг державного сектору у 27 країнах ЄС зросла з 69% у 2015 році до 82% у 2018 [311].

Хоча попит на електронне урядування (його використання) відстає від пропозиції (його доступності), повсюди органи влади переконують громадян користуватися їхніми послугами та скористатися перевагами онлайн-інформації. Наразі у 27 країнах ЄС 42% осіб віком від 16 до 74 років використовують Інтернет для взаємодії з органами державної влади. Ключова мета Цифрової програми, стратегії ЄС щодо використання цифрових інструментів для розвитку економіки, - збільшити цю кількість до 2025 року до 70%. Включення в Інтернет, або електронне включення, також є одним із семи центральних стовпів Цифрової програми, й спрямоване на підвищення цифрових грамотності, навичок та включення. Згідно з опитуванням Pew Internet and American Life Project (дослідницький неприбутковий проект щодо Інтернету, технології, та життя у США, https://www.pewinternet.org) у 2017 році, 61% усіх дорослих у США шукали інформацію або виконували дії на урядовому веб-сайті за попередні 12 місяців [447].

Зусилля щодо переведення активності уряду у режим онлайн усе частіше зустрічаються на всіх рівнях урядів, та в усьому світі. В одних випадках це відбувається задля зовнішніх цілей, щоб задовольнити попит користувачів на персоналізовані пропозиції за допомогою різних каналів, таких як мобільний уряд (м-уряд) та інструменти Web 2.0. В інших – із внутрішніх причин ефективності, щоб працювати з секретною інформацією або підключити електростанції до Інтернету. Хоча, безумовно, рушійною силою є ефективність, але також державний сектор піддається усе зростаючому тиску використовувати Інтернет задля прозорості.

Для прикладу, Декларація міністрів ЄС 2009 року про електронне урядування у Мальме, Швеція, закликала до посилення онлайн-прозорості як

засобу сприяння підзвітності та довірі до влади. У Сполучених Штатах президент Барак Обама пообіцяв «безпрецедентний рівень відкритості в уряді», й одразу стикнувся із витоком конфіденційної урядової інформації Вікілікс (WikiLeaks). За даними CNN, тоді офіс Білого дому з управління та бюджету надіслав меморандум від 3 грудня 2010 року, що забороняв неуповноваженим працівникам федерального уряду отримувати доступ до веб-сайту та читати секретні документи. Це ще один приклад виникнення проблем кібербезпеки.

Відповідно до щорічного опитування федеральних керівників інформаційних служб (CIO) у США у березні 2010 року, проведеного Торговою асоціацією інформаційних технологій (TechAmerica, https://www.techamerica.org), CIO теж схвильовані щодо відкритого уряду, але також вони стурбовані кібербезпекою, вважаючи її своїм найбільшим викликом, що випереджає інші питання, такі як інфраструктура, робоча сила, управління, ефективність, підзвітність та закупівлі.

Глобалізація та Інтернет зумовили зростання нових можливостей державного сектору для підвищення внутрішньої ефективності та кращого обслуговування виборців у формі електронного уряду. Але зі збільшенням кількості користувачів та зростанням опори на Інтернет, цифрові інструменти також піддають публічний сектор великим ризикам, отже звідси витікає важливість кібербезпеки.

Як колись заявив Вальтер Врістон, колишній голова Сітібанку (Citibank), у взаємопов’язаному світі інформаційні мережі вразливі для нападу будь-кого та у будь-який час [528]. Цифри доводять його думку.

Багато керівників інформаційних служб (CIO) заявляють, що вони щодня бачать мільйони зловмисних спроб отримувати доступ до їхніх мереж. Згідно з опитуванням федеральних CIO, проведеним TechAmerica, учасники стурбовано відзначають «зростання кібератак, підтримуваних країнами, які шукають секретну інформацію або способи контролю ключових частин наших військової та критичної інфраструктури» [478, с. 7].

Згідно зі «Звітом про загрози у IV кварталі 2019 року» безпекової компанії McAfee, спостерігається зростання цілеспрямованих атак, збільшення досвідченості та зростання кількості атак на нові класи пристроїв, які, здається, з'являються регулярно. У звіті зазначається, що наприкінці року зловмисне програмне забезпечення досягло свого найвищого рівня ніж будь коли раніше. У 2019 році компанія McAfee виявляла близько 65 000 таких загроз щодня.

Опитування 2100 респондентів у 27 країнах про стан безпеки підприємств, проведене у 2010 році безпековою компанією Symantec (https://www.symantec.com), виявило, що три чверті всіх підприємств зазнали кібератак у попередньому році, і всі вони зазнали кібервтрат, таких як крадіжка інформації, втрата продуктивності чи втрата довіри клієнтів [475].

Опитування 217 керівників вищого рівня у сфері інформаційних технологій з федеральних організацій США, проведене у 2016 році консультаційним відділом інституту Ponemon, показало, що 75% респондентів зазнали одного або більше випадків зламу даних у попередньому році. За даними цього ж опитування, 71% респондентів заявили, що кібертероризм зростає [450].

Кібер-загрози можна класифікувати декількома способами, один з яких – порівняння політично вмотивованих загроз (наприклад, кібервійна, кібертероризм, кібершпигунство та хактивізм – хакерство в політичних цілях) із неполітичними (зазвичай фінансово мотивованими, як то кіберзлочин, крадіжка інтелектуальної власності та шахрайство, а також злам для розваги чи відплати, наприклад, від незадоволеного працівника). Цікавою в цій класифікації є усвідомлення того, що міжнародна співпраця є складною щодо політично мотивованих загроз, оскільки хтось, ймовірно, може захищати злочинців. Водночас існує тенденція до широкого порозуміння у боротьбі з кіберзлочинністю, оскільки більшість урядів зацікавлені в цьому.

Метою політично мотивованих атак є зазвичай порушення роботи різних служб. Додатковим наміром може бути також завдання фізичної

шкоди. Поширений підхід полягає у використанні так званого бот-нету (мережі ботів), коли використовується якась кількість інфікованих комп'ютерів (агентів), якими хтось може керувати віддалено, щоб запускати так звані атаки DDoS (розподілені атаки на обладнання з метою перевантажити обладнання та спричинити його відмову працювати). Метою таких атак є зірвати роботу обраного сайту, переповнюючи його трафіком. Широко відомий приклад такої атаки на Естонію під час її дипломатичного протистояння з Росією у квітні 2007 року, коли низка урядових веб-сайтів були недоступними протягом 3 тижнів. Проблема бот-нету, ймовірно, посилиться, оскільки мережі ботів дедалі більше націлюються на «завжди увімкнені» широкосмугові пристрої, кількість яких зростає.

Напади з фізичними наслідками трапляються порівняно зрідка з огляду на необхідну досвідченість. Втім, такі напади викликають зростаюче занепокоєння та, ймовірно, поширюватимуться, оскільки дедалі більше речей стають підключеними до Інтернету. Наприклад, у 2010 році комп'ютерний хробак Stuxnet став першим шкідливим програмним забезпеченням. Він був спеціально розроблений для нападу на критичну інфраструктуру – ядерні енергетичні реактори Ірану, того разу атаку вдалося зірвати. Критична інфраструктура, як от електростанції, часто є важливою для діяльності урядів, але в багатьох випадках належить приватному сектору або керується ним. Отже, з урахуванням необхідності захисту таких систем, лунають та частішають заклики до державно-приватного партнерства (ДПП).

Політично мотивовані напади також можуть прагнути розголосу, маючі на меті підірвати сприйняття, довіру громадськості. У 2010 році група під назвою «Анонімус» змогла зламати веб-сайти різних організацій, в тому числі прокуратури Швеції, та сайти приватного сектору MasterCard та Visa на підтримку Вікілікс (WikiLeaks), одного з так званих сайтів – «Інформаторів», «Тих, хто дує у свисток» (whistle-blowing website). Коли напади на веб-сайти публічного сектору вдаються, досягають своєї мети, вони можуть вплинути на довіру до електронного уряду настільки, що сприйняття громадськості

стає все більш негативним. У таких випадках люди можуть бути проти виконання певних транзакцій в Інтернеті, можуть не бажати ділитися даними, або не вірити наданій інформації. І це вже проблема. Згідно з даними веб-сайту «Цифрового порядку денного для Європи», лише 12% європейських користувачів відчувають себе цілком безпечно під час здійснення онлайн-транзакцій.

Поширені підроблені банківські електронні листи та веб-сайти, які виглядають схожими на їх справжні аналоги. Мабуть, лише питання часу, коли ми побачимо такі підробки у державному секторі, які будуть запитувати в нас конфіденційні дані або надавати нам оманливу інформацію. Певною мірою це вже відбувається. Інтернет широко використовувався у повстаннях 2010, 2011 років на Середньому Сході, й урядові веб-сайти часто густо повідомляли інформацію, яка відрізнялась від тої, що повідомляли блогери. Траплялося, що деякі уряди, наприклад, у Єгипті, намагалися вимкнути Інтернет, щоб зупинити плин інформації.

Політично мотивовані загрози також зачіпають безпеку контенту та даних, наприклад, у випадках шпигунства чи діяльності «Тих, хто дує у свисток» (whistle-blowing). І те, і інше, щодалі поширюються внаслідок того, що все більше інформації потрапляє в Інтернет.

Мотивація неполітичних атак зазвичай фінансова, і більшість нападів вважатимуться кіберзлочинами. Як такі, вони тяжіють до крадіжки даних, як то інформація про кредитну карту, та їх чисельність зберігається на низькому рівні. Поширений підхід полягає у використанні зловмисного програмного забезпечення, яке або розробляється з нуля, або пере-налаштовується існуюче, чи то купляється на чорному ринку. Зловмисне програмне забезпечення може поширюватися різними шляхами, зокрема електронною поштою або через веб-сайти, і може виконувати різноманітні дії, як то встановлення додатків, які можуть відстежувати ключові характеристики індивідуальних пристроїв. Воно також може зламати комп’ютери та зробити їх частиною бот-нету (мережі ботів), які можна взяти в оренду на чорному

ринку для проведення DDoS-атак, або використовувати як платформу для розповсюдження спам-листів.

Одна з поширених спам-технік – це фішинг, шахрайська спроба вимагати від користувачів конфіденційну інформацію, як то логіни, паролі, за допомогою небажаного електронного листа, який посилається на зловмисний веб-сайт. Й хоча людей постійно попереджують про те, щоб вони не надавали таку інформацію, це залишається проблемою з огляду на витонченість цих електронних листів. За даними Cisco, близько 3% всіх користувачів переходять за посиланнями зловмисного програмного забезпечення. Щоб підвищити рівень обізнаності про фішинг у державному секторі, Тайванська національна команда реагування на надзвичайні ситуації (TWNCERT, https://www.twncert.org.tw) надіслала 186564 імітованих фішингових електронних листів 31094 працівникам державного сектору в 62 державних установах. Загалом 15484 (8,30%) цих електронних листів було відкрито, і були натиснуті 7836 (4,20%) посилань, які в них містилися. Потенційно це піддавало ризику тисячі довірливих працівників державного сектору, так само, як і їхнього роботодавця – уряд.

Ще один спосіб класифікації кібератак – за ознакою загрози – зовнішня, або внутрішня. В більшості наведених вище випадків це загроза зовнішня. Джерелом внутрішніх загроз можуть, наприклад, бути нинішні чи колишні незадоволені працівники. Знову ж таки, WikiLeaks - це приклад, коли, нібито, солдат армії США завантажував конфіденційну інформацію на USB-накопичувач лише для того, щоб потім передати її. Але також зовнішній носій пам’яті може бути використаний для того, щоб встановити на комп’ютер програму чи програмне забезпечення, як от встановлення «таємних дверей» (backdoor), для інших, шкідливих, цілей, таких як моніторинг натискань клавіш або прихований віддалений доступ до нього. Наводять приклад, коли USB-накопичувачі використали для встановлення високо-розвинутого хробака Conficker на комп’ютери Манчестерської міської ради. Цей інцидент спричинив збитки на суму приблизно в 1,5

мільйони фунтів стерлінгів. З того часу Рада заборонила використовувати такі носії пам’яті, а також відключила всі USB-порти. Як врівноважити продуктивність щодо моніторингу користувачів та призначення їм відповідних рівнів доступу – це питання, що хвилює організації державного сектора в усьому світі.

Важливо розуміти, що кожен підключений до Інтернету пристрій є потенційною загрозою, оскільки хтось інший може його пере-підпорядкувати та використовувати в якості агенту, наприклад, як частину мережі ботів. Кажуть, що Conficker перепідпорядкував понад сім мільйонів комп’ютерів в усьому світі, включаючи, серед інших, такі, що належали постійним користувачам вдома, військово-морським силам Франції та військово-повітряним силам США, які й гадки про це не мали.

Оскільки глобалізація, Інтернет та електронний уряд будуть продовжувати зростати, публічний сектор повинен знайти шлях подолання виклику кібербезпеки в усе більш взаємопов’язаному світі. Кожного дня все більше людей долучаються до Інтернету; кожного дня до Інтернету підключаються все більше речей; з кожним днем публічний сектор все більше використовує інформаційно-комунікаційні технології; з кожним днем наслідки кібератак зростають.

Кібербезпека – це організаційна проблема, але водночас є глобальним явищем. Таким чином, це має вирішуватися на всіх рівнях – від міжнародної арени до регіонального, національного та місцевого рівнів.

Діяльність органів влади – це, власне, усе, що пов’язане з даними, інформацією та знаннями про публічний сектор, що створюються, змінюються, переміщуються та розгортаються для задоволення потреб суспільства. Електронний уряд оцифровує деякі або всі ці процеси та отримані результати, потенційно змінюючи їх шляхами, що не завжди прогнозовані або бажані, як для внутрішніх потреб публічного сектора, так і для користувачів публічними послугами та можливостями. Ці ненавмисні наслідки можуть бути проблематичними. Наприклад, вони можуть

спричинити серйозні проблеми для кібербезпеки в частині несанкціонованого доступу або використання даних та інформації державного сектору. Керівники публічного сектору мають настільки ж усвідомлювати ці ненавмисні наслідки, як й ті, яких вони очікують від запровадження електронного уряду.

Звісно, у цілому електронний уряд – це дуже гарна річ, й вона має багато зрозумілих та задокументованих переваг. Для прикладу, існує багато доказів того, що наслідком оцифрування внутрішніх робочих процесів може стати суттєва економія витрат уряду завдяки більш ефективним та раціональним процесам, об'єднанню адміністрацій задля обміну та економії ресурсів, кращому дизайну та персоналізації сервісів, а також більш інтелектуальній розробці більш впливової політики на основі доказів. Зовнішній, що працює з користувачами, офіс електронного урядування, безперечно, надає їм кращі, зручніші послуги, що заощаджують час та доступні 24/7. Оцифровування сприяє прозорості, відкритості та залученості, надає користувачам інструменти для споживання та залучення до розробки послуг, що більше відповідають їхнім індивідуальним потребам.

Для прикладу, опитування, що було проведено в 2017 році Торговою асоціацією інформаційних технологій [477], показує, як федеральні агенції та відомства в США доклали зусиль для публікації наборів даних та використання інструментів соціальних медіа (що є складовою наполегливого просування прозорості) та продовжують боротися у напрямках кібербезпеки, створення інформаційної інфраструктури, питань людського ресурсу. Перехід до більш відкритого уряду створив не тільки можливості, але й загрози теж. Згідно з опитуванням, деякі керівники інформаційних служб (CIO) щодня бачать «мільйони шкідливих спроб отримати доступ до своїх мереж» – від хакерів-аматорів аж до досвідчених кіберзлочинців.

Ця глава висвітлює деякі питання переходу державного сектору до онлайн-обробки інформації, показуючи, що це має як прямі, так і опосередковані наслідки у великому діапазоні областей діяльності

електронного уряду. Часто густо ці наслідки не беруться до уваги. Наприклад, багато урядів помиляються, намагаючись встановити системи безпеки на занадто високому рівні для надаваних функціональних можливостей, що призводять до втрати ресурсів, які могли б бути використані під час роботи більш вразливих систем. Було багато невдалих спроб впровадити складну інфраструктуру відкритих ключів (Public Key Infrastructure, PKI) та системи цифрового підпису, в той час, коли вистачило б простих паролів чи PIN-кодів. Урок полягає в тому, щоб поставитись до безпеки та захисту даних вкрай серйозно і розглядати це як найнагальнішу технічну проблему, але в той же час підходити до цих питань поступово та пропорційно, беручи до уваги, що завжди має бути компроміс між підвищеною безпекою та придатністю до використанням. Підхід, який потрібно застосувати, полягає у побудові безпеки та захисту даних від самого початку будь-якої ініціативи електронного уряду.

Починаючи з 2004 року, під час своєї еволюції всесвітня павутина перейшла від стадії Web 1.0 (що складається з веб-сайтів та веб-сторінок Інтернету, електронної пошти, миттєвих повідомлень, служби коротких повідомлень (SMS), простого онлайн-обговорення тощо) до Web 2.0, що також дозволяє користувачам надавати контент, впливати на нього, та бути безпосередньо залученими. На веб-сайтах Web 2.0 зазвичай є «архітектура участі», яка заохочує користувачів додавати цінність додатку під час його використання, наприклад, через діалог у соціальних мережах навколо створеного користувачем у віртуальній спільноті контенту. Також точиться багато дискусій про розвиток Web 3.0 до широкомасштабних повсюдних суцільних мереж (подекуди їх називають мережевими обчисленнями), мережевих та розподілених обчислень, відкритих ідентифікаторів, відкритої семантичної мережі, великомасштабних розподілених баз даних та штучного інтелекту.

Дехто також нетерпляче чекає на Web 4.0, як глобальну семантичну павутину (тобто методи та технології, що дозволяють машинам зрозуміти

зміст/сенс або «семантику» інформації в Інтернеті), включаючи використання статистичних, побудованих машиною, семантичних тегів та алгоритмів. На думку Тіма Бернерса Лі, «батька» Інтернету, ми напевне вже на порозі віку семантичної павутини, яка певною мірою вже використовує Інтернет даних, а не Інтернет документів, як наразі відбувається. Це дозволить використовувати Інтернет більш інтелектуально, тобто скоріше ставити питання, а не просто шукати ключові слова, а також більш автоматичний обмін даними між базами даних, пошук даних та подібні види використання.

Напрямок розвитку Інтернету впливає й на електронний уряд з посиленням уваги до парадигми уряду 2.0 (Government 2.0). Ця парадигма значно більше концентрується на боці попиту, на розширенні прав та можливостей користувачів, на їх залученні, а також на вигодах та впливах на вирішення конкретних суспільних проблем, а не просто на наданні онлайн адміністративних послуг.

Цього слід досягати, підтримуючи реальну трансформацію механізмів управління в напрямку від ізольованості та урядо-центричності до більшої орієнтованості на користувачів та їхні потреби. Як зазначав Вест, користувачів та інших законних зацікавлених сторін більш відкрито запрошують до взаємовідносин з урядом у сенсі більшої участі і розширення прав та можливостей щодо розробки та надання послуг; розширення роботи державного сектора та державного управління; щодо державної політики та прийняття рішень [520].

З цією метою протягом останніх 10 – 15 років було досягнуто величезного прогресу електронного уряду. Протягом цього часу використання інформаційно-комунікаційних технологій у публічному секторі перейшло від переважно зацікавленості окремих міністерств в оцифровуванні своїх документації та процесів, до стану, коли ІКТ використовуються для об’єднання міністерств, реінжинірингу процесів, для пропонування багатьох нових послуг громадянам та бізнесу. Електронний

уряд став головним пріоритетом для урядів у всьому світі та основним напрямком інвестицій. Це можна виміряти постійним з 2000 року зростанням доступності послуг електронного урядування в усіх країнах. Наприклад, згідно з поточними звітами про дослідження, що виконані консалтинговою компанією Capgemini (https://www.capgemini.com), повна онлайн-доступність в Інтернеті кошика 20 найпоширеніших послуг електронного урядування в Європі збільшилися з 20% у 2001 р. до 86% у 2018 р., за той таки час онлайн-досвідченість зросла з 45% у 2001 р. до 90% у 2018 р. Опитування Інституту Понемон 2016 року показує, що на глобальному рівні громадяни мають користь від більш високого рівня надання електронних послуг, кращого доступу до інформації, більш ефективного урядового управління та покращення взаємодії з урядами, насамперед внаслідок збільшення використання у державному секторі інформаційно-комунікаційних технологій [450].

Цей розвиток невблаганно вказує у тому самому напрямку. Оскільки павутиння розвивається, а дані всіх типів та якостей стають все більш повсюдними, питання не лише в тому, чи можемо ми їх захистити, але й у вирішенні глибоких питань щодо того, хто володіє даними, де вони знаходяться, наскільки вони точні, та хто відповідальний за них.

Поза сумнівом, найбільшим операційним викликом електронному уряду є кібербезпека, включаючи загрози ідентифікації, конфіденційності та системам даних.

Адекватна конфіденційність та захист даних та довіра до цієї підтримки мають вирішальне значення для отримання переваг від електронного уряду. Якщо вони там, де і мають бути, та добре працюють, вони можуть забезпечити стабільну, передбачувану та таку, що будує довіру, структуру. Насправді вони є ключовими для будь-якої діяльності, що використовує інформаційно-комунікаційні технології (ІКТ) у суспільстві – в державному, приватному чи цивільному секторах, тому їх не слід розглядати ізольовано. Але якщо їх немає, це може мати негативний вплив на

використання. За даними ОЕСР, «лише 12% користувачів Інтернету в ЄС відчувають себе безпечно під час виконання транзакцій в Інтернеті, тоді як 39% користувачів Інтернету в ЄС мають великі сумніви в безпеці, а 42% - не наважуються виконувати фінансові онлайн-операції [438]. Постійні повідомлення про втрачені дані кредитних карток та приватну інформацію як в приватному, так і в публічному секторах, мабуть, не покращують цей імідж.

Наприклад, згідно з повідомленням агентства новин БіБіСі (BBC News) у листопаді 2007 року, зникли два захищені паролем комп'ютерні диски, що містили особисті дані всіх сімей у Великобританії з дитиною до 16 років, загалом 25 мільйонів людей. Про пакунок з дисками більше ніхто не чув, й він не був знайдений після фізичного перевезення між двома відділеннями. Це був один випадок серед багатьох, які викликали суттєвий сумнів у належному поводженні уряду з конфіденційними даними.

Також зростає кількість зловмисних хакерських атак, фінансово мотивованих порушень і навіть політично мотивованих зусиль на відключення інформації, наприклад, під час нападів на Естонію, іранських демонстрацій у 2010 році та повстань 2011 року на Середньому Сході. Відомо багато про основні загрози кібербезпеці, але набагато менше про те, як їх подолати. Оскільки головним обов'язком органів влади є захист своїх громадян, публічний сектор має будувати високоефективні та інтегровані системи захисту від злочинності, шпигунства, тероризму та війни в кіберпросторі.

Але реакція публічного сектору на проблеми кібербезпеки здебільшого відстає від приватного сектору, незважаючи на те, що він, напевне, є більш важливим, а згідно з доповіддю Організації економічного співробітництва та розвитку (ОЕСР) за 2016 рік, доступність даних про зусилля публічного сектору обмежена. Навіть у країнах, що вже далеко просунулись у напрямку електронного урядування, таких як Норвегія, лише меншість публічних адміністрацій пропонували безпечні способи комунікації зі своїми веб-

сайтами, незважаючи на багато опитувань, які показують, що побоювання щодо незахищеності даних користувачі сприймають як найбільший стримуючий для них чинник у використанні е-уряду.

Однак, також варто відзначити, що реакція на загрози кібербезпеці дуже мінлива, наприклад, центральні органи влади набагато частіше вживають адекватних заходів, ніж місцеві, що вочевидь відображає відповідну чисельність населення та наявні ресурси. Але багато послуг електронного уряду надаються на місцевому чи регіональному рівнях, й кількість інформації, яку надають ці суб'єкти, швидко збільшується. Одним із викликів кібербезпеки в публічному секторі є те, що він характеризується великою операційною незалежністю та «ізоляцією» серед різних його частин, що в приватному секторі такою мірою не спостерігається.

Таким чином, кібербезпека в публічному секторі є першочерговою турботою, і зрозуміло, що нинішні системи, як організаційні, так і технічні, не завжди відповідають цьому виклику. Майбутнє, ймовірно, потребуватиме рішень, дуже відмінних від сучасних систем, що орієнтовані на порівняно стабільні, чітко визначені, послідовні конфігурації, контексти та учасників щодо безпеки. На наш погляд, потрібна нова парадигма, що відрізнятиметься «відповідною» безпекою, за якої ступінь і характер безпеки, пов'язані з будь-яким конкретним типом дії, змінюватимуться з часом, при зміні обставин та при зміні наявної інформації. І у цьому напрямку публічному сектору доведеться стикатися з викликами у п'яти сферах: конфіденційність, довіра, безпека даних, втрата контролю даних та поведінка людини.

Насамперед, ініціативи з питань кібербезпеки у публічному секторі мають брати до уваги наслідки для конфіденційності, які у багатьох випадках можуть значною мірою загрожувати їхній ймовірній дієвості. Наприклад, конфіденційність та захист даних потребуватимуть відповідних систем безпеки, адаптованих до мінливих потреб доступу та ідентифікації людей та організацій. Ці системи також мають діяти через національні кордони, що вимагатиме не лише політичних угод, але й сумісних структур та стандартів

даних. Безпека даних також буде покращена шляхом надання користувачам набагато більшого контролю над їхніми власними даними та над їхньою власною (почасту) множинною ідентифікацією, наприклад, через довірених третіх сторін. Для сервісів, які можуть працювати через кордон, життєво важливими будуть добре функціонуючі системи ідентифікації та аутентифікації. Гарантія інформації також необхідна за цілісного підходу, що включає управління ризиками, з урахуванням того, що жодна система не може забезпечити цілковиту безпеку. Довгострокове зберігання даних та доступ до них також важливі, враховуючи швидко мінливі технічні формати та очікуване величезне збільшення генерації даних.

Конфіденційність має захищатися, наприклад, шляхом регламентації та міжнародних угод, таких як Європейський закон про захист даних (що може бути адаптованим та ратифікованим і в Україні), включаючи відповідних омбудсменів, хранителів даних або довірених третіх осіб. Слід обережно уникати «сповзання місії», коли дані використовуються для цілей, на які не були призначені спочатку, або «гонки до низу» в міжвідомчому чи транскордонному обміні даними шляхом повернення до стандартів самого слабкого члена. Потреби та довіра користувачів повинні будуватися на розумінні реальної поведінки людини під час використання даних, а також на технічних вимогах. Технічний аспект кібербезпеки може виявитися легкою частиною. Певно, що розуміння та обслуговування того, що деякі називають ірраціональним, а саме, поведінки людини, може бути справжнім викликом для кібербезпеки.

Довіра є критичною проблемою, і вона будується за допомогою мінімізації інформації (тобто з використанням якомога меншої кількості даних, тільки тих, що необхідні для виконання завдання) та інформування користувачів або отримання згоди користувачів під час доступу та обробки їхніх даних, сприяючи користувачам відстежувати, володіти, або контролювати їхні власні дані. Довіра також будується шляхом належного врядування, роз’яснення та мінімізації ризиків втрати або витоку даних.

Загальновідомо, що довіру важко побудувати, але її можна дуже швидко та руйнівно знищити одним єдиним порушенням. Це підкреслює необхідність вважати довіру багатовимірною. Очевидно, що для максимальної вигоди користувачі мають довіряти своєму уряду чи постачальнику послуг, але для органів влади стає все більш важливим довіряти користувачам, наприклад, дозволяючи їм розгортати дані публічного сектору та залучаючи їх до розробки політики та прийняття рішень. Електронний уряд потребуватиме також персоналізованих та контекстно-релевантних інформаційно-комунікаційних технологій, систем управління відносинами з клієнтами (або громадянами), та систем підтримки прийняття рішень та прогнозування на основі інтелектуального управління знаннями та архівування. В електронному врядуванні, мабуть, стануть важливими особисті модулі/простори, що чутливі до контексту, розвинені та персоналізовані. Також вони важливі для супроводу, та розвитку обслуговування супроводу.

Хоча багато дискусій щодо кібербезпеки (що, безумовно, є мейнстрімом у медіа та повсякденним дискурсом), далекі від раціональності, поінформованості чи точності, але також дуже важко бути безпристрасним. Як і у фізичному світі, так й у кіберпросторі, терорист однієї людини – це водночас борець за свободу іншої людини – буквально, як у випадку з WikiLeaks та Джуліаном Асанжем. З одного боку, існує думка, яку підтримують багато урядів, що, чим більше доступно даних про громадян, тим краще громадянам можна допомогти та захистити їх. Порівняйте це з протилежним поглядом, якого дотримуються багато громадян, страхаючись стану спостереження/нагляду, від якого нема де сховатися. Якщо органи влади володіють занадто багатьма даними, це втручається у приватне життя громадян. Більше того, органи влади мають поганий послужний список щодо збереження даних, є чимало прикладів, коли органи влади зловживали даними, свідомо чи несвідомо.

Проте, у той самий час, ті самі громадяни, які занепокоєні поведінкою органів влади, що зазвичай називають «великий брат», охоче надають

приватним компаніям (які, як їм добре відомо, займаються лише зароблянням на них грошей), набагато більше особистих даних, ніж вони будь-коли надають органам влади. Багато людей також розкидають ще більше своїх особистих та подекуди інтимних подробиць про себе на сайтах соціальних мереж. Можливо, громадяни сприймають органи влади настільки великими, монолітними та всепроникними, що будь-яке неналежне використання даних матиме дуже великі наслідки, тоді як приватний сектор чи сайти соціальних мереж настільки, порівняно, розрізнені та строкаті, що неналежне використання даних не може бути надто важливим. Професіонали знають, що це дуже далеко від того, що насправді відбувається.

Хто є володарем даних, це може бути глибоко філософським питанням, але це є реальне важливим на практиці, коли йдеться про кібербезпеку, оскільки це визначає, хто може (або має) їх захистити. Наприклад, хто є володарем тих даних, що приватні особи чи організації надають органам влади, або органи влади – вони самі, чи органи влади, з моменту, коли вони їх отримали?

Можливо, важливіше значення має право на використання даних незалежно від володіння, особливо якщо вони мають економічну або іншу цінність. Нещодавні дослідження у Великобританії, такі як, наприклад, проведені Newbery, Bentley, Pollock та Європейською Комісією, показали, що «інформація публічного сектору» (public sector information, PSI) має чітку та значну економічну цінність, яку можна продати комерційним чи іншим організаціям, щоб забезпечити надходження доходів до бюджету. Це було нормою в більшості розвинених країн протягом багатьох років, але узгоджена кампанія «звільніть-наші-дані» у Великобританії протягом останнього десятиріччя призвела до того, що більшість державних установ відкривають інформацію PSI у машино-читабельному та легко доступному форматах для безкоштовного користування будь-ким. Основним аргументом є те, що тим самим створюється ще більша економічна цінність для суспільства в цілому, коли підприємці всіх типів можуть розробляти нові оф-

лайн-продукти (наприклад, бізнес-послуги щодо економічних даних), а також нові онлайн-смарт-сервіси (або «додатки»), до яких, на власний розсуд підприємців, може надаватися вільний доступ. Звільнення даних у такий спосіб є частиною зростаючого руху «за відкритий уряд», як от Британська ініціатива прозорості та підзвітності 2010 року, хоча цей рух поки що став вагомим лише у кількох країнах.

Багато хто стверджує, що безпека даних буде покращена шляхом надання користувачам набагато більшого контролю над їхніми власними даними та над їх власною (почасту) множинною ідентифікацією, оскільки так вони будуть безпосередньо зацікавлені у забезпеченні безпеки та точності таких даних. Наприклад, у 2003 році в Естонії було прийнято Закон про захист персональних даних, який охоплює інформацію, щодо визначених фізичних, ментальних, фізіологічних, економічних, культурних та соціальних характеристик фізичної особи, її відносин та зв'язків. На запит фізична особа має законне право на доступ до всіх персональних даних, що стосуються його/її, - цілей, призначення цих даних, їх категорій та джерел, а також третіх осіб чи категорій, яким передача цих даних дозволена. Згідно із Законом про захист персональних даних країни, особа має подальше право вимагати припинення обробки своїх персональних даних, виправлення у випадку помилок, та блокування чи видалення їхніх даних через Інспекцію захисту даних або суди. Питання щодо безпеки домашнього комп'ютера особи під час вивчення її даних на офіційному веб-сайті не розглядаються в цьому законодавстві, оскільки це значною мірою поза контролем уряду, але вважається, що це викликає менше занепокоєння, оскільки будь-який витік даних був би порівняно частковим, ніж масовим. Проте дуже мало країн мають настільки ж добре розвинене забезпечення власності та прав на дані, як Естонія, і це, ймовірно, дає уявлення про відхилення підходу урядів до впровадження кібербезпеки від ставлення громадян до цього питання.

Вже з'являються дуже корисні приклади аутсорсингу, коли кібербезпека, як виглядає, не була під загрозою, але сам факт поширення

даних, вже не під прямим контролем органів влади, та їхнього розповсюдження, збільшує ризики. Вони виникають за обставин технічної несумісності та через почасту різні організаційні та робочі культури і наміри залучених учасників, коли стає все складніше забезпечувати загальний контроль та контролювати стандарти.

Впровадження електронного уряду передбачає необхідність повністю переробити як організаційні структури (по суті, зламати ізольованість), так і архітектуру даних, щоб забезпечити обмін послугами та ресурсами всередині державних адміністрацій та між ними. Це все частіше відбувається в центрах спільного обслуговування з охопленням програм ІКТ, структурних частин, інформації та даних електронного уряду, а також загальних бізнес-процесів. Це також може сприяти аутсорсингу до інших суб'єктів, у тому числі поза державним сектором, якщо витрати можуть бути скорочені. Проте основна критика полягає в тому, що у довгостроковій перспективі витрати можуть бути й не зекономлені, якість може зменшитися, і поза сумнівом, це призводить до втрати контролю з боку урядів, які, в решті решт, є демократично відповідальними на відміну від приватних підрядників.

Зрозуміло, проте, що відбуваються значні збої. Можна стверджувати, що ми перебуваємо на порозі серйозного просування до «товаризації» (commoditization) великої кількості бізнес-процесів на основі ІКТ, і це також глибоко позначиться на публічному секторі, зробивши аутсорсинг, а також більшу залученість користувачів набагато більш ймовірними. Аналізуються, стандартизуються та шаблонізуються всі типи бізнес-процесів. Це відбувається не лише щодо розробки та надання послуг, але також від розробки програмного забезпечення та найму персоналу до принаймні деяких аспектів моделювання та розробки політики за допомогою автоматичних моделювання, сценарію та відпрацювання. Ці знання кодифікуються та забезпечуються за допомогою ІКТ. Це може призвести до масової «товаризації» процесів та їх аутсорсингу.

Поширення використання ІКТ, поза сумнівом, означає, що публічний

сектор має усвідомити та докласти зусиль, щоб уникнути одночасної втрати знань та контролю над основними процесами (та компетенціями, рішеннями та політикою, необхідними для їх підтримки), які є основою надання всіх державних послуг. Необхідно краще зрозуміти, які аспекти діяльності публічного сектора можуть і повинні бути кодифіковані, «товаризовані» (наприклад, за допомогою ІКТ) та передані в аутсорсинг або «підключені до мережі» з іншими суб'єктами, включаючи приватний та громадський сектори, і, як все більше здається, включаючи користувачів. Ті, що мають приймати рішення, поки що не долучаються до всіх цих питань, але в умовах, коли уряди намагаються скоротити витрати, значення цих питань знову різко зростає.

Створення технічної стійкості з «витонченими розподіленими ідентифікацією, обробкою та реагуванням» під час кібератаки та забезпечення швидкого відновлення життєво важливих функцій є ключовими з технічної сторони. Проте головне відоме-невідоме кібербезпеки (оскільки ми рідко перестаємо думати про це, і це так непередбачувано) виявляється важливішим, ніж суто технічне питання (як зробити, щоб усе працювало), це – поведінка людини. Більшість приймає, що безпека ніколи не може бути ідеальною, але причини цього мають бути вивчені більш уважно, а надто, коли також стає зрозумілим, що між використанням систем (що ми, очевидно, хочемо заохотити) та безпекою цих систем існує зворотна залежність. Це нагадує давню приказку, що, якщо ви хочете бути у повній безпеці і не піддаватися жодним ризикам, залишайтеся в ліжку цілий день - хоча тут не йдеться про землетруси, тому навіть цей варіант не є абсолютно поза ризиком. Й це не є прийнятним шляхом керувати суспільством, розвивати економіку, не кажучи вже про життя.

Поведінка людини, раціональна чи ні, є стрижнем кібербезпеки – що люди думають про свою ідентифікацію, про дані своєї ідентифікації, хто володіє ними, має до них доступ, та як їх використовує. Відомо, що головним викликом є краще розуміння співвідношення ризиків, що пов'язані з

кібербезпекою, та переваг використання системи, але все ще не достатньо відомо про те, як досягти певної рівноваги. Зокрема це стосується публічного сектора (порівняно з приватним), де неможливо або небажано застосовувати ринкові рішення, щоб знайти баланс. Натомість її потрібно досліджувати шляхом спроб та помилок, збору доказів, а також свідомим застосуванням етичних та демократичних принципів.

1.3. Виклики для електронного врядування у контексті забезпечення кібербезпеки

З прийняттям інструментів та підходів Web 2.0 багато урядів переходять до парадигми Gov 2.0 («Врядування 2.0»), яка дозволяє «спільно вироблені» сервіси, в яких користувачі активно співпрацюють з постачальниками послуг, та «само-створені» сервіси, в яких послугу визначають переважно користувачі. Це також може призвести до «краудсорсингового уряду», коли контент та вклади отримуються від широкого кола користувачів та інших суб'єктів, які мають певні знання та інтереси, яких не має уряд. Важливість кібербезпеки для публічного сектору, а також для громадян та підприємств полягає в тому, як, та ким, ці дані розповсюджуються, передаються та використовуються. Певно, ще важливіше – чи можливо з'ясувати, хто саме використовує дані? Одна річ – втрата контролю, але справжньою проблемою є – не знати, хто наразі має цей контроль. Наприклад, окремі частини Австралії в програмі Google Earth досі залишаються розмитими. Google повідомляє, що видалив фотографії з високою роздільною здатністю через проблему з одним із постачальників зображень, проте інтернет-видання «IT Security», вказує на побоювання, що карти можуть бути використані як терористичний інструмент. Деякі із заблокованих районів включають (або включали в якийсь момент) військово-морську базу Garden Island, реактор на висотах Lucas, будинок парламенту та

штаб сил оборони Австралії в Канберрі.

Менше щодо безпеки, але все ще турбує публічний сектор питання не тільки про те, чи знаходяться дані у безпеці, але також чи можуть вони бути збережені та надані для дозволеного використання в довгостроковій перспективі, зважаючи на постійні зміни форматів та стандартів даних. Тут знову очевидна необхідність компромісу між безпекою та використанням. Наприклад, для доступу до даних, що збережені на дискетах 15 років тому, сьогодні потрібне втручання фахівців при використанні музейних артефактів. Можуть допомогти хмарні обчислення, оскільки вони потенційно дозволяють розподіляти дані та інші ресурси на декількох серверах десь в Інтернеті. Але навіть якщо це вирішує проблему «куди», довгострокове збереження все ще вимагає, щоб стандарти та формати були доступними в довгостроковій перспективі.

Коли збереження даних передається на аутсорсинг до спеціалізованої приватної компанії, або коли послуги електронного уряду, наприклад, можуть бути автоматично надані з «публічної хмари», виникають складні питання контролю та власності, зокрема можливу втрату підзвітності та демократичного нагляду.

Так, приклад у Нідерландах демонструє не лише втрату державного контролю, а й узурпацію всього, що робить уряд, оскільки інші можуть отримати доступ або навіть створити власні дані, релевантні до того, що раніше було публічною функцією. Мається на увазі поєднання інструментів Web 2.0 та побутової електроніки, як-от записувальне обладнання високої роздільної здатності, датчики та камери, які стають все більше вільно доступними для всіх, а не лише для професіоналів. Скарги людей, які живуть поблизу аеропорту Schiphol в Амстердамі, щодо рівня шуму літаків були ігноровані або відхилені державними органами, внаслідок чого мешканці розробляли власну систему вимірювань на основі сенсорної технології з під’єднанням до комп’ютера та Інтернету. Система встановлена в садках протестуючих і реєструє рівень шуму літаків. Це записується в електронному

вигляді, збирається, поєднується з іншими даними та додатками та публікується на їхньому власному веб-сайті http://www.geluidsnet.nl/en/geluidsnet. Це ілюструє зростаючу тенденцію, коли професійне обладнання та програмне забезпечення стають товарами, доступними для кожного, щоб розробити та впровадити власні послуги, орієнтовані на інтереси користувачів. Цей випадок показує, як компетенції публічних установ та довіра до них можуть бути підірвані та узурповані. Після деякої боротьби органи влади визнали, що система мешканців була більш точною та надійною, і тепер це стало сервісом де-факто. Можливо, з іншого боку, деяким зиском для органів влади тут можна вважати нагоду усвідомити, що це залишається проблемою, яку необхідно обговорити, а саме те, що, втрачаючи контроль, вони також можуть втратити свою спроможність, як політичну, так і фінансову.

Іншим аспектом втрати контролю з боку уряду є вельми невтішне використання порталів електронного уряду та зростання альтернативних інструментів, керованих користувачами. Наприклад, портал https://www.gov.uk у Великій Британії є шлюзом для всіх державних служб і його часто оцінюють як сервіс світового класу. Проте, за словами одного з фахівців з підрозділу з питань трансформації в кабінеті Великої Британії, використання порталу було насправді невисоким [274].

Як свідчать декілька джерел, включаючи Європейську комісію, OECP та консалтингову групу McKinsey [410], це поширена проблема для порталів електронного уряду в усьому світі. Натомість, подобається це органам влади чи ні, доступ до даних у публічному секторі стає розповсюдженим як через зростання кількості сторонніх провайдерів, так і завдяки урядам. Насправді деякі країни зараз переходять від концепції порталу до багатоканальних методів надання послуг, які пропонують громадянам прямий доступ до місцевих послуг, спрощуючи послуги та скорочуючи час, необхідний для здійснення запиту на послуги, та зменшуючи кількість кроків, необхідних для здійснення транзакції. Такий перехід ілюструє підхід «без помилок», що

забезпечує прямий доступ до послуг, де б громадянин не знаходився в Інтернеті.

Втрата державного контролю над даними також, ймовірно, призводить у контексті послуг електронного уряду для інших комерційних та особистих потреб, до того, що організації, підприємства та особи все частіше роблять свої дані (контент та функціональні можливості) доступними у хмарі, а не через портал або навіть веб-сайт. Це означає, що користувачі послуг зможуть створювати свій власний контент та послуги на власних платформах, як правило, через аватари або через автоматичних електронних посередників. Вхід через «вхідні двері» веб-сайту, можливо, все більше користувачів сприйматиме як зайвий непотрібний крок. Також спостерігається швидке зростання нових каналів ІКТ, таких як мобільне та цифрове телебачення, що призводить до розповсюдження безлічі каналів і платформ, де портали та веб-сайти складають одну, мабуть, невелику частину пропозиції.

Такий розвиток подій, ймовірно, означає, що кібербезпека може стати ще більш актуальною, оскільки навіть, якщо значення мережі знижується, збільшення використання ІКТ на різних каналах робить безпеку як більш важливою загально, так і більш складною для електронного уряду. Гучні атаки на урядові веб-сайти (Білий дім, Пентагон, кібератака на Естонію – усе це є відомими прикладами), своєю чергою, можуть відполохати багатьох користувачів. Це ще більше зменшить довіру до використання електронного уряду та може спонукати користувачів до попиту на повернення до більш традиційних послуг віч-на-віч, які, на їхню думку, є більш безпечними. Може бути досить важко переконати у тому, що ця думка є часто цілком помилковою, не зважаючи на те, що паперові записи набагато легше псуються, губляться або знищуються, а інформація у цьому випадку набагато менш доступна при необхідності.

Те, що електронному уряду вдається добре робити, це надання користувачам даних в якості послуг способами, які ніколи не можна було навіть уявити, і є багато хороших прикладів цього, таких як веб-сайт

https://www.fixmystreet.com (відремонтуйте мою вулицю) у Великій Британії. Однак це робиться не завжди органами влади, як і у цьому прикладі, коли «третя» організація збирала дані від усіх органів влади про їх відповідальність за утримання та ремонт вулиць та місцевих мікрорайонів, геть усе – від розбитої бруківки до графіті та сміття. Ці дані потім використовуються для автоматичного генерування та надсилання скарг, просто супроводжуваних поштовим кодом, до відповідального органу, що робить цю службу електронного уряду однією з найбільш використовуваних у Великій Британії.

Ще один приклад 2016 року, також з Великобританії, - це наявність на веб-сайті для обслуговування громадян статистики злочинів на локальних картах. За повідомленням британської газети Guardian, виникали проблеми, яких ніхто не передбачав. По-перше, були побоювання, що ціни на житло в районах з високою злочинністю можуть знизитися, а деякі власники будинків можуть подати позови до відповідного агентства за їх збитки. По-друге, багато даних були помилковими, погано обчисленими, або неправильно розміщеними, почасту даючи абсолютно неправильне уявлення. Масштаб дуже важливий не лише для представлення даних на карті, але навіть для збору даних та визначення місця. Проблеми виникали з приводу того, як збиралися дані, хто робив збір даних, як, та де вони були зареєстровані. Беззаперечна об’єктивність представлених даних знову виявилася підданою махінаціям з боку далекої від досконалості поведінки людини, яка була посилена через ІКТ. Перевага висвітлення цих проблем у публічному секторі, однак, у тому, що це сприяє підвищенню усвідомлення, що подібні проблеми, які майже напевно існують у приватних комерційних службах, приховуються, або їх намагаються приховати. Це також дає нам зрозуміти, що такі проблеми існували завжди, і однією з переваг оцифрування є те, що це робить їх прозорими, навіть якщо це може їх перебільшувати.

Так само, як і координація та інтеграція в публічному секторі, зростає тенденція до співпраці з іншими суб’єктами, як приватного, так і

громадського секторів, а також з користувачами. Все це взагалі дуже корисно для всіх причетних. Хоча приватний сектор вже протягом багатьох років виступає важливим партнером органів влади, громадський сектор також зараз починає ставати важливим, та почасту новим, джерелом ресурсів та досвіду для виконання завдань публічного сектору та надання послуг. Отже, крім публічно-приватних партнерств (ППП), тенденція також стосується публічно-громадських партнерств. Наприклад, волонтерський сектор та соціальні підприємці, особливо коли вони виступають посередниками між державним постачальником та відповідним користувачем, можуть додавати низові ресурси, знання, інновації та навіть корисну конкуренцію.

Таким чином, уряд стає відкритим та доступним для співпраці шляхом, якого немає в інших секторах, і це може призвести до корисних змін поточного способу функціонування публічного сектору та його обов'язків. По-перше, задля надання кращих послуг та кращого управління технологія допомагає «вивернути» публічний сектор зсередини назовні, відкриваючи спосіб його роботи та «виштовхуючи» його діяльність у суспільство. Наприклад, електронний уряд дозволяє виборним посадовцям та політикам звільнитися від обмежень мерії та безпосередньо спілкуватися з громадянами на вулицях чи в їхніх домівках та з підприємствами у їхніх власних приміщеннях, постійно підтримуючи зв'язок з інформацією та знаннями, які їм потрібні у внутрішньому офісі. По-друге, технологія допомагає «вивернути» публічний сектор ззовні всередину, запрошуючи комерційних і громадських акторів «всередину», щоб взяти участь у розробці та наданні послуг, а також надаючи їм інструменти долучення до розробки публічної політики та прийняття рішень.

Все це загалом приносить багато користі, але є також небезпеки або, принаймні, виклики, які повинні братися до уваги. Коли влада є лише одним із численних акторів у публічній сфері, яка тепер також легітимно складається з суб'єктів приватного та громадського секторів, потрібно знайти нові форми підзвітності. Двоє дослідників, Бовенс та Лоос [253] вирішили це

питання, коли описали перехід від законності до прозорості. Нова форма підзвітності необхідна, коли органам влади доводиться обмінюватися даними, владою та відповідальністю, наприклад, через процеси горизонталізації, де-територіалізації та масштабованості. Горизонталізація дозволяє частково перенести розробку загальнообов'язкових правил від традиційної законодавчої влади до інших регуляторних органів, які можуть не мати демократичної легітимності, таких як незалежні адміністративні органи (наприклад, кванго – Quangos), «парасолькові» організації та «інтерактивні партнери з політики». Процес оцифрування може дати можливість всім акторам, в тому числі в приватному та громадському секторах, рухатися швидше, ніж законодавці в публічному секторі та парламенті.

Де-територіалізація означає те, що численні виклики та проблеми, з якими стикаються органи влади через кордони (наприклад, торгівля, забруднення, міграція, злочинність тощо), можуть представити національному законодавчому органу факти про події, що вже здійснилися, але над якими він не має безпосереднього контролю.

Глобалізація, швидкі зміни та турбулентність призводять до відставання формального законодавства та вимагають нових гнучких форм регулювання. Фінансова криза і крах 2008 року стали можливими, якщо не були спричинені «великим ударом» в середині 1980-х, коли сектор фінансових послуг перейшов у цифровий режим, що дозволило мільярдам доларів переміщуватися по всьому світу за мілісекунду. Як для горизонталізації, так і для де-територіалізації, кібербезпека має не тільки впоратись з системами даних (державного сектору або національними) та їх розповсюдженням, але й з глобальними загрозами, що все більшають в реальному часі. Мається на увазі не лише технологічна складність, але й політична, організаційна, культурна та поведінкова складність у масових масштабах.

Обмеженість можливостей органів влади щодалі помітніше. Складні

політичні виклики починаючи від міжнародного рівня до рівнів осіб – у таких різноманітних сферах, як зміна клімату, старіння населення та ожиріння – не можуть бути вирішені лише діями органів влади. Їх ефективне вирішення вимагатиме узгоджених зусиль усіх суб'єктів суспільства, включаючи окремих громадян. Органи влади скрізь знаходяться під тиском, щоб зробити більше з набагато меншими витратами. Більшість наполегливо працюють над тим, щоб забезпечити ефективну політику та послуги принаймні компенсуючи собівартість у державний гаманець; багато хто намагається використовувати ресурси поза публічним сектором. І останнє, але не найменш важливе, органи влади прагнуть забезпечити та підтримувати високий рівень довіри населення, без якого їхні дії, в кращому випадку, будуть неефективними, або в гіршому випадку – контр-продуктивними. У той же час, більш освічені, добре інформовані та менш покірні громадяни судять свої уряди з точки зору їх демократичності, політики та ефективності надання послуг.

Роль публічного сектора може полягати у збереженні компетенції та контролю над цими питаннями високого рівня в інтересах суспільства маючи на тямі суспільне благо та суспільну цінність. Якщо публічний сектор не буде цього робити, небезпека може полягати в тому, що публічний сектор, як ми його розуміємо сьогодні, роблячи лише те, що ринок не цікавить, в той час, коли все «товаризоване», на аутсорсі, приватизоване, або віддане на примхи та упередженість благодійних організацій, може зникнути або скоротитися до розмірів «огузка». Це може бути одним з найбільших викликів державній службі та етиці державних служб. За такого сценарію захистити публічний сектор від кіберзагроз буде ще важче, оскільки дані будуть розповсюджені.

Це також може означати, що насправді захищати дані публічного сектору доведеться суб'єктам приватного сектору. Чи будуть вони вважати це, та суспільне благо, своїм головним пріоритетом? Проте, незважаючи на проблеми, що пов'язані з втратою органами влади контролю над даними,

дехто вважає, що розподілення прав власності, контролю та використання даних публічного сектору може бути корисним, оскільки це зменшує концентрацію влади та збільшує відповідальність, креативність та інновації.

Те саме розподілення може також покращити кібербезпеку, оскільки, хоча ризик порушення безпеки явно збільшується, будь-який збиток, ймовірно, буде набагато меншим та більш керованим, ніж за низького ризику, але з катастрофічністю зриву безпеки високо-централізованої системи, яка контролює більшість якщо не всі дані. І ще раз: зрозуміло, що основна проблема кібербезпеки не є технічною (яка, проте, важлива та пов'язана з цим), а полягає в необхідності збалансувати кібербезпеку та використання системи в контексті почасту непередбачуваних поведінок і потреб організацій та індивідуумів.

Отже, довіра, прозорість та підзвітність – це, мабуть, три найбільші виклики, що стоять перед успішним електронним урядом, і всі вони нерозривно взаємопов'язані. Без довіри до публічного сектору електронний уряд зазнає невдачі. Ще раз згадаємо загальновизнану істину, що довіру важко отримати і легко зіпсувати, тому вкрай важливо знайти способи повернути цю тенденцію. Довіра і недовіра йдуть пліч-о-пліч і потребують збалансованості. Довіра зменшує трансакційні витрати, але здорова недовіра заохочує конструктивну критику та обговорення. Справа в тому, щоб знати різницю. Органи влади можуть сприяти у цьому, досягнувши максимальної прозорості та відкритості, щоб громадяни могли бачити, як приймаються рішення, хто їх приймає та чому. Відповідні можливості для оскарження процесу прийняття рішень також необхідні в рамках чітких правил.

Як зазначає Hansard Society [343], некомерційна організація у Великобританії, хоча ІКТ може бути дуже важливими для збільшення участі, важливо також мати чітку, прозору та засновану на певних правилах відповідальність за всі форми участі, щоб відновити зв'язок між незадоволеними виборцями та політиками. Окрім того, що ІКТ використовуються для надання доступу до публічної інформації (що є дуже

важливим аспектом електронної участі), ІКТ можуть підтримувати просування до набагато ширшої прозорості як частини концепції відкритого уряду. Наприклад, дозволяючи користувачам простежувати кожну взаємодію в рамках публічної адміністрації аж до імені державного службовця, який займається їх запитом чи справою в режимі реального часу.

В іншому прикладі, як частина переходу від електронних закупівель, уряд Великобританії створив веб-сайт, на якому відображаються бюджети та видатки всіх державних установ, і це розповсюджується серед місцевих органів влади, наслідуючи зразок Recovery.gov 2009 року – офіційного веб-сайту уряду США, який забезпечує простий доступ до даних, пов'язаних із «Recovery act» витратами (Recovery act – закон США 2009 року про відновлення та реінвестування, який охрестили «Актом про відновлення»), та дозволяє повідомляти про можливі шахрайства, марні витрати та зловживання. Подібні розробки можуть бути частиною руху до прозорості не тільки інформації та послуг, але й прозорості мети, дій, процесів та результатів органів влади. Це означало б, що всі потенційно можуть мати доступ до (майже досконалих) знань про те, що відбувається, та про вплив, який це має чи може ймовірно мати. Як зазначають двоє дослідників, Блейкмор та Ллойд [248], це могло б дозволити дуже точно співвідносити рішення та дії з усім набором різноманітних (іноді суперечливих, іноді взаємодоповнюючих) потреб усіх суб'єктів. Публікація конфіденційної інформації на веб-сайті WikiLeaks є вагомим прикладом того, що така тенденція відбувається, незважаючи на те, чи подобається це урядам, чи ні.

Прозорість системи та даних може дати можливість користувачам та публічним службовцям супроводжувати та відслідковувати запити і справи у публічному секторі, щоб слідкувати за їх просуванням, знати, яка частина системи зараз несе відповідальність, а також краще передбачати та обходити вузькі місця чи корки. Покладання відповідальності (та прав інтелектуальної власності, коли це є відповідним) може бути вирішальним, особливо щодо користувачів, які за своїм статусом чи станом можуть не мати можливості

здійснювати власні права/обов'язки, як от діти, літні люди, інваліди тощо. Це також дозволить користувачам долучитися, бути більш поінформованими та мати більшу можливість контролю задля власної користі.

Як зазначає Європейська ініціатива щодо прозорості [319], прозорість часто є основою довіри. Прозорість у публічному секторі фактично означає можливість справді «бачити і отримувати те, за що ми платимо» та зробити це видимим для всіх. Це також має означати закінчення невидимих, розділених «Kafkaesque» бюрократій (Kafkaesque – характерні для, або ті, що нагадують гнітючі або кошмарні якості вигаданого світу Франца Кафки), які не знають нічого окрім того, що служити своїм цілям. Також прозорість може заощаджувати час та гроші за рахунок зменшення помилок, об'єднання ресурсів та знань, зменшення дублювання та сприяння співпраці. Прозорість також зменшує корупцію.

Важливо підкреслити, що хоча існує постійна потреба у підвищенні довіри користувачів до органів влади щодо всіх завдань публічного сектору, органам влади також необхідно збільшити свою довіру до користувачів, щоб вони, за підтримки та в рамках чітких рекомендацій, могли брати участь відповідально. Така довіра потенційно проявляється багатьма способами. Наприклад, коли органи влади надають доступні дані про місцеві злочини, в тому числі у форматі, придатному для машинного читання та повторної обробки, вони довіряють суспільству, розумно використовуючи їх для інформування, а не для залякування або паніки. Так само, коли органи влади відкривають громадянам процеси прийняття рішень та формування політики, необхідна взаємна довіра. Очевидно, що, як для органів влади, так і для громадян, існує «крива навчання» розумному та відповідальному поводженню із звільненими даними та їх інтерпретацією, та тому, як уникнути небезпеки неправильного використання у багатьох можливих формах.

Хоча очевидно, що широке оприлюднення даних публічного сектору може принести величезні переваги, майже напевно існують законні інтереси,

які слід захистити від повної прозорості та відкритості. Наприклад, існують, безперечно, законні потреби та інтереси приватності громадян та підприємств, коли їхні дані використовуються органами влади. Однак настільки ж важливими є й інтереси публічних службовців та політиків, особливо під час процесу прийняття рішень та політичної діяльності, наприклад, у захисті від настирливого впливу та моніторингу, які можуть стати наслідком того, що всі їх дії та рішення стають абсолютно прозорими. Це може спричинити стрес та надлишкову зосередженість на вимірюванні та виконанні обов'язків на особистому рівні, та призвести до надто бюрократичної позиції, роботи суворо за правилами замість того, щоб бути гнучкими та готовими сприймати вимірний ризик політичних ідей. Це також може спровокувати небажання приймати рішення або брати на себе відповідальність за них. У статті 2007 року газета Guardian цитує одного з високопоставлених державних службовців уряду Великобританії: «Наразі я би волів ніколи не писати поради міністрам» [342]. Він звинувачує Закон про свободу інформації 2007 року в «перешкоджанні ефективній роботі уряду, не в останню чергу тому, що чиновники стикаються з «нісенітними», або такими, що «марнують час» заходами від журналістів, агітаторів та громадян» [там само].

Підзвітність випливає як з відповідальності, так і з відкритості та прозорості. Це також пов'язане з етичними міркуваннями, які, як теоретично, так і на практиці, мають велике значення в суспільній сфері. Існують різні види підзвітності.

По-перше, політичну підзвітність мають виконувати політики та демократично обрані представники.

По-друге, адміністративна підзвітність покладається на публічних службовців, а також на публічний сектор як інститут. Це також включає ймовірність зміни системи підзвітності, коли залучені партнери з приватного сектору та громадських організацій, що беруть на себе виконання завдань публічного сектору, таких як вироблення політики або надання послуг.

По-третє, існує підзвітність користувача щодо неправильного користування та зловживання послугами чи можливостями публічного сектору, а також щодо участі законними та відповідальними способами. Все це стосується обов'язків.

По-четверте, це загальна етична та моральна підзвітність усіх суб'єктів, включаючи громадян, підприємства, громади та публічний сектор.

Якщо щось йде не так, межа між повноваженнями, підзвітністю та відповідальністю органів влади та користувача стає важливою, тому необхідна також відкрита та справедлива процедура оскарження. Можливо, потрібно буде укладати офіційні угоди, такі як Угода про рівень обслуговування або статут громадян, як для окремих осіб, так і для груп користувачів. Прикладом є Статут електронного уряду щодо громадян в Нідерландах [261]. Підзвітність повинна бути чіткою і простежуваною, щоб, якщо щось пішло не так, було чітко зрозуміло, хто несе відповідальність і як можна вирішити ситуацію.

Простота допомагає усім цим питанням, підвищуючи розуміння та усвідомлення демократичного процесу. Однак, як показує практика, електронний уряд часто призводить до підвищення складності та масового розмивання між ролями та завданнями, коли задіяно так багато суб'єктів й так багато голосів вимагають, щоб їх почули.

Отже, у цілому можна визначити п'ять основних викликів для електронного врядування у контексті забезпечення кібербезпеки:

1. Публічному сектору властива велика ступінь оперативної незалежності та «ізольованості» між різними його частинами, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного.

2. Наразі важливі загальнодоступні дані створюються, зберігаються та застосовуються суб'єктами та особами поза органами влади, тому визначення безпеки публічного сектора має бути розширене та переосмислене.

3. Поведінка людини, раціональна чи ні, є стрижнем кібербезпеки – що

люди думають щодо своєї ідентифікації, даних про неї, кому вона належить, хто має до неї доступ і як вона використовується.

4. Існує зворотна залежність між використанням систем (що заохочується), і безпекою цих систем, але наразі не зрозуміло, як досягти тут певної рівноваги.

5. Користувачі електронного уряду, можливо, потребують такого ж кіберзахисту від органів влади, як органи влади потребують захисту від третіх сторін, зокрема, коли органи влади некомпетентні або корумповані.

Наслідки цих викликів полягають у тому, що координація та контроль стають все складнішими, а спектр загроз кібербезпеці, які потрібно подолати, збільшився в обсязі та масштабах для всіх суб'єктів суспільної сфери. Деякі відповіді на перші чотири виклики очевидні. Зрозуміло, що всеосяжні стратегії для всіх органів влади щодо подолання викликів кібербезпеки мають бути розроблені та застосовані у тісній співпраці з приватним сектором, який надасть деякі рішення, але також має бути швидким та усвідомлювати постійно мінливий ландшафт загроз.

Оскільки для таких загроз не існує політичних кордонів, необхідно узгодити та налагодити міжнародне співробітництво. Мабуть, найважливішим з усього є те, що культурні зміни в органах влади мають здійснюватися у зв'язку з усвідомленням питань кібербезпеки, відповідальності за їх вирішення та робочих практик, що є основою цих питань.

Як зазначали консалтингова компанія Booz Allen Hamilton [250] та журнал Fed Tech (https://fedtechmagazine.com), інші відповіді випливають із цих загальних переконань, та включають необхідність вдосконалення загального управління та координації кібербезпеки, спрощення процесів та правил, а також необхідність виховування відповідних здібностей та навичок у публічному секторі. В опитуванні 2017 року, проведеному компанією TechAmerica, було зазначено, що «високий відсоток порушень безпеки відбувається, оскільки внутрішні користувачі недбалі або не дотримуються

процедур» [478, с. 8].

Місцеві органи влади, можливо, знаходяться під загрозою навіть більшою мірою, ніж центральні через їх відносну нестачу ресурсів та досвіду, але навіть тут можна зробити багато чого. Відповідно до посібника з питань кібербезпеки, опублікованого Міждержавним центром обміну інформацією та аналізу у співпраці з Департаментом внутрішньої безпеки США, це включає усвідомлення проблеми; призначення відповідальності; захист основного обладнання, програмного забезпечення та інформації; контроль доступу; поліпшення навчання та обізнаності; та забезпечення безпечної утилізації.

Відповіді на п’ятий виклик набагато менш прості, і для подолання цього виклику може знадобитися поступова зміна образу мислення. Однак, як на це вказував Європейський журнал е-практики (European Journal of e-Practice) за 2010 рік, зараз багато свідчень вказують на переваги створення нейтральних довірених третіх сторін між органами влади та постачальниками даних, з одного боку, та громадянами з іншого, а також на необхідність забезпечення справедливого захисту інтересів та прав усіх зацікавлених сторін. Такі треті сторони можуть бути комерційними, громадськими або навіть коло-урядовими органами, але вони мають бути юридично та операційно незалежними та сприйматися саме такими. Вони можуть з перевагами виконувати деякі з наступних завдань:

• Виступати як «чемпіон» та «сторожовий собака» для користувачів щодо використання даних та участі у політиці та прийнятті рішень, таким чином, бути як «омбудсмен» для користувачів у відносинах з органами влади.

• Погодити та оприлюднити громадянську хартію прав та обов’язків користувачів щодо використання публічних даних та громадської участі, покладаючись на те, що вже є у законі чи нормативно-правових актах, та відкрити це для обговорення користувачами та внесення змін.

• Визначити та впровадити рамки для реальної мотивації,

стимулювання та винагороди користувачів за залучення до розробки послуг та участі у політиці.

• Постійно контролювати потенційні ризики та інформувати користувачів про них, а також пропонувати можливі рішення та допомогу.

• За запитом, та якщо доцільно, забезпечувати як про-активну, так і пасивну модерацію Web 2.0 медіа, а також нейтрально і врівноважено допомагати у проведенні рамкових дебатів.

• Відстежувати та підтримувати права користувачів на конфіденційність та захист даних у відносинах з органами влади та інших їхніх інтересів. Це може включати запобігання неправомірному використанню особистих даних, незалежно від того, надаються вони свідомо користувачами чи збираються автоматично під час використання сервісу.

• Забезпечувати, щоб всі публічні послуги, хто б їх не надавав, ідентифікували походження всіх даних та інших використаних джерел, водночас дотримуючись інших вимог до відкритого джерела щодо відповідної власності та відповідальності. Це має також включати функції моніторингу та перенаправлення для забезпечення того, щоб будь-яка служба, розроблена для громадського використання, відповідала узгодженим стандартам точності, якості та суспільного блага.

• Незважаючи на величезні потенційні вигоди від звільнення всіх типів публічних даних, існує небезпека перевантаження даних та нецільового використання даних. Дані, як і статистика, можуть бути серйозно зіпсовані з метою, щоб вони означали будь-що, чого бажає будь-хто. Довірена третя сторона має відстежувати це та надавати нейтральні та прозорі настанови, а також втручатися в такі питання.

Такі, як ці, запобіжники важливо встановити для забезпечення того, щоб органи влади або будь-які суб’єкти не маніпулювали неналежним чином іншими суб’єктами. Цьому також сприятиме забезпечення відкритості та прозорості публічних даних та процесів, оскільки це врівноважує владу з усіма суб’єктами та зменшує зловживання та корупцію.

1.4. Системи кібербезпеки в публічному секторі: зміст і впровадження

Активна розробка та впровадження *систем* кібербезпеки (СКБ) на різних рівнях почались з початку 2000-х років. При цьому загальні принципи та основні особливості таких систем кібербезпеки знайшли відображення у низці керівних документів, основні з яких наведено у таблиці 1.1.

Таблиця 1.1

Основні глобальні системи кібербезпеки

№	Рік	Система	Керівні документи
1	2004	Стратегія кібербезпеки Організації американських держав (OAS)	Комплексна міжамериканська стратегія кібербезпеки: мультиаспектний та міждисциплінарний підхід до створення культури кібербезпеки [428]
2	2007	Глобальна програма кібербезпеки (ITU- GCA)	Звіт голови Групи експертів вищого рівня (HLEG) щодо Глобальної програми кібербезпеки (GCA) MCE [458] Керівництво з національної стратегії кібербезпеки [368] Глобальний індекс кібербезпеки (GCI) [369]
3	2010	Структура Союзу комерційного програмного забезпечення (BSA)	Глобальна система кібербезпеки BSA [258]
4	2012	Принципи та керівні вказівки Всесвітнього економічного форуму (WEF)	Партнерство заради забезпечення кіберстійкості: ризик та відповідальність у гіперпов’язаному світі - Принципи та керівні вказівки [515]. Ризик та відповідальність у гуперпов’язаному світі: шляхи до глобальної кіберстійкості [516]. Ризик та відповідальність у гіперпов’язаному світі: значення для підприємств [517].
5	2012	Керівництво експертного центру спільного кіберзахисту (CCDCOE)	Керівництво по системі національної кібербезпеки [384]

Продовження табл. 1.1

№	Рік	Система	Керівні документи
6	2012	ISO 27032	ISO/IEC 27032:2012 Інформаційні технології. Методи забезпечення безпеки. Керівні вказівки по кібербезпеці [365]
7	2012	Стратегія кібербезпеки ЄС	Національні стратегії кібербезпеки: практичне керівництво з розробки та реалізації [314]. Стратегія кібербезпеки Європейського Союзу: відкритий, безпечний та надійний кіберпростір [310].
8	2013	Керівництво з кібербезпеки Microsoft	Розробка національної стратегії кібербезпеки: основи безпеки, зростання та інновації [413]
9	2013	Nexus для кібербезпеки від ISACA	Трансформація кібербезпеки [364]
10	2014	Система Національного інституту стандартів та технологій (NIST)	Система для покращення критичної інфраструктури кібербезпеки [426]
11	2014	Модель спроможності та надійності розробки кібербезпеки (CMM)	Модель спроможності та надійності розробки кібербезпеки [332]
12	2015	Керівні принципи кібербезпеки Співтовариства	Підхід Співтовариства до розробки національних стратегій кібербезпеки: керівництво по створенню цілісного та всеоб'ємного підходу до створення безпечного, надійного та безвідмовного кіберпростору [288] Модель кіберуправління Співтовариства [281]

Певні особливості та відмінності можуть бути знайдені в кожній СКБ, адже кожна СКБ у певному сенсі є унікальною.

Проаналізувавши зазначені керівні документи, ми визначили чотири аспекти такої унікальності, а саме: 1) заохочувані дії; 2) драйвери; 3) середовище та 4) аудиторія (табл. 1.2).

Таблиця 1.2.

Різні аспекти систем кібербезпеки

Рік	**Система кібербезпеки**	**Заохочувані дії**	**Драйвери**	**Середовище**	**Аудиторія**
2004	Стратегія в області кібербезпеки OAS	Позитивна взаємозалежність	Ризикоцентричний	Регіональне	Країна-член OAS
2007	ITU-GCA	Позитивна взаємозалежність	Ціннісноцентричний	Міжнародне	Члени ITU
2010	Система BSA	Позитивна взаємозалежність, підвищення кіберспроможності	Ризикоцентричний	Міжнародне	Уряд
2012	Принципи та рекомендації WEF	Позитивна взаємозалежність, підвищення кіберспроможності	Ризикоцентричний	Міжнародне	Члени WEF
2012	Керівництво CCDCOE	Позитивна взаємозалежність, підвищення кіберспроможності	Ціннісноцентричний	Регіональне	Члени NATO
2012	ISO27032	Позитивна взаємозалежність	Ризикоцентричний	Міжнародне	Організації
2013	Керівництво з кібербезпеки Microsoft	Позитивна взаємозалежність, підвищення кіберспроможності	Ризикоцентричний	Міжнародне	Органи влади
2013	Стратегія кібербезпеки ЄС	Позитивна взаємозалежність	Ціннісноцентричний	Регіональне	Члени ЄС
2013	Система кібербезпеки ISACA Nexus	Підвищення кіберспроможності	Ціннісноцентричний Ризикоцентричний	Внутрішня організація	Організації
2014	Система NIST	Підвищення кіберспроможності	Ціннісноцентричний Ризикоцентричний	Внутрішня організація	Організації
2014	CMM	Підвищення кіберспроможності	Ризикоцентричний	Внутрішня організація	Організації
2015	Керівні принципи кібербезпеки Співтовариства	Позитивна взаємозалежність	Ціннісноцентричний Ризикоцентричний	Регіональне	Країни Співтовариства

При цьому, заохочувана дія – це бажана чи рекомендована дія, що пов’язана з основним змістом СКБ; драйвер є фактором, що мотивував створення даної СКБ; середовище – це ситуаційні обставини, в яких можна використовувати СКБ; аудиторія – ймовірні користувачі СКБ.

Розглянемо зазначені аспекти докладніше.

1. Заохочувані дії.

Заохочувані дії у СКБ можна поділити на два основні типи. Дії першого типу просувають колаборацію з іншими акторами (зовнішня стратегія), в той час як дії другого типу спрямовані на збільшення кіберпотенціалу певної організації, інституції, структури тощо (внутрішня стратегія).

Дії першого типу сприяють співпраці між різними акторами в кіберпросторі, посилюють їхню позитивну взаємозалежність. Основна ідея, закладена в основу цих дії, полягає у тому, що кібербезпека є загальною відповідальністю, а виникаючі проблеми пов’язані зі взаємозалежностями всіх зацікавлених сторін у кіберпросторі [258; 310; 365; 458]. Тому захист кіберпростору не є окремою відповідальністю однієї організації (інституції, структури), натомість, він повинен стати загальною справою і, як наслідок, потребує партнерства між зацікавленими сторонами [515]. Цей тип включає такі СКБ, як ISO/IEC 27032, Принципи та керівні вказівки WEF, Глобальна повістка денна по кібербезпеці ITU, Стратегія кібербезпеки OAS та Керівництво по кібербезпеці CTO.

На відміну від дій, орієнтованих назовні, інший тип заохочуваних дій підтримує внутрішні процеси та сприяє внутрішньому укріпленню організації (інституції, структури) шляхом створення/збільшення кіберпотенціалу. В той час як заохочувані зовнішні дії спрямовані на спільну боротьбу з кіберзагрозами, для організації (інституції, структури) також важливо мати достатню кіберспроможність, щоб бути надійним та сильним самостійним актором. З цієї причини, деякі СКБ, такі як Oxford University CMM та система NIST, виступають за посилення організаційного потенціалу,

наприклад, шляхом нарощення потенціалу людських ресурсів, укріплення критично важливих інформаційних інфраструктур та зміцнення внутрішніх систем (тобто нормативних актів, правил та організаційної структури).

2. Драйвери.

Як показує аналіз СКБ, стратегія кібербезпеки може визначатися двома загальними драйверами: ризиком та цінностями. Орієнтовані на ризик або на цінності драйвери здійснюють значний вплив на дії та загальну розробку стратегії кібербезпеки. Мета першого драйвера, орієнтованого на ризик, полягає у тому, щоб звести до мінімуму ризики, пов'язані з кіберзагрозами. Цей загальний драйвер відіграє важливу роль у стратегії кібербезпеки – оскільки кіберпростір характеризується невизначеністю, то необхідно оцінювати ризики та керувати ними.

Але у той час, коли деякі СКБ роблять акцент на попередженні ризиків, пов'язаних з кіберзагрозами, інші рекомендують зосередитись на узгодженні цінностей організації (інституції, структури) зі стратегією кібербезпеки. Тому інший драйвер, тобто драйвер, орієнтований на цінності, вказує на те, що розробка системи кібербезпеки була обумовлена чи заснована не певних цінностях. У такому ціннісно-орієнтованому контексті, створення кіберполітики означає розгляд кіберпростору не лише як ізольованого домену, а й як сфери, що включає політичну ситуацію та загальну національну стратегію розвитку [384]. Тому, захист кіберпростору має зважати також і на політичні чинники. Наприклад, Система кібербезпеки Співдружності ґрунтується на таких цінностях Співдружності, як захист основних прав людини, збереження відкритого, вільного та безпечного кіберпростору, розширення демократії, підтримка міжнародного миру та безпеки й заохочення сталого розвитку [288]. Всередині приватної організації це може прийняти форму узгодження бізнес-стратегії зі стратегією безпеки, що означає додавання функції кібербезпеки на основі бізнес-середовища, бізнес-цілей та цілей безпеки [364; 426].

СКБ, що містять орієнтовані на цінність драйвери, можна знайти, в

першу чергу, в IGO СКБ, таких як Керівні принципи Стратегії кібербезпеки Співдружності, Стратегія кібербезпеки ЄС, Структура кібербезпеки CCDCOE та ITU-GCA, де основним є намір просувати свої інституціональні цінності (табл. 1.3).

Таблиця 1.3.

Ціннісноорієнтовані чинники для розробки кіберстратегій

Система	**Чинники**
Структура кібербезпеки CCDCOE	Національна безпека сприяє створенню Національної стратегії кібербезпеки, яка повинна враховувати 5 мандатів і 5 дилем
Керівні принципи Стратегії кібербезпеки Співдружності	Застосування принципів Співдружності
Стратегія кібербезпеки ЄС	Пропагування цінностей ЄС Захист основних прав Доступ для всіх Демократичне та ефективне багатостороннє управління
ITU-GCA	Юридичні чинники Технічні та процедурні чинники Організаційні структури Нарощування потенціалу Міжнародне співробітництво.
Стратегія кібербезпеки OAS	Розробка міжамериканської стратегії боротьби з загрозою кібербезпеці
Система NIST	Бізнес стратегія
Система ISACA	Бізнес стратегія

3. Середовище.

Неможливо впроваджувати та розвивати СКБ, реалізовувати стратегії з кібербезпеки не розуміючи їх зовнішнє середовище. При цьому слід зважати на те, що деякі системи покликані забезпечити відповідні результати на організаційному рівні, а інші призначені для використання на регіональному

або міжнародному рівні (що вимагає позитивної взаємозалежності між міжнародними кіберорганізаціями). На організаційному рівні, беручи до уваги систему NIST та CMM в якості прикладу, системи можуть бути належним чином реалізовані, надаючи лише вузьку сферу внутрішніх організаційних «налаштувань», наприклад, для посилення кіберспроможності організації або критичної інформаційної інфраструктури.

Інші структури, такі як ITU-GCA, що мають широкий спектр можливостей для використання в міжнародних масштабах, потребують позитивної взаємозалежності між кожним суб'єктом, пов'язаним з даною сферою, наприклад, шляхом розвитку міжнародного співробітництва та співпраці у даній сфері. Деякі системи працюють лише для певної аудиторії. Зазвичай це системи, створені для членів міжнародної структури, які мають спільні інституційні цінності, наприклад, це такі системи як Керівні принципи Стратегії кібербезпеки Співдружності та Структура кібербезпеки CCDCOE. У цьому випадку головна мета цієї системи – взаємодія з кожним членом, який поділяє загальні інституційні цінності.

Таким чином, зовнішнє середовище СКБ можна поділити на три рівні: перший – організаційний рівень, другий – регіональний рівень, третій – міжнародний рівень. Організаційний рівень, як правило, стосується підвищення потенціалу організації, тоді як інші два мають на меті забезпечення позитивної взаємозалежності різних суб'єктів у сфері кібербезпеки. При цьому організаційна система може використовуватися як система, що доповнює системи вищого рівня, тому організація може також впроваджувати ще одну систему високого рівня поряд із системою організаційного типу. Регіональна система, як правило, будується для задоволення конкретних потреб країн-членів, які мають подібні спільні інституційні цінності. Натомість міжнародні системи, підкреслюючи важливість позитивної взаємозалежності, що має характер кооперації, сприяє встановленню співпраці будь-яких організацій і структур, що мають аналогічні інтереси.

4. Аудиторії.

Відповідно до аудиторії або передбачуваних користувачів СКБ можна розділити на два типи: 1) СКБ, орієнтовані на специфічну аудиторію; 2) СКБ, орієнтовані на загальну аудиторію.

СКБ першого типу, як можна бачити з назви, створені для конкретного типу аудиторії. Наприклад, система NIST була розроблена у відповідь на Указ Президента США № 136362 від 11.05.2017, оскільки ця система була спочатку побудована для оператора критичної інформаційної інфраструктури в Сполучених Штатах Америки. Як інший приклад можна навести такі СКБ, як Стратегія кібербезпеки OAS, Стратегія кібербезпеки ЄС та Керівні принципи Стратегії кібербезпеки Співдружності, які були створені для членів відповідних міжнародних утворень та приведені у відповідність з їхніми місіями. Все це сталося тому, що більшість міжнародних організацій, таких як OAS, ITU, EU/ENISA, NATO/CCDCOE та CTO, розробили свої СКБ з акцентом на створення стратегій кібербезпеки країнами-учасниками.

Другий тип СКБ має загальну застосовність щодо своєї аудиторії та зосереджений на наданні організаціям і структурам можливості збільшити їхню спроможність зменшити кіберзагрози; їх може використовувати будь-яка організація та структура, оскільки вони не прив’язані до конкретної місії. Цей тип СКБ зазвичай будують НУО та академічні установи, такі як Оксфордський університет, ISO/IEC, Microsoft або BSA.

Таким чином, кожну СКБ можна охарактеризувати, віднісши її до певного типу за категоріями: заохочувані дії – позитивна незалежність або збільшення потенціалу; драйвери – орієнтовані на ризик або орієнтовані на цінності; середовище – організаційне, регіональне або міжнародне; аудиторія – специфічна або загальна. Але у той же час, СКБ можуть мати і демікласифікацію, що означає проміжне положення між декількома категоріями. Наприклад, незважаючи на те, що система NIST розроблялася на підставі Указу Президента США, її можуть використовувати організації або критичні інфраструктурні компанії за межами США. Аналогічна ситуація

стосується і СКБ WEF, які призначені для членів цієї організації і зосереджуються на забезпеченні безпеки економічних відносин. Однак принципи, закладені у цих СКБ, можуть бути прийняті глобально будь-якою організацією.

Хоча існують різні точки зору на сутність і зміст СКБ, також існують і загальні моменти, притаманні більшості СКБ. Хоча існують різні точки зору на сутність і зміст СКБ, також існують і загальні моменти, притаманні більшості СКБ. І насамперед це стосується тих понять, що використовуються для опису побудови і розвитку СКБ. Проаналізувавши багато як концептуальних документів, про які йшлося вище, так і наукових джерел, нами було визначено тридцять спільних понять, що зустрічаються у багатьох з них (табл. 1.4) і стосуються забезпечення кібербезпеки в органах публічної влади.

Таблиця 1.4

Спільні поняття в описах систем кібербезпеки

Спільні поняття	**Загальне трактування**	**Кількість документів**	**Кількість згадувань**
Побудова онлайн-довіри	Підвищення впевненість всіх сторін у використанні кіберпростору	15	228
Цифрове резервування	Підтримання стійкості та можливостей системи, резервне зберігання даних	3	11
Захист важливих активів кіберпростору	Захист нематеріальних та матеріальних критичних кіберактивів, таких як конфіденційність, дані та інфраструктура	11	27
Просування конфіденційності в Інтернеті	Сприяння захисту інформації від несанкціонованого доступу та розголошення	13	170
Створення координації, співпраці та взаємодії	Координування, співпраця та взаємодія із зацікавленими органами кібербезпеки, включаючи зовнішніх та внутрішніх акторів	17	371
Зовнішнє	Зовнішні дії	16	167

Продовження табл. 1.4

Спільні поняття	Загальне трактування	Кількість документів	Кількість згадувань
Альянс та партнерство	Співпраця з іншими організаціями для взаємної вигоди у сфері боротьби з кіберзагрозами та реагуванням на небезпечні події та інциденти	12	62
Дипломатія та «м'яка сила»	Використання здатності визначати міжнародні норми та стандарти, що стосуються міжнародної поведінки в кіберпросторі, представляючи форму «м'якої сили»	3	4
Обмін інформацією	Співпраця, обмін інформацією про кіберзагрози та кібератаки, аби бути в курсі останніх погроз та подій	12	50
Сприяння залученню	Сприяння інклюзії та розподіленню відповідальності між всіма стейкхолдерами у сфері кібербезпеки	12	32
Освоєння третьою стороною	Забезпечення дотримання кібербезпеки третіх сторін, які не підпорядковуються внутрішнім політикам організації, структури	8	23
Внутрішнє	Внутрішні дії	16	202
Комунікація	Взаємодія з усіма акторами з приводу забезпечення кібербезпеки	6	17
Координація	Координація за допомогою внутрішньої системи мандатів кібербезпеки	12	64
Створення управління	Створення набору систем та механізмів для керування кібербезпекою, включаючи організаційну структуру, офіційні політики та керівні принципи для деяких аспектів кібербезпеки	12	54
Ролі та відповідальність	Мінімізація функцій, що дублюються між організаціями шляхом створення чітких ролей та обов'язків	13	66
Профілювання кібербезпеки	Визначення структури цілей	14	249
Узгодження стратегії з основними цінностями	Встановлення послідовної підтримки основних цінностей стратегічними заходами	11	87

Продовження табл. 1.4

Спільні поняття	**Загальне трактування**	**Кількість документів**	**Кількість згадувань**
Бюджетування та визначення ресурсів	Визначення бюджетів та необхідних ресурсів для реалізації заходів з кібербезпеки	12	46
Створення припущень	Оцінювання того, що потрібно організації (структурі) для забезпечення кібербезпеки, та визначення її контексту	12	109
Сприяння освоєнню	Заповнення розриву між небезпечними та безпечними умовами функціонування шляхом збільшення кіберспроможності, можливостей та стійкості внутрішніх стейкхолдерів для досягнення необхідних результатів	16	270
Обізнаність	Підвищення поінформованості людей про кіберпростір, зокрема, шляхом створення керівництв по безпеці, допомоги стейкхолдерам у розумінні їх ролей та обов'язків в кіберпросторі, а також підвищення залученості суспільства	13	76
Культура	Просування культури кібербезпеки	4	14
Дослідження та інновації	Сприяння дослідженням та інноваціям у сфері кібербезпеки	10	24
Інноваційні технології	Розробка та впровадження технологій і методів, які використовуються як надійні інструменти для боротьби з кіберзлочинністю	8	31
Реактивність	Раннє виявлення загроз та підвищення потенціалу, готовності та залученості при адаптації до загроз. Це також включає створення груп для реагування на інциденти	8	48
Розширення прав та можливостей людини	Посилення кадрового потенціалу	13	62
Огляд	Переконання у тому, щоб програма кібербезпеки мала необхідні цілі	12	173
Перевірка та аналіз	Забезпечення моніторингу та аналізу поточної ситуації	7	52

Закінчення табл. 1.4

Зворотній зв’язок	Залучення зовнішніх спостерігачів для повідомлення про випадки неправомірних дій	5	9
Уточнення програми	Регулярне докладання зусилля для постійного покращення програми кібербезпеки та її оцінка з метою удосконалення відповідної стратегії	9	52
Самооцінка	Виявлення нових тенденцій та потреб кіберпростору, що розвивається	10	51
Створення правового середовища	Розробка правового середовища як основи для визначення легальної та нелегальної діяльності в кіберпросторі	16	132
Визначення політик	Створення легального обґрунтування для здійснення дій у кіберпросторі	13	55
Розробка стратегії та відповідних рамок	Розробка стратегії, механізмів її реалізації та «дорожньої карти», що функціонують як тактичне та пряме керування для захисту кіберпростору	10	42
Посилення правового аспекту	Ухвалення спеціального законодавства з питань кібербезпеки	10	38
Розробка стандартів	Розробка і впровадження стандартів у сфері кібербезпеки	15	117
Сприяння сумісності	Дотримання визнаних стандартів, керівних принципів, норм та кращих практик, які є відкритими, глобальними та загальноприйнятими на міжнародному рівні	13	49
Стандартизація поведінки	Розробка та встановлення мінімальних вимог до поведінки у кіберпросторі	8	42

Зазначені основні поняття ми пропонуємо далі поділити на дві групи, відповідно до їх змісту: 1) виміри кібербезпеки; 2) дії, необхідні для забезпечення кібербезпеки (рис. 1.4).

Як можна бачити з рисунку, до першої групи входять п’ять вимірів кібербезпеки: людський, організаційний, інфраструктурний, технологічний, нормативний. А до другої групи належать такі заходи: побудова онлайн-

довіри; розвиток координації, співпраця та кооперація; профілювання кіберстану; сприяння впровадженню СКБ; перегляд; створення правового середовища; встановлення стандартів. Розглянемо їх.

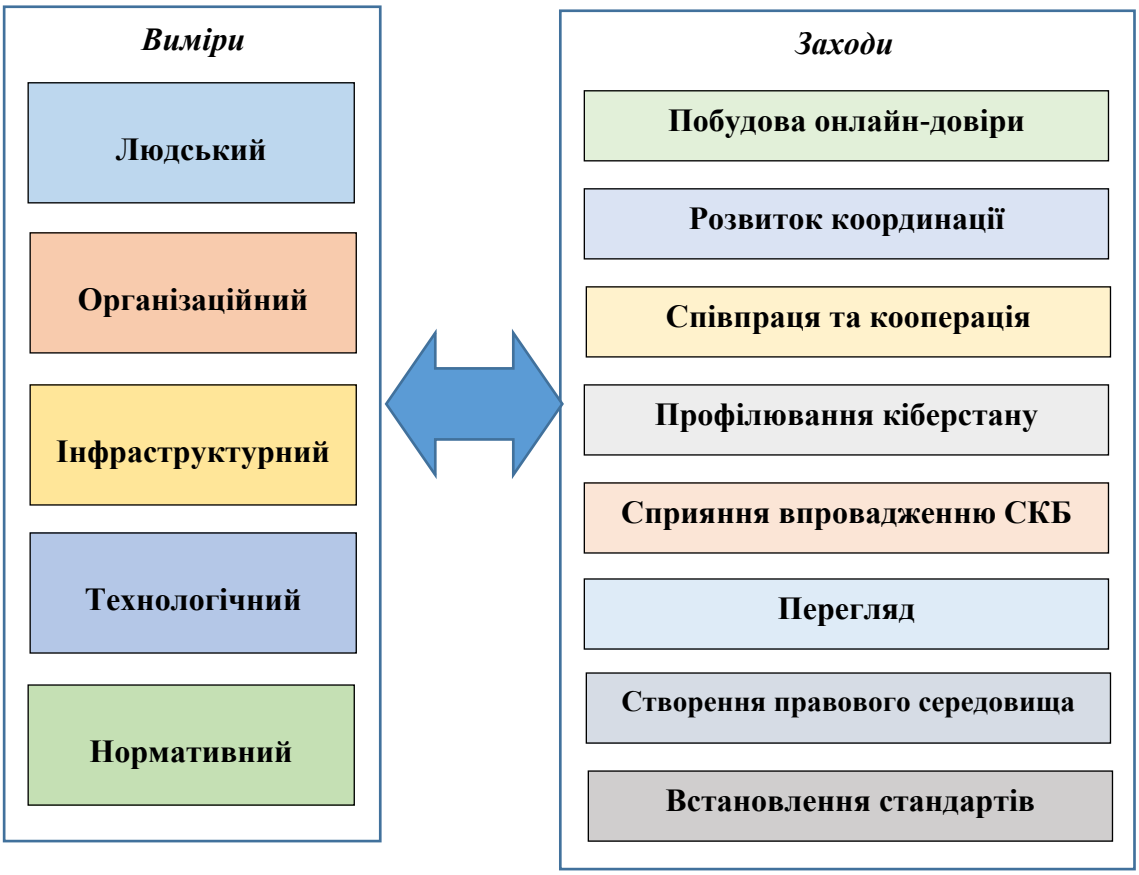

Рис. 1.4. Концептуальні засади забезпечення кібербезпеки в органах публічної влади

Виміри кібербезпеки.

Людський вимір є найбільш фундаментальним і, можливо, найбільш слабким елементом кібербезпеки. Хоча кіберпростір побудований на технологіях, людина управляє ними і контролює їх. Оскільки люди є основними акторами, що забезпечують кібербезпека, недостатня поінформованість і недостатні знання роблять людей головною проблемою і найбільш вразливою ланкою в порівнянні з іншими. Крім того, вирішення проблеми нестачі знань не є простим завданням, оскільки вимагає навчання

та підготовки протягом певного часу. З цієї причини СКБ рекомендують посилення кібербезпеки шляхом підвищення обізнаності, розвитку культури кібербезпеки, а також забезпечення навчання осіб, які займаються питаннями кібербезпеки.

Організаційний вимір зосереджений на інститутах всередині кіберпростору. Це функціональна структура, яка контролює кіберпростір. Зміцнення цього виміру може відбуватись за двома напрямами: 1) стратегічні дії орієнтовані всередині країни, такі як підвищення потенціалу і можливостей відповідної структури; 2) стратегічні дії орієнтовані назовні, які активізують співпрацю для забезпечення безпеки кіберпростору. Наприклад, перший напрям може бути реалізований шляхом забезпечення необхідних ресурсів для організації та підвищення реагування на кіберзагрози. Однак кожна організація в кіберпросторі також повинна співпрацювати з іншими, наприклад, шляхом визначення чітких ролей і обов'язків для кожної організації, координації дій, обміну інформацією про загрози і створення альянсів і партнерств.

Інфраструктурний вимір є, мабуть, найбільш важливим елементом кіберпростору. Це середовище, яке створює кіберпростір. Без інфраструктури кіберпростір – ніщо, тому зміцнення цього виміру необхідно для підтримки кіберсередовища у цілому. Якщо цей вимір слабкий, транзакції в кіберпросторі можуть «впасти». Тому більшість СКБ звертають особливу увагу на інфраструктурні проблеми, у тому числі, на способи забезпечення безпеки критично важливої інформаційної інфраструктури. У цьому сенсі, структура NIST є найбільш придатною для захисту критично важливої інформаційної інфраструктури, але у більшості випадків системи захисту інформаційної інфраструктури відрізняються від однієї організації до іншої, в залежності від потреб кожної організації та відповідного кіберпрофілю.

Технологічний вимір розширює можливості кіберпростору. Оскільки кіберпростір включає в себе найбільш передові технології, зміцнення цього виміру в першу чергу означає впровадження новітніх та найбільш

ефективних технологій, що забезпечують кібербезпеку і дозволяють проводити подальші дослідження і розробки у цій сфері.

Нормативний вимір структурує кібербезпеку і створює певне імперативне середовище у кіберпросторі. Цей вимір спрямований на формування національної кіберекосистеми шляхом створення нормативно-правової бази та розробки норм і стандартів, а також правозастосування. Хоча деякі стверджують, що кіберпростір не повинний регулюватися і має залишатися вільним від втручання органів влади та політики [239], правова поведінка все ж необхідна для підтримки стабільності в кіберпросторі.

Цікаво порівняти визначені нами виміри з тими, що їх визначає ITU (International Telecommunication Union) і які вважаються багатьма авторами як певні еталони у цій сфері. ITU також визначає п’ять вимірів, але дещо інших: 1) правовий; 2) технічний і процедурний; 3) організаційний; 4) створення потенціалу; 5) міжнародне співробітництво.

Як можна бачити, чотири з п’яти вимірів ITU, – технічний і процедурний, організаційний та міжнародне співробітництво, – можуть бути охоплені організаційним виміром. Як зазначалось, організаційний вимір виступає в якості функціональної структури, що контролює кіберпростір, та передбачає внутрішні стратегічні дії (підвищення потенціалу і можливостей організації, що охоплює такі виміри ITU, як технічні та процедурні, організаційні та створення потенціалу); і зовнішні стратегічні дії (розширення співпраці в цілях забезпечення безпеки в кіберпросторі, що відповідає міжнародному співробітництву ITU).

Натомість, є основних виміри, запропоновані нами, які не визначаються ITU – інфраструктурний і технологічний, а людський вимір хоча і згадується, але не визначається як окремий. Таким чином, запропонована нами класифікація вимірів є більш повною і точною.

Дії, необхідні для забезпечення кібербезпеки.

Побудова онлайн-довіри.

При створенні стратегії кібербезпеки, деякі СКБ рекомендують, щоб

особливу увагу було приділено підвищенню довіри стейкхолдерів до онлайн-середовища, тобто побудові онлайн-довіри. Це означає не лише надання стейкхолдерам (наприклад, громадянам і бізнесу) упевненості в безпечності та надійності онлайн-форм, а також забезпечення доступності відповідної інфраструктури (іншими словами, підвищення стійкості інфраструктури та обслуговування критично важливої інформаційної інфраструктури). Це може бути досягнуто, зокрема, шляхом впровадження надійної системи захисту даних та регулювання конфіденційності, розробки національного плану регулювання в надзвичайних ситуаціях в кіберпросторі (управління національними кризами) та забезпечення захисту критично важливої інформації.

Існують три напрями реалізації дій, що сприяють побудові онлайн-довіри:

1. Збільшення цифрової надлишковості – для підтримки стійкості та можливостей служб, що страждають через негативні наслідки подій, пов’язаних з порушенням кібербезпеки.

2. Захист важливих активів в кіберпросторі – для захисту нематеріальних та матеріальних критичних активів, таких як конфіденційність, дані та інфраструктура.

3. Забезпечення конфіденційності в онлайн-середовищі – для захисту приватної інформації від несанкціонованого доступу та розголошення.

Розвиток координації, співпраці та кооперації.

Враховуючи широкий спектр необхідного захисту кіберпростору, включаючи захист на особистому, соцієтальному, національному та міжнародному рівнях, а також захист глобального кіберпростору, кібербезпека не може забезпечуватись лише одним суб’єктом. Захист кіберпростору потребує співпраці багатьох суб’єктів, і, крім того, кіберпростір потребує кумулятивного захисту. Це означає, що кожний суб’єкт повинен постійно працювати над підтримкою (та покращенням) своєї

кіберспроможності, щоб бути надійним актором у кіберпросторі [518]. В результаті захист кіберпростору потребує дій по забезпеченню координації, співпраці та кооперації усіх стейкхолдерів у сфері кібербезпеки.

Можна визначити дві категорії дій з координації, співпраці та кооперації певної організації. Перша категорія включає в себе взаємодію з іншими організаціями. Інформаційно-пропагандистська діяльність може бути досягнута, наприклад, шляхом альянсів та партнерських відносин з іншими організаціями, розширення можливостей кібернетичної дипломатії та м'якої сили, обміну інформацією стосовно боротьби з загрозами, поділу відповідальності шляхом заохочення інтеграції та збільшення кіберпотенціалу сусідських організацій. Друга категорія включає в себе підвищення рівня внутрішньої координації в рамках організаційної структури. Цей тип дій призначений для покращення зв'язку усіх внутрішніх стейкхолдерів організації, координації їхніх дій у сфері кібербезпеки та створення системи кіберуправління з чіткими ролями та обов'язками.

Профілювання кіберстану.

Деякі СКБ рекомендують визначати існуючі потреби і цілі, перш ніж вживати заходів щодо захисту кіберпростору; це називається профілювання кіберстану. Профілювання кіберстану містить три основні дії: приведення стратегії у відповідність з основними цінностями; складання бюджету та підготовка відповідних ресурсів; формулювання припущень.

Перша дія, узгодження стратегії, покликана встановити організаційну поведінку, що відповідає поточним основним цінностям. При цьому основні цінності повинні застосовуватися як в кіберпросторі, так і в «реальному» світі.

Друга дія, складання бюджету та виділення ресурсів, передбачає формування бюджетів і визначення ресурсів, таких як люди, інфраструктура, фінанси, матеріальні засоби тощо, необхідних для досягнення цілей кібербезпеки.

Третя дія, формулювання припущень, означає оцінку потреб організації

в контексті кіберсередовища. Це включає, наприклад, створення профілів ризику, визначення активів, які повинні бути захищені, визначення вимог безпеки, оцінку вразливостей тощо.

Сприяння впровадженню СКБ.

Впровадження СКБ означає для будь-якої організації створення сильного кіберсередовища. Такі дії можуть приймати форму підвищення обізнаності, створення кіберкультури, інвестування в дослідження та інновації, використання інноваційних технологій, підвищення рівня кіберреактивності, а також навчання з питань кібербезпеки.

Перегляд.

Діяльність, яка здійснюється для захисту кіберпростору, повинна періодично переглядатись, щоб гарантувати, що СКБ виконує свої завдання. Перегляд призначений для коригування стратегії і програм з кібербезпеки для досягнення визначених цілей у даній сфері. Прикладами таких дій можуть бути заповнення спеціальних журналів, налагодження каналів зворотного зв’язку, проведення самооцінки тощо.

Заповнення спеціальних журналів дозволяє реєструвати інциденти безпеки, що, в свою чергу, дозволяє організації краще розуміти і реагувати на ситуації із загрозами і коригувати свою безпеку. Записи у журналах також можна використовувати для перевірки відповідності вимогам до кібернетичного ризику.

Оцінку стратегії і програм з кібербезпеки можна проводити як зсередини, так й із залученням зовнішнього суб’єкта. Перший підхід полягає в проведенні самооцінок, наприклад, шляхом створення ключових показників ефективності (KPI), безперервного моніторингу і порівняльного аналізу. Другий підхід здійснюється шляхом отримання зворотного зв’язку. Отримання зворотного зв’язку означає залучення стороннього спостерігача для повідомлення про інциденти або неправомірні дії. Отримання зворотного зв’язку може приймати форму організації кібервправ, отримання відгуків від окремого експерта або отримання відгуків від певних спільнот.

Створення правового середовища.

Правове середовище забезпечує основу для поведінки в кіберпросторі, оскільки встановлює межу між тим, що допустимо, і тим, що є проступком. Для запобігання і припинення неправомірних дій необхідні відповідні закони і правила [428], тому більшість СКБ радять визначати, що таке правомірна і неправомірна поведінка, і створити відповідне правове середовище. Тобто створення правового середовища передбачає побудову основи для розмежування легальної та нелегальної діяльності в кіберпросторі. Створення правового середовища також може бути використано в якості обґрунтування для прийняття коригувальних заходів проти зловмисних дій в кіберпросторі, а також слугувати основою для розробки та реалізації відповідної політики. При цьому при розробці такої політики СКБ рекомендують враховувати наступне:

1. Політика повинна визнавати природу Інтернету, означаючи, що він повинен зберігати відкритість і вільний потік інформації [310; 437].

2. Політика повинна враховувати усі аспекти сучасної кіберзлочинної діяльності [258; 426].

3. Політика повинна заохочувати співпрацю і розроблятися з урахуванням існуючих міжнародних та регіональних структур [310; 332; 368; 426].

4. Політика повинна використовуватися для мінімізації ризику у кіберпросторі та як форма стримування неправомірної поведінки у ньому [288; 365; 518].

Політика повинна також бути пов’язаною з розробкою стратегії кібербезпеки і визначенням дорожньої карти її реалізації, а також швидко адаптуватися до мінливих соціально-політичних і технологічних умов, нових загроз, що виникають у кіберпросторі.

Одним з важливих аспектів створення правового середовища є прийняття законів, нагляд за виконання яких покладається безпосередньо на правоохоронні органи. Зокрема, це означає прийняття спеціального закону

про кібербезпеку. Але оскільки кіберзлочини охоплюють усю земну кулю та мають широке коло зацікавлених сторін і широкий спектр застосування, слід враховувати наступне:

1. Правоохоронні органи повинні діяти в різних юрисдикціях, оскільки вирішення проблеми кіберзлочинності вимагає міжнародного співробітництва та координації [314].

2. Для забезпечення дотримання закону в кіберпросторі потрібно всебічне розуміння як інноваційних технологій, так і відповідних правових підходів, а також необхідна наявність достатніх спеціалізованих ресурсів і можливостей (наприклад, слідчих, прокурорів і суддів) для викриття злочинів, пов'язаних з кіберзлочинністю [332].

Встановлення стандартів.

Захист кіберпростору вимагає ефективних дій, які можна реалізувати шляхом впровадження передового досвіду та стандартизації поведінки. Цього можна досягти, встановивши стандарти, які також сприяють сумісності та систематизації поведінки у кіберпросторі. Сприяння сумісності означає слідування визнаним міжнародним стандартам кібербезпеки. На даний час існують декілька визнаних стандартів, які можуть використовуватися як своєрідний шаблон. Організації можуть також стандартизувати свою поведінку у кіберпросторі, розробивши і встановивши певні вимоги до неї.

Таким чином, впровадження СКБ є досить непростим процесом, але, більше того, цей процес є циклічним і безперервним. У більшості документів, пов'язаних із СКБ, даний цикл називається життєвим циклом СКБ.

Життєвий цикл СКБ складається з трьох загальних етапів: профілювання кіберстану, досягнення встановлених цілей кібербезпеки та оцінювання. Причому результати оцінювання на останньому етапі використовуються для уточнення кіберстану і удосконалення стратегії кібербезпеки. Ці етапи є у всіх СКБ, хоча можуть називатися і дещо по-різному. Так само схожим є зміст кожного з цих етапів, хоча й існують певні

особливості (табл. 1.5)

Таблиця 1.5

Карта життєвого циклу кібербезпеки

	Профілювання	**Досягнення**	**Оцінювання**
ITU-GCA	План	Дія	Перевірка
Керівництво експертного центру спільного кіберзахисту CCDCOE	Крок 1 – Встановлення політичного керівництва Крок 2 – Визначення потреб/вимог Крок 3 – Розподіл вимог та поставлених цілей	Крок 4 – Сприяння впровадженню СКБ	Крок 5 – Перегляд результатів
Стратегія кібербезпеки ЄС	Розробка	Здійснення	Оцінка
ISO 27032	План	Дія	Регулювання Перевірка
Керівництво з кібербезпеки Microsoft	Ідентифікація ризику	Профілактика	Відновлення
Система NIST	Аналіз ризику Визначення оцінки ризику	Виявлення Реагування Захист	Відновлення
Керівні принципи кібербезпеки Співтовариства	Розробка	Виявлення Реагування Досягнення	Огляд
Nexus для кібербезпеки від ISACA	План Розробка	Впровадження Здійснення	Оцінювання Оновлення

Процес профілювання призначений, як зазначалось раніше, для визначення поточного кіберстану. Для позначення профілювання використовуються різні терміни. Наприклад, ISO використовує «план», ITU використовує «цілі», НАТО використовує «попередній розгляд», WEF використовує «вихідне припущення», Microsoft використовує «встановлення

чітких пріоритетів і базових показників безпеки», СТО використовує «підхід», а ISACA використовує «план і розробка». Але у загальному випадку профілювання можна визначити як процес планування, що містить визначення припущень, узгодження запланованих дій з основними цінностями, формування бюджету, визначення необхідних ресурсів та створення правового середовища.

Досягнення встановлених цілей кібербезпеки є основним засобом захисту кіберпростору. Цей процес повинен здійснюватися на основі припущень, визначених в процесі профілювання. Деякі СКБ використовують терміни, такі як «захищати» (NIST), «робити» (ISO), «способи-засоби» (MCE) або «впроваджувати і працювати» (ISACA), в той час як інші використовують неявні терміни, які в основному описують основні дії в СКБ.

Оцінювання передбачає огляд і аналіз процесу досягнення та отриманих результатів, у тому числі з використанням зворотного зв’язку. Оцінювання тягне за собою перегляд, уточнення і модифікацію стратегії кібербезпеки та СКБ у цілому.

На наш погляд, можна об’єднати визначені вище виміри кібербезпеки та етапи життєвого циклу для створення концептуальної схеми СКБ, яка матиме універсальний характер (табл. 1.6).

Таблиця 1.6

Концептуальна схема системи кібербезпеки

	Профілювання	**Досягнення**	**Оцінювання**
Людський вимір	Розробка бюджету та визначення ресурсів Встановлення припущень	Обізнаність Кіберкультура Забезпечення конфіденційності у кіберпросторі Навчання	Зворотній зв’язок

Продовження табл. 1.6

	Профілювання	**Досягнення**	**Оцінювання**
Організаційний вимір	Узгодження стратегії з основними цінностями Розробка бюджету та визначення ресурсів Створення системи управління Розподіл ролей та обов'язків	Альянс та партнерство Комунікація Координація Дипломатія та «м'яка сила» Обмін інформацією Сприяння включенню Реагування Стороння участь	Уточнення стратегії і програм Самооцінка
Інфраструктурний вимір	Встановлення припущень Визначення ресурсів	Цифрове резервування Інноваційні технології Захист критичних зон кіберпростору Реагування Стандартизація поведінки	Аудит і ведення журналів
Технологічний вимір	Встановлення припущень Визначення ресурсів	Інноваційні технології Сприяння сумісності Дослідження та інновації Реагування	Аудит і ведення журналів
Нормативний вимір	Визначення політики Розробка стратегії і програм	Правове забезпечення Стандартизація поведінки	Правовий контроль

Тобто, як видно з таблиці 1.6, зміцнення п'яти вимірів кібербезпеки можна здійснювати у циклі, що містить три етапи: 1) профілювання поточного кіберстану; 2) здійснення певних дій по забезпеченню кібербезпеки на основі визначеного профілю; 3) оцінювання того, наскільки зазначені дії сприяли досягненню цілей, визначених під час профілювання.

Висновки до першого розділу

Дослідження особливостей інформаційного суспільства, що впливають на кібербезпеку, дало можливість зробити такі висновки:

1. З’ясовано, що відсутність ефективних заходів з кібербезпеки може потенційно вплинути на інформаційну революцію та розвиток інформаційного суспільства по всьому світу. Без відповідних заходів безпеки кіберзагрози можуть підірвати стабільність інформаційних суспільств, зробивши цифрові технології джерелом ризиків, а не лише джерелом розвитку. Крім того, відсутність безпеки цифрових технологій зруйнує довіру користувачів до них, а це, у свою чергу, завадить впровадженню інновацій, насамперед, у публічному секторі. Створення надійних інформаційно-комунікаційних систем має прямі та непрямі наслідки для публічних інтересів інформаційного суспільства, оскільки це дає можливість належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології. Це дає підстави стверджувати, що кібербезпека є суспільним благом.

2. Визначено, що три важливі переваги випливають із управління кібербезпекою як суспільним благом: системний підхід до безпеки; спільна відповідальність між різними стейкхолдерами; розвиток співпраці у сфері кібербезпеки. Що стосується системного підходу, то управління суспільним благом вимагає розгляду як прямих, так і непрямих зовнішніх чинників, а також середньо- і довгострокових наслідків. Це сприяє використанню підходів, спрямованих на визначення та аналіз взаємозалежностей щодо безпеки різних, але пов’язаних, технологій та їх впливу на різні суспільні сфери. Стосовно спільної відповідальності: управління суспільним благом вимагає співробітництва між приватним і публічним сектором в цілях забезпечення високого рівня надійності відповідних систем та інфраструктур. Публічний сектор насамперед повинен встановлювати стандарти,

здійснювати сертифікацію та тестування, процедури нагляду, щоб забезпечити підтримання достатнього рівня кібербезпеки для захисту та сприяння суспільним інтересам, а також вживати відповідних заходів, коли кібербезпека не забезпечується належним чином. У той же час, приватний сектор несе відповідальність за розробку надійних систем, розробку та вдосконалення методів забезпечення надійності послуг та продуктів, які вони пропонують, та співпрацює з публічним сектором для здійснення відповідного контролю. Визначення кібербезпеки як суспільного блага також покладає на користувачів певні обов'язки щодо їх кібергігієни. При цьому розподіл відповідальності між різними акторами, а також необхідність врахування прямих та непрямих зовнішніх ефектів сприяє співпраці та обміну інформацією. Обмін інформацією про уразливість різних систем, наприклад, є важливим для приватного сектора для гарантування надійності інформаційно-комунікаційних системи. У той же час, публічний сектор може підтримувати цю практику, включаючи обмін інформацією та співпрацю як частину ініціатив та процедур щодо підвищення власної спроможності.

3. Виявлено, що кібербезпека охоплює широкий набір практик: оцінка ризиків і тестування проникнення; аварійне відновлення; криптографія; контроль та спостереження за доступом; мережева архітектура, програмне забезпечення та безпека; безпекові операції; фізична безпека тощо. При цьому кібербезпека має три основні складові: 1) інформаційно-комунікаційні системи, які є *надійними* і можуть протистояти атакам; 2) методи та системи виявлення загрози та аномалій для забезпечення *стійкості* інформаційно-комунікаційних систем; 3) забезпечення системної *реактивності* на кібератаки. Причому щоб зрозуміти кібербезпеку в публічному секторі, слід усвідомити конвергенцію трьох основних чинників: глобалізації, ступеню підключення до мережі та тенденції до надання послуг публічному сектора в Інтернеті, що зазвичай називають електронним урядом (е-урядом).

4. Показано, що реформування публічного управління, частиною якого є впровадження електронного врядування, можна спостерігати як

загальносвітову тенденцію, що простежується у багатьох країнах. І це не просто експерименти щодо впровадження нових режимів надання послуг, оскільки електронне врядування неминуче також охоплює (і керується) новими моделями формування політики, новими моделями участі громадян у публічному управлінні та політичних процесах, новими моделями відносин громадян і влади, новими варіантами соціально-економічного розвитку. При цьому електронне врядування слід розглядати як самостійну парадигму публічного управління, оскільки впровадження ІКТ *суттєво* змінило його характер. Це вірно, як з точки зору внутрішньої діяльності органів влади (G2G), так і з точки зору їх взаємодії з іншими стейкхолдерами (G2C та G2B). Слід визнати і те, що електронне врядування сильно впливає на розвиток і в інших галузях, таких як інформаційно-комунікаційні технології та електронна комерція, які у свою чергу впливають на електронне врядування.

5. Визначено, що кіберзагрози можна класифікувати декількома способами, один з яких – порівняння політично вмотивованих загроз (наприклад, кібервійна, кібертероризм, кібершпигунство та хактивізм – хакерство в політичних цілях) із неполітичними (зазвичай фінансово мотивованими, як то кіберзлочин, крадіжка інтелектуальної власності та шахрайство, а також злам для розваги чи відплати, наприклад, від незадоволеного працівника). Ще один спосіб класифікації кіберзагроз – за тим, чи є вони зовнішніми або внутрішніми по відношенню до об’єкта впливу.

6. З’ясовано, що поширення використання ІКТ, поза сумнівом, означає, що публічний сектор має усвідомити та докласти зусиль, щоб уникнути одночасної втрати знань та контролю над основними процесами (та компетенціями, рішеннями та політикою, необхідними для їх підтримки), які є основою надання всіх державних послуг. Необхідно краще зрозуміти, які аспекти діяльності публічного сектора можуть і повинні бути кодифіковані, «товаризовані» (наприклад, за допомогою ІКТ) та передані в аутсорсинг або «підключені до мережі» з іншими суб’єктами, включаючи приватний та

громадський сектори, і, як все більше здається, включаючи користувачів. Ті, що мають приймати рішення, поки що не долучаються до всіх цих питань, але в умовах, коли уряди намагаються скоротити витрати, значення цих питань знову різко зростає. І хоча очевидно, що широке оприлюднення даних публічного сектору може принести величезні переваги, майже напевно існують законні інтереси, які слід захистити від повної прозорості та відкритості. Наприклад, існують, безперечно, законні потреби та інтереси приватності громадян та підприємств, коли їхні дані використовуються органами влади. Однак настільки ж важливими є й інтереси публічних службовців та політиків, особливо під час процесу прийняття рішень та політичної діяльності, наприклад, у захисті від настирливого впливу та моніторингу, які можуть стати наслідком того, що всі їх дії та рішення стають абсолютно прозорими. Це може спричинити стрес та надлишкову зосередженість на вимірюванні та виконанні обов'язків на особистому рівні та призвести до надто бюрократичної позиції, роботи суворо за правилами замість того, щоб бути гнучкими та готовими сприймати вимірний ризик політичних ідей. Це також може спровокувати небажання приймати рішення або брати на себе відповідальність за них.

7. Виявлено, що активна розробка та впровадження систем кібербезпеки (СКБ) на різних рівнях почались з початку 2000-х років. При цьому загальні принципи та основні особливості таких систем кібербезпеки знайшли відображення у низці керівних документів. Певні особливості та відмінності можуть бути знайдені в кожній СКБ, адже кожна СКБ у певному сенсі є унікальною, і аналіз керівних документів з впровадження СКБ дав можливість визначити чотири аспекти такої унікальності, а саме: 1) заохочувані дії; 2) драйвери; 3) середовище та 4) аудиторія. При цьому, заохочувана дія – це бажана чи рекомендована дія, що пов'язана з основним змістом СКБ; драйвер є фактором, що мотивував створення даної СКБ; середовище – це ситуаційні обставини, в яких можна використовувати СКБ; аудиторія – ймовірні користувачі СКБ.

8. З’ясовано, що життєвий цикл СКБ складається з трьох загальних етапів: профілювання кіберстану, досягнення встановлених цілей кібербезпеки та оцінювання. Причому результати оцінювання на останньому етапі використовуються для уточнення кіберстану і удосконалення стратегії кібербезпеки. Процес профілювання призначений для визначення поточного кіберстану, і у загальному випадку профілювання можна визначити як процес планування, що містить визначення припущень, узгодження запланованих дій з основними цінностями, формування бюджету, визначення необхідних ресурсів та створення правового середовища. Досягнення встановлених цілей кібербезпеки є основним засобом захисту кіберпростору. Цей процес повинен здійснюватися на основі припущень, визначених в процесі профілювання. Оцінювання передбачає огляд і аналіз процесу досягнення та отриманих результатів, у тому числі з використанням зворотного зв’язку. Оцінювання тягне за собою перегляд, уточнення і модифікацію стратегії кібербезпеки та СКБ у цілому.

РОЗДІЛ 2
СУЧАСНІ ТЕНДЕНЦІЇ І ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ПУБЛІЧНОМУ СЕКТОРІ

2.1. Особливості розвитку кіберпростору у сучасному світі

Початок XXI століття ознаменувався істотним збільшенням кібератак на різноманітні підприємства та установи у публічному та приватному секторі. Так, шкоди зазнали естонський уряд та парламент, а також офіси політичних партій, естонські банки постраждали від масових кібератак у вигляді розподілених атак за відмову в обслуговуванні; за допомогою шкідливого та шпигунського програмного забезпечення («Stuxnet», «DuQu» або «Flames») було порушено роботу ядерних потужностей в Ірані; було здійснено атаку проти низки польських Інтернет-сервісів на знак протесту проти прийняття Торгівельної угоди проти контрафакту, що, врешті-решт, призвело до її скасування. Згідно з деякими дослідженнями, найчастіше ставали жертвами кібератак Китай і США, в той час як Індія, Пакистан, Південна Корея та КНДР брали участь в більшості атак у 2001-2011 рр. [505]. Щоправда, немає жодних ґрунтовних доказів, що у наступному десятилітті ці тенденції збереглися. Проте всі визнають, що кількість кібератак щороку зростає, а й рівень загроз лише збільшується.

Нижче на двох класичних прикладах буде показано вразливості та можливості кіберпростору у публічному секторі – від ключових об’єктів інфраструктури до міжнародних відносин. Дані конкретні випадки ілюструють мінливий характер середовища безпеки в інформаційну добу. На першому прикладі («Stuxnet») можна побачити, як шкідливий код використовується для нанесення серйозної шкоди ядерній інфраструктурі країни. Існує припущення, що цей акт кіберсаботажу було здійснено певною державою або партнерством держав, враховуючи складність та витратність проекту. На другому прикладі (WikiLeaks) можна побачити, що трапляється,

коли окремий викривач у організації вирішить розкрити конфіденційну інформацію усьому світу. Сайт «WikiLeaks» був апологетом прозорості і надавав користувачам відносно безпечне та надійне середовище для кібершпигунства. Разом ці приклади доводять, що кібербезпека може слугувати для того, щоб налаштувати одну державу проти іншої, окремих осіб проти держав(и), а держави – проти окремих осіб. Набутий досвід можна застосовувати до окремих осіб, організацій та інституцій по всьому світу.

«Stuxnet».

«Stuxnet» – це мережевий вірус, який вражає комп'ютери з операційною системою «Windows» і який був розроблений з метою нанесення шкоди промисловим системам та об'єктам інфраструктури. Його було викрито у 2010 р. Враховуючи саморозповсюджуваний характер «Stuxnet», контроль над поширенням вірусу було втрачено. В результаті «Stuxnet «проникнув на декілька об'єктів по всьому світу, хоч головний удар припав на іранські центрифуги для збагачення урану. Згідно з «Сі-Кей Мегезін», фактично 60% всіх систем, інфікованих Stuxnet, було розташовано в Ірані. Таким чином, кібератака на установки по збагаченню урану в Ірані відкинули ядерну програму цієї країни на декілька років назад.

Окрім цього було уражено 45000 промислових систем управління ключовими об'єктами інфраструктури таких як «електромереж, нафтогазових трубопроводів, загат або комунікаційних мереж» по всьому світу. Щоправда «його структура спрямована на спеціальний набір пристроїв, виготовлених лише у Фінляндії та Ірані, які використовуються для визначення швидкості, з якою обертаються центрифуги» [296]. Також Stuxnet було запрограмовано таким чином, щоб «він не діяв на комп'ютери, які не підключені до механізмів управління, які були ціллю». Таким чином, хоч вірус було виявлено на комп'ютерах по всьому світі, він нашкодив лише центрифугам для збагачення урану у Ірані. В цьому сенсі це була розумна зброя.

В 2005 р. дослідниця проблем безпеки Міріам Данн зауважила, що зв'язок між національною безпекою та вразливостями кіберпростору важко

довести через те, що загрози для ключових об’єктів інфраструктури і «загрозливі сценарії масштабних порушень роботи у кіберпросторі, спричинених лиходіями, залишились виключно сценаріями» [302, с. 10)]. Але «Stuxnet» все змінив. Вперше в історії він надав прямі докази, що кібератаки можуть використовуватися не лише для відключення ключових об’єктів інфраструктури а й для фізичного знищення систем (у випадку з центрифугами для збагачення урану).

Як було зазначено в одній статті у Нью Йорк Таймз, «Stuxnet» – «це найскладніша кіберзброя, яку коли-небудь застосовували» [255, с. 1]. «Stuxnet» продемонстрував, що «атаки за допомогою шкідливого програмного забезпечення ...становлять все більшу загрозу для національної безпеки» [262, с. B3]. Ліма О. Мурчу, дослідник кібербезпеки у компанії «Symantec», з цього привиду зазначив таке: «Stuxnet продемонстрував, що може трапитися, коли злодії встановлюють контроль над промисловими системами» [355]. Джозеф Вайсс, партнер і консультант компанії «Applied Control Solutions» зазначив, що «Stuxnet довів потребу у посиленні федерального нагляду за кібербезпекою у комунальній сфері» [там само]. За його словами «щоб зламати систему управління, багато розуму не треба, а от щоб захистити – треба». Джон Міллер, директор «Accuvant Labs» зауважив, що «тим, хто пише шкідливий код, достатньо написати лише одну якісну шкідливу програму. Тим, хто захищається від шкідливих програм, потрібно захищатися від різних типів шкідливих програм. Тому навіть якби кількість захисників та нападників була рівною, захисники будуть у програші» [406, с. 31].

Ситуація зі «Stuxnet» довела, що подібні кіберзагрози важко попередити. Відомо, що «Stuxnet» навряд чи був результатом роботи одного хакера або навіть команди хакерів. Характер хробака свідчить про те, що це справа рук якоїсь держави або коаліції держав. Аналітики схиляються до такого пояснення походження вірусу з низки причин.

По-перше, «лише організація зі значними фінансовими ресурсами для

розробки, тестування та випуску програми могла...створити шкідливий код Якщо точніше, вірус використовує чотири вразливості «нульового дня» для атаки цілі», а, купівля інформації про ці вразливості «влетить у копієчку, отже більшість приватних команд хакерів не можуть собі дозволити цей вірус» [331, с. 88].

Підтверджуючи цю думку Фрідман зазначив, що «Stuxnet було написано командою, яка включає з десяток програмістів, які працювали над вірусом не менше, аніж півроку, а витрати сягнули понад 3 мільйони доларів» [там само]. Схожої думки дотримуються і фахівці компанії «Microsoft», які оцінили, що «ймовірно створення вірусу зайняло 10 000 людино-днів, а займалися цим системні програмісти вищого рівня» [355]. З часом з'явилися припущення про те, що до виготовлення цього вірусу причетні США та Ізраїль, які за його допомогою намагалися призупинити ядерну програму Ірану. Але ці країни й досі не взяли на себе відкриту відповідальність за кібервійну проти ядерної програми Ірану.

Відзначимо, що з метою безпеки промислових систем управління часто запускають на комп'ютерах, не підключених до Інтернету. В цьому випадку вірус «Stuxnet» був незвичайним, оскільки атакував системи управління, не підключені до Інтернету. Вірус Stuxnet обійшов цей захід безпеки таким чином:

1) його було навмисно або ненавмисно завантажено за допомогою USB-пристрою;

2) він відправив центральному комп'ютеру і програмам запуску промислових систем управління, які вважалися непідключеними до мережі, команду про підключення до Інтернету;

3) отримавши доступ до Інтернету, вірус відправив подробиці системи на сервер, який, ймовірно, знаходився у Данії або Малайзії;

4) з серверу було відправлено інструкції зі зміни частини програмного забезпечення на комп'ютері управління, які у випадку з Іраном були вразливостями «нульового дня» – «прогалинами у захисті програми,

невідомими розробнику» і які необхідно було виявити, щоб скинути центрифуги до максимальної швидкості [473, с. 7];

5) як зазначив Фрідман, аналітик з питань безпеки, «всі тисяча центрифуг у Натанзі було оснащено програмно-керованим контролером [331, с. 88]. Ймовірно, управління кожним контролером відбувалося за допомогою однакового програмного забезпечення і більшість з них (або всі) з'єднані між собою, тому зміни у програмному забезпеченні на одному комп'ютері почали діяти й для інших»; в результаті

6) тисячі іранських центрифуг для збагачення урану – пристроїв, які обертаються на надзвуковій швидкості – було знищено. Метою вірусу було змінити електричну частоту, яка контролює швидкість обертання центрифуг, внаслідок чого вони починають обертатися з шаленою швидкістю, яка перевищує допустимі значення, поки вони не тріснуть або не зможуть обертатися належним чином. Друга частина вірусу змінила мотори конвертера частот, відправивши «нормальні показники, щоб замести сліди» [там само].

Під час цієї атаки Іран втратив одну п'яту своїх центрифуг для збагачення урану.

Грег Тільманн і Пітер Крейл зазначили, що успішність цієї атаки полягала у внутрішніх дефектах ядерної програми Ірану, яку було розроблено зворотнім способом на основі пакистанської моделі, вкраденої у голландців у 1970-х роках. Там же зазначено, що проблему підсилює дефектне поцуплене обладнання, яке Іран намагався розробити зворотнім способом [490]. Технологія збагачення урану за допомогою центрифуг потребує конструювання складного обладнання з точними технічними характеристиками, щоб циліндричні пристрої могли цілодобово крутитися на надзвуковій швидкості. Враховуючи слабкі місця конструкції іранської ядерної програми, система, на думку цих фахівців, була вразливішою, аніж, скажімо, АЕС у США чи Європі [там само].

Одночасно з атакою за допомогою Stuxnet було ліквідовано ведучих

іранських вчених-ядерників. Однією з жертв став Маджид Шахріарі «29-го листопада загинув у Тегерані від вибуху бомби, приклеєної до його автомобіля найманими вбивцями на мотоциклах» [482]. Відщначимо, що на час вбивства пан Шахріарі займався очищенням ядерної програми Ірану від «Stuxnet». На думку низки фахівців, у результаті кібератаки за допомогою «Stuxnet» і ліквідації провідних іранських вчених-ядерників ядерну програму Ірану було відкинуто на декілька років назад, що знизило ймовірність традиційного військового нападу (наприклад, за допомогою крилатих ракет, авіабомбардувань), тим самим, надавши шанс на дипломатичне вирішення конфлікту і врятувавши життя сотням невинних людей.

Проте, науковці за результатами цієї кібератаки зробили декілька висновків, які були можуть бути доцільними для використання не тільки в промисловому, а й публічному секторі.

1. Не користуватися USB-носіями.
2. Вимкнути опцію автоматичного запуску Windows при підключенні USB-носія.
3. Проводити часту заміну апаратного та програмного забезпечення з метою підвищення «надійності захисту від атак» [331, с. 89].
4. Той факт, що ключові об’єкти інфраструктури не підключені до Інтернету, не означає, що вони невразливі до кібератак.
5. Кібератаки можуть відбуватися звідки завгодно (зі сходу або заходу, з боку держав чи окремих осіб, від союзників та ворогів); їх важче передбачити або зупинити, аніж здійснити. Тому злочинець/агресор має більшу перевагу, аніж захисник.
6. «Stuxnet» – це лише початок, але це сигнал і раннє попередження для будь-яких організацій, робота яких залежить від інформаційних мереж. Необхідно виділяти величезні кошти на покращення кібербезпеки, в тому числі раннє виявлення та відслідковування проникнень або аномалій. Часта зміна та покращення систем (як апаратного, так і програмного забезпечення), можуть підвищити рівень безпеки.

7. Початок кібервійни означає нову сферу потенційної вразливості, а при розрахунку параметрів безпеки держави необхідно їх враховувати. Організація безпеки у XXI сторіччі постійно стає складнішою. «Stuxnet» продемонстрував помітне зростання шкідливості потенційних загроз від комп'ютерного хакерства, Інтернет-шахрайства в промисловому та публічному секторах.

8. «Stuxnet» став ілюстрацією того, наскільки просто один рядовий співробітник або сторонній підрядник може запустити вірус в інформаційну інфраструктуру і руйнівні наслідки такого втручання.

9. «Stuxnet» став «майбутнім взірцем прихованої кіберзброї» і за його допомогою «вперше було продемонстровано зброю, створену державою (або державами) для досягнення цілі, якої в інших випадках досягають за допомогою крилатих ракет» [296].

10. Той факт, що код Stuxnet зараз знаходиться в широкому доступі, означає, що зворотна розробка та злочини, скоєні наслідувачами, зроблять творців цього коду та всіх інших ще вразливішими до шкідливих кібератак. Іншими словами, «вірус може повернутися»…

11. «Stuxnet» – це сигнал до розширення або перегляду Женевських конвенцій, що регулюють ведення війни. Вони повинні включати кібервійну, де може уражатися фізична ціль або «електронні та інформаційні ресурси (наприклад, пошкодження даних та сервісів)».

«WikiLeaks».

«WikiLeaks» – це неурядова організація, заснована у 2006 р., з метою підвищення рівня прозорості уряду, покращення стану журналістики, кращого висвітлювання зовнішньої політики та ефективнішого управління міжнародної спільнотою. Зокрема, саме так писали про цю організацію Крістіан Сайенс Монітор і Джуліан Ассанж – редактор та номінальний власник «WikiLeaks». Наразі цей ресурс більш відомий своєю серією опублікованих таємних документів, що нашкодило зовнішній політиці та міжнародним відносинам США. Наприклад, Гілларі Клінтон у статті,

опубліковані в Сідней Монін Геральд, заявила, що «для подолання наслідків розкриття інформації у WikiLeaks знадобиться кілька років» [512, с. A11]. У Хьюмен Івентс WikiLeaks назвали «цунамі у сфері безпеки», найбільшим витоком таємних документів в історії і сигналом для всіх організацій про те, що необхідно захищати конфіденційну інформацію.

Відзначимо, що на «WikiLeaks» було опубліковано більше, аніж півмільйонна таємних урядових документів, багато з яких висвітлювали незручні подробиці зовнішньої політики США, військових операцій в Афганістані, Іраку та Сирії, а також негативні оцінки міжнародної дипломатії США.

Витік інформації призвів до того, що деякі члени вищих ешелонів влади США втратили роботу, зокрема Пі Джей Кроулі, спікер Держдепартаменту, за його коментар про «безглузде» відношення до рядового Бредлі Меннінг (звинувачуваного у витоку інформації) у в'язниці; Хізер Ходжес, посол в Еквадорі, через коментар про корупцію в поліції Еквадору, який з'явився у WikiLeaks; Джин Кретц, посол у Лівії, за коментарі щодо «пристрасної медсестри» Каддафі. Витік інформації також поставив під удар відносини між США та ключовими союзниками, оскільки було поставлене питання про те, наскільки США вдається зберігати конфіденційність закритої інформації. Також вважалося, що витік інформації про війну в Іраку та Афганістані міг поставити під загрозу життя військових із США. Деякі з опублікованих документів поставили союзників у незручне становище, зокрема, кількох голів держав на Близькому Сході [512].

У дискусії між правом держави на конфіденційність у міжнародних справах і правом громадськості на інформацію «WikiLeaks» зайняв сторону громадськості. На сайті організації (на дзеркалі, оскільки хостинг витіснив ресурс організації з публічного домену) вказано, що WikiLeaks діє на основі наступних принципів:

– публікація інформації підвищує рівень прозорості і це дозволяє змінити суспільство на краще;

– вищий рівень контролю дозволяє знизити рівень корупції і зробити всі інститути суспільства демократичнішими, в тому числі уряд, корпорації та інші організації;

– здорові та прискіпливі журналістські канали відіграють важливу роль у досягненні цих цілей [523].

WikiLeaks – це продукт нового інформаційного середовища, яке з'явилось внаслідок появи Інтернету, та збільшеного потоку інформації, який технологічно підтримується по всьому світу. Творці «WikiLeaks» дотримуються тієї ж думки, що і член Верховного Суду Г'юґо Блек, який у 1971 р. під час розгляду справи про свободу преси у Верховному Суді, ініційованою через витік інформації з Документів Пентагону, визначив, що «лише вільна преса без обмежень може ефективно розкрити брехню в урядових колах» [246]. Формально, такої ж думки дотримувалися і керівники США Так, Гілларі Клінтон у своїй промові у Ньюзіумі в 2010 р. після скандалу з Google у Китаї зазначала, що інформаційні мережі допомагають людям дізнаватися нові факти і підвищують підзвітність уряду [512]. Аналогічно, під час візиту до Китаю у 2009 р. Барак Обама відмітив, що чим «вільніший потік інформації, тим сильніше суспільство», оскільки «доступ громадян до інформації підвищує підзвітність уряду» [429].

Між тим, фактично, всі викривачі, які допомагали «WikiLeaks» в отриманні інформації були визнані в США порушниками Закону про шпигунство 1917 р. і звинувачені у «нанесенні шкоди безпеці США шляхом публікації документів» [341, с. 1]. Так, Бредлі Меннінг, 23-річний рядовий Армії США, який служив у розвідці, був звинувачений в тому, що скопіював та відправив майже мільйон таємних документів на «WikiLeaks» [там само]. Ці документи включали:

1. Таємні архівні кадри авіа нальоту в липні 2007 р. на передмістя Багдаду на гелікоптерах Апач, в результаті якого постраждало цивільне населення та журналісти в Іраку (опубліковано у квітні 2010 р.)

2. Архівний журнал бойових дій в Афганістані, який складався з

92000 «звітів про бойову обстановку», складених солдатами, які приймали у бойових діях на суші. Звіти містять оцінку військових дій (опубліковано у липні 2010 р.)

3. Журнал бойових дій в Іраку, який складався з 392000 звітів, де вказувалися подробиці кожної смерті та нещасного випадку під час війни (опубліковано у жовтні 2010 р.)

4. Дипломатичні телеграми Держдепартаменту, який містить 250000 прикладів відвертої оцінки союзників та ворогів США по всьому світу (опубліковано у листопаді 2010 р.)

*З*а словами Меннінга, він «щотижня мав безпрецедентний доступ до таємних мереж впродовж 14 годин на день 7 впродовж більше, аніж 8 місяців [341, с. 2]. Він «приходив з диском CD-RW, на якому було записано музику... стирав її… і виносив інформацію. Зрештою, це стало найбільшим витоком даних за всю історію США». Меннінг пояснював, що він стикнувся із «слабкими серверами, слабкою системою реєстрації подій, слабким рівнем фізичної безпеки, слабкою контррозвідкою і неуважним аналізом сигналів» [там само].

Після публікації цих матеріалів «WikiLeaks» пояснила причини цього на своєму сайті. «У результаті технічного прогресу (зокрема, появі Інтернету та криптографії) ризики, пов’язані з передачею важливої інформації, зменшилися. Ми вважаємо, що не лише громадяни однієї країни слідкують за чесністю свого уряду: інші громадяни слідкують за цим урядом у ЗМІ. Впродовж декількох років до заснування «WikiLeaks» ми помітили, що публікації у світових ЗМІ стають все більше залежними і рідше піднімають незручні питання, пов’язані з урядом, корпораціями та іншими організаціями. На нашу думку, це слід було змінювати [523].

Отже, «WikiLeaks» яскраво вказав на недоліки навіть самих захищених інформаційних систем усього світу і за результатами цього скандалу науковцями було зроблено декілька практичних висновків.

1. Кіберзагрози можуть бути зовнішніми (у традиційному сенсі) та

внутрішніми (викривачі, незадоволені співробітників, колишні співробітники з ідеєю-фікс, злочинці, які діють під маскою лояльного співробітника/свідомого громадянина).

2. Не можна дозволяти підключення зовнішніх носіїв до комп'ютерів, які підключено до серверів з конфіденційною інформацією.

3. Необхідно постійно моніторити мережі на предмет незвичайних бітових та байтових потоків.

4. Надавати співробітникам доступ до секретної інформації необхідно лише у межах, необхідних для виконання своїх обов'язків. Всіх інших слід розділити на категорії, щоб запобігти масштабному витоку інформації до джерел на кшталт WikiLeaks.

5. Необхідно пам'ятати, що у інформаційну добу конфіденційність і цензура стають все слабкішим ресурсом навіть у авторитарних державах. Як зазначив адмірал Блер, колишній Директор національної розвідки США, XXI сторіччя стане добою взаємних образ [247].

6. Навіть якщо інформація конфіденційна, це не означає, під грифом «таємно» постійно приховують погану політику. Якби люди при владі знали, що за ними слідкує весь Інтернет, чи змінилася б їхня поведінка на догоду громадському нагляду? Якщо так, це означає, що вони приймають погані рішення, якщо їх доводиться тримати у таємниці, щоб не порушувати дипломатичні відносини, не викликати протести громадськості та регіональні заворушення. За словами Блера, прозорість уряду і корпорацій – найкращий захист від майбутньої шкоди від WikiLeaks [247].

Таким чином, проблема зростання кількості кібератак на мережі та ускладнення їх характеру робить питання кібербезпеки все більш актуальнішим. Нові агресивніші форми кіберактивності та поява неурядових акторів у якості активних учасників процесів визначення внутрішньої та зовнішньої політики викликають численні запитання про майбутнє публічного сектору з точки зору забезпечення національного суверенітету та незалежності. Широкий діапазон потенційних загроз створює серйозні

виклики існуючим міжнародним структурам, які часто не встигають за кіберпростором, що динамічно розвивається. Водночас, політика, яка націлена проти різних загроз у кіберпросторі, зазвичай розвивається ізольовано, що призводить до невідповідностей та відсутності узгодженості рішень, що ухвалюються окремими урядами. Отже, глобальним кіберзагрозам протиставляються локальні рішення, які часто не встигають за технологіями та тенденціями розвитку кіберзлочинності. Таким чином постає питання визначення цих тенденцій, оцінка їх значення для окремих держав, а також розробка конкретних пропозицій щодо системного протистояння цим загрозам.

Можна зазначити, що у міжнародних наукових та політичних колах протягом останніх років сформувалися певна спільна думка щодо наступних позицій.

1. Всі (більшість держав та їх громадян) згодні, що життєдіяльність людства залежить від мережі, а інформаційні технології – це ключ до подальшого соціального та економічного розвитку.

На практиці це перетікає у зростаюче визнання того, що залежність життя у XXI сторіччі від інформаційної інфраструктури робить всіх (як окремих громадян, так і різноманітні установи, організації, підприємства і навіть цілі країни) надзвичайно вразливими до кіберзагроз.

2. Потенційні загрози є досить серйозними, враховуючи залежність від мережі та відомих випадків вразливості кіберпростору.

3. Наразі сучасні державі не готові боротися з кіберзагрозами; атаки трапляються все частіше, а наслідки все триваліші.

Згідно з дослідженнями конкретних випадків та висновками, всі держави вразливі до переворотів, програми у сфері атомної енергетики вразливі до кібератак, а витоки інформації та революції через «Facebook» можуть нашкодити державам та дипломатичним відносинам між ними.

4. Необхідно вживати певних заходів для того, щоб е цифрове життя та інтереси стали безпечнішими. Хоч конкретні випадки, проаналізовані

вище, не дають конкретних відповідей, як вирішити проблеми, пов'язані з кібербезпекою, вони висвітлюють кілька реальних прикладів того, що чекає людство, якщо воно не буде вживати колективних заходів для захисту цифрового майбутнього. Визнання характеру та масштабу проблеми – це перший крок до її вирішення у майбутньому.

5. Кіберпростір являє собою «справжню», відносно нову сферу взаємодії (як місцевої, так і міжнародної), яка є такою ж важливою, як і взаємодія у повітрі, на морі, на суші та в космосі. «Кіберпростір» – це не наукова фантастика. Він заслуговує на той же рівень взаємодії, захисту і уваги, як і будь-яка інша сфера.

Конкретні приклади демонструють, якими можуть бути «справжня» взаємодія, ризики та можливості у кіберпросторі у XXI сторіччі. Будь-який актив, який залежить від мережевих комунікацій - від дипломатичних відносин до центрифуг для збагачення урану і урядової інфраструктури – вразливий до кібератак.

Між тим, ані науковцям, ані політиками й досі не вдається досягти згоди по таким питанням:

1. Хто/яка(-і) організація(-ї) та особа(-и) повинні відповідати за кібербезпеку (як за напад, так і за оборону)?

Ця картина відповідальності особливо ускладняється географією. Хто охороняє мережу? Приватний сектор? Окремий уряд? Спільнота держав? Окремі компанії? Міжнародні організації? Конкретні приклади нижче ілюструють, наскільки глобальним є масштаб кіберпростору. Організаціям (сім'ям, корпораціям або державам) доведеться навчитися, як краще захищатися, відштовхуючись від минулих атак та вразливостей. В інформаційну добу одна єдина особа з ідеєю-фікс може кинути виклик США і всім їх союзникам на Близькому Сході («WikiLeaks»). Стратегії кібербезпеки повинні бути достатньо гнучкими та обширними, щоб враховувати ці та багато інших випадковостей, які трапляються зараз і можуть трапитися у майбутньому.

2. Що конкретно може зробити кіберпростір безпечнішим (політики/уряд/технологічні спільноти/приватний сектор досі обговорюють це питання, але так і не дійшли згоди; їх рішення іноді порушують конфіденційність або право власності, тому їх відхиляють)?

Це питання є досить чутливим для міжнародної спільноти, оскільки воно включає правові та культурні аспекти. Пошуки рішень досі тривають. Хто такий Джуліан Ассанж? Злочинець (напевно, так, якщо враховувати подробиці справи про некоректний сексуальний вчинок) чи герой, враховуючи, що він публікував подробиці сумнівних закулісних обговорень та пліток, що стосувалися міжнародних відносин? У новій сфері кібербезпеки це питання виникатиме все частіше. Отже, постає необхідність у створенні нової етичної норми для керування взаємодією у кіберпросторі на кшталт універсальної декларації прав людини. Необхідно прийняти узгоджений набір прав та обов'язків в інформаційній сфері. Естонія включила доступ до Інтернету до складу основних прав людини. У більшості країн вже є законодавство проти работоргівлі та дитячої порнографії, яке регулює окремі операції у кіберпросторі. Між тим, необхідно окреслити правові наслідки кібершпигунства та кібератак на ключові об'єкти інфраструктури.

2. Яка політика впровадження кібербезпеки є оптимальною?

Оскільки загрози є досить різноманітними на всіх рівнях (місцевому, національному та міжнародному), важко визначити, яка стратегія або набір стратегій захистить публічний сектор

4. Яку нормативно-правову базу необхідну впровадити для (a) притягнення тих, хто здійснює кібератаки, до відповідальності і (b) для того, щоб бодай превентивно протидіяти кібератакам або кіберзагрозам (реальним і потенційним)?

Загрози у кіберпросторі з'являються швидше, аніж законодавство, яке регулює кібербезпеку. Таке законодавство визначає, чи є кібератака або витік військовими діями, а також яким чином і до якої держави, компанії або особи необхідно застосовувати заходи у відповідь.

5. Яким чином виникнення проблем з кібербезпекою повинно змінити наше сприйняття (систему понять) світу, починаючи від навчання майбутніх поколінь і закінчуючи нашим розумінням того, де відбудуться потенційні атаки у майбутньому.

Є очевидні потреби у перегляді поняття безпеки в інформаційну добу. Мережа, яка об'єднує людей, держави та компаній, стосується кожного аспекту життя, як прямо, так і опосередковано. Залежність від мережевих комунікацій постійно зростає, як і кількість вразливостей. Конкретні приклади ілюструють декілька шарів загроз і можливостей, які існують у інформаційну добу.

Отже, політики, громадські активісти та науковці повинні допомагати і прагнути змін у процесу, контролювати та захищати кіберпростір, особливо коли з'являються очевидні прогалини і виклики у інформаційній (люди, мережі, інфраструктури) культурі. У приватного сектору також є зацікавленість в управлінні та безпеці. Таким чином, кібербезпека – це рухома ціль і живий організм, а не статичне середовище. Через постійні зміни кіберпростір стає складнішим, аніж сукупність його компонентів, що вимагає розробки комплексного наукового підходу щодо регулювання і розвитку цієї сфери.

Як свідчить аналіз результатів наукових досліджень з цієї теми, останнім часом наукові дебати точилися переважно навколо кількості кібератак на установи публічного сектору, а також наслідків загроз, викликаних тими атаками. Серед таких найчастіше називалися, зокрема, отримання безпосередньої матеріальної вигоди, доступ до службової інформації про клієнтів, конкурентів або навіть правоохоронні органи. У сфері міждержавних відносин кібератаки дозволяють меншим державам і недержавним акторам компенсувати свою військову слабкість, а великим державам – стримувати слабших акторів.

Суттєву частину існуючої літератури зосереджено також на питаннях, пов'язаних із захистом інформації, ключових об'єктів інфраструктури і

використання засобів ведення кібернетичної війни, тобто атаки проти комп'ютерів та даних, комп'ютерних мереж і систем, які залежать від комп'ютерів. Оскільки у більшості випадків ресурси, які необхідні для здійснення масивних кібератак, знаходяться в руках у держави, часто в науковій літературі використовується термін «кібервійна». Також часто вживається термін «мережева війна», який означає використання інформаційних засобів у військових цілях з метою унеможливлення доступу ворога до його власних комп'ютерів та мереж. Певна частина досліджень також присвячена аналізу правових засад боротьби з кібершпигунством, кібертероризмом і кіберзлочинністю у широкому сенсі.

Між тим, однією з основних проблем у науковій літературі з питань кібербезпеки в публічному секторі є невідповідність кількості досліджень, присвячених характеру кібератак, а також захисту від них, і наукових праць, пов'язаних з питаннями їх виявлення та запобігання.

Так, зокрема, контент-аналіз існуючих наукових досліджень, присвячених технічним аспектам протидії кіберзазгрозам, виявив концентрацію уваги дослідників на засобах «оборони», таких, як: шифрування, переміщення порту, проксі-сервіси, зменшення кількості інформації, антивірусні системи, програмне забезпечення захисту від шкідливих програм, системи виявлення втручань, сильні паролі, захист апаратного забезпечення, моніторинг трафіку, файлів, діяльності співробітників, обмеження фізичного доступу, захист баз даних, резервне копіювання, радіоелектронна протидія, резервування/підвищення резервної області SSD, відключення критичних систем від мережі, радіоелектронна протидія.

Порівняно з цим «наступальні» засоби, спрямовані на попередження загроз (системи запобігання втручань, сканування соцмереж, портів і адрес, фішинг/фармінг, публічні експлойти, експлойти «нульового дня», кейлоггінг/перехоплення даних з екрану, аналіз/перехоплення пакетів, ексфільтрація аналогів, ексфільтрація мережі, маршрутизація проксі,

віртуальні приватні мережі (VPN), індивідуальні шкідливі програми, відмова в обслуговуванні (DOS), пошкодження системи/бази даних та ін.), майже не досліджуються. Однак, швидкість, з якою еволюціонують загрози, ускладнює процес боротьби з ними.

Між тим, одним з потенційних рішень може стати розробка засобів, які забезпечують доступ до інформації про осіб, які можуть становити загрозу національній безпеці, та її аналіз. Поява таких засобів дозволить створити систему ретельного моніторингу кібератак і водночас забезпечить тісний зв'язок із нормативно-законодавчою сферою для подолання етичних або юридичних складнощів. Щоправда, слід визнати, що такий превентивний підхід не повинен обмежувати приватні права та втручатися у сферу життя приватних осіб та організацій.

Ще один виклик для національних урядів – обмежена кількість ресурсів. З одного боку, варто визнати, що витрати на кібербезпеку у національних бюджетах щороку зростають. З іншого боку – кібербезпека коштує достатньо дорого, а враховуючи, що наразі бюджети на національну оборону підлягають безперервному перегляду, можливості для гідного протистояння кіберзагрозам постійно зменшуються. Таким чином, обґрунтування виділення ресурсів на кібербезпеку, що зазвичай сприймається більшістю науковців та політиків як боротьба з гіпотетичною загрозою, (враховуючи обмежену кількість точних даних про конкретні результати інвестицій у цю сферу) – представляється достатньо складним завданням. Ускладнює ситуацію і те, що зазвичай через недостатню прозорість уряди і приватні компанії не бажають розкривати всю інформацію про атаки на їх активи. Таким чином, спільна проблема публічного та приватного секторів полягає у пошуку інвестицій, необхідних для покращення стандартів безпеки. Згідно з опитуванням, проведеним «Ponemon Institute», щоб досягнути максимального рівня інформаційної безпеки (тобто здатності захиститися від 95% атак), національним урядам необхідно вдев'ятеро збільшити витрати на кібербезпеку: з 5,3 млрд доларів до 46,6

млрд [450].

У звіті Американського центру стратегічних та міжнародних досліджень витрати на боротьбу з кіберзлочинністю вивчаються в контексті міжнародної економіки; в ньому зазначено, що вони складають всього 0,4-1,4% світового ВВП. Вони на порядок менше витрат на боротьбу з наркоторгівлею, що складає щорічно близько 600 мільярдів доларів (або близько 5 % світового ВВП). Навіть незважаючи на те, що опосередковані витрати (тобто пряме порушення роботи та виконання платіжних транзакцій, крадіжки службових даних, зокрема, таких, як комерційна таємниця і інформація кредитних карт, юридична відповідальність та довготривала шкода для бренду) призводять до поступового збільшення цього проценту, виправдання додаткових витрат на кібербезпеку може виявитися складним завданням. Також існує проблема з потенційними витратами, які викликані суперечливими новими стандартами і нормативними інструментами, що діють для компаній. Надмірно суворі правила, які створюють додаткові перешкоди для Інтернет-індустрії, можуть негативно вплинути на економіку та компанії, які відіграють важливу роль у науково-технічному прогресі та розробці нових технологій.

У цьому контексті безпека ланцюжків постачання та зменшення загрози внутрішніх вразливостей для кібератак є основними проблемами для забезпечення кібербезпеки в публічному секторі.

Таким чином, дослідникам належить вирішити кілька пов’язаних завдань, пов’язаних із підвищенням рівня кібербезпеки та збільшенням рівня профілактики глобальних кіберзагроз в публічному секторі в умовах обмеження ресурсів, необхідності дотримання прав та свобод громадян і забезпечення національного суверенітету окремих країн.

Додаткову складність створює ситуація, за якої дуже важко визначити потенційного ворога або носія загрози. Оскільки ворог – це не держава з визначеними характеристиками, а розсіяна по всьому світу мережа недержавних акторів, які діють у віртуальному просторі. У ситуації, коли

уряд повинен забезпечувати щоденне функціонування державних інститутів, в тому числі, діяльність правоохоронних органів, армії, надання базових послуг (тобто охорона здоров'я, громадський порядок, безпека тощо), виконання деяких функцій щодо забезпечення кібербезпеки у багатьох країнах перекладається на інших акторів (тобто компанії, Інтернет-провайдери та громадяни), що певною мірою обмежує їх здатність повністю контролювати ризики у кіберпросторі.

Додаткові складнощі полягають ще у тому, що дискусія про майбутнє кібербезпеки пов'язана з безперервною дискусією про майбутнє Інтернету загалом і необхідності дотримання балансу між безпекою та громадянськими свободами і демократичними стандартами. Держави вже не є єдиними акторами у цій дискусії: низка міжнародних організацій перехоплюють на себе управління кіберпростором і намагаються впливати на задіяні політичні процеси. Вони приєднуються до такого середовища, яке саме по собі є доволі складним і складається з багатьох традиційних суб'єктів, таких як Робоча група інженерів Інтернету, Інтернет-корпорація по наданню імен та доменів, Консорціум Всесвітньої мережі (W3C) та інших. В цьому контексті розвиток управлінських структур, які об'єднують старих і нових акторів, став справжнім викликом, особливо у сферах, в яких у них немає спільних інтересів, цілей і правового забезпечення. Незважаючи на ці перешкоди, спільною задачею всіх зацікавлених осіб є створення цілісної та ефективної системи кібербезпеки, яка забезпечить належний розвиток для економіки та національних держав. Така система повинна охоплювати багато аспектів, в тому числі організаційні структури, урядовий нагляд, громадські і державні об'єднання, міжнародну співпрацю та ін.

Між тим, така система поки що створена. У той час не можна сказати, що уряди національних країн не докладають зусиль у цьому напрямку. Так, багато країн працюють над покращенням координації взаємодії у даних питаннях. Так, наприклад, США та Китай запровадили практику постійних двосторонніх діалогів з даної проблематики: офіційні зустрічі на високому

рівні та досить неформальні діалоги між ключовими неофіційними групами [395]. Основною метою формальних та неформальних зустрічей є підвищення рівня довіри, знаходження спільної мови та обмін думками. Однак питання підходящої моделі дипломатичної співпраці досі залишається відкритим, а паралелі зі структурами контролю озброєння або охорони здоров'я досі перебувають у стані розгляду.

Однією з найбільших проблем у міжнародних відносинах з питань кібербезпеки є визначення «червоної лінії» – події у кіберпросторі, яка може погіршити дипломатичні відносини або навіть призвести до військового удару у відповідь.

При цьому деякі дослідники передбачили можливість появи несприятливого ефекту від традиційних заходів, які спрямовані на протидії імовірним кіберзагрозам. Наприклад, жорстка політика фізичної безпеки (безпека кордонів, обмеження пересування тощо) можуть призвести до того, що у своїй тактиці терористи перейдуть від традиційних терактів (з використанням вибухівки) до кібератак, які не підвладні аналогічним фізичним обмеженням. Ефект збільшення дрібних кібератак також вважається важливим ризиком в контексті ескалації [251].

Інша гостра проблема – це відсутність загальної нормативно-правової бази, яка стосується кібербезпеки та кібернападу. Наразі не існує універсальної нормативно-правової бази, яка принципово визначає, чи є кібератаки військовими діями. Традиційне поняття війни, зафіксоване у Міжнародному праві, є недостатньо точним з точки зору сучасних реалій, в яких кібератаки можуть наносити більше шкоди супротивнику ніж військові дії. При цьому такі атаки зазвичай проводяться з невідомих адрес, що ускладнює їх відслідковування та встановлення суб'єктів відповідальності. Враховуючи взаємопов'язаність військових та громадянських мереж, стає очевидним, що кіберзагрози можуть стати не тільки державною, а й соціальною проблемою. Саме тому стратегія США по боротьбі з кіберзлочинністю, оголошена Пентагоном у 2011 р., визначила

комп’ютерний саботаж з іншої країни як «військові дії», на які США може відповідати із застосуванням традиційної військової сили [338]. Стратегія США також передбачає координацію доктрини кібервійни разом з політикою безпеки, яку проводять інші актори, найвідоміших з яких є Об’єднаний центр передових технологій з кібероборони НАТО [там само].

Відзначимо, що кібербезпека вже давно була на повістці дня у НАТО і стала особливо важливою після атаки на Естонію у 2007 р. Як наслідок, упродовж останніх років НАТО зробила великий крок вперед у сфері кібербезпеки і створила низку органів, які займаються кібербезпекою. У стратегічній рамковій програмі НАТО викладено заходи організації для підвищення стійкості до зовнішніх факторів та зміцнення національних стандартів кібербезпеки, пропонуючи добровільні послуги своїм країнам-членам [393]. Так, зокрема, учасники Празького саміту 2002 р. вирішили розширити механізми кібербезпеки і створили основу для ініціатив з кібербезпеки в межах НАТО відому як Агентство з обслуговування комунікаційних та інформаційних систем («перша лінія оборони» НАТО від кібертероризму) і Технічний центр інформаційної безпеки, відповідальний за комунікаційну та комп’ютерну безпеку. Зокрема, Управління нових викликів безпеці займається координацією політико-стратегічного огляду оборонних заходів організації. Об’єднаний центр передових технологій з кібероборони НАТО було засновано у якості центру для створення експертних знань, наукових досліджень і розробок. Після Бухарестського саміту у 2008 р. з метою об’єднання основних органів НАТО, задіяних у сфері кібербезпеки, було створено Орган управління кібербезпекою. Багатоярусний підхід організації свідчить про гнучкий підхід до поняття кібербезпеки (майже як у США) замість прийняття виклику з фіксованим набором правил і інструкцій [там само].

Між тим, в останніх наукових дослідженнях було визначено вісім ключових інновацій, які окреслюють майбутні ризики та загрози в сфері кібербезпеки:

– хмарне середовище;

– великі дані,

– мобільний Інтернет,

– нейронний інтерфейс,

– безконтактні платежі,

– мобільні роботи,

– квантові обчислення ;

– мілітаризація кіберпростору [304].

Зокрема, хмарне середовище і великі дані вказано у якості основних джерел ризику. Надмірне використання мобільних пристроїв та безпровідних технологій створює нові складнощі і нові потенційні вразливості для публічного сектору. Причинами типових загроз, пов'язаних з кібербезпекою, є встановлення шкідливих програм або так звані розподілені атаки на відмову в обслуговуванні, які призводять до того, що комп'ютер або мережі стають недоступними або виходять з ладу. Цей аспект особливо важливий для країн, де так зване функціонування електронного уряду досить розвинене, а атака перешкоджає його ефективній роботі (як було після кібератак в Естонії).

Саме тому у 2010-х рр. акцент дискусій щодо політики національної безпеки зміщується в бік захисту таких фізичних активів, як глибоководні кабелі, супутники та інші комунікації, а не лише традиційних ключових об'єктів інфраструктури (мостів, електростанцій тощо).

При цьому міжнародне співтовариство протягом останніх років створило неабиякий потенціал щодо боротьби з кіберзлочинністю та кібертероризмом.

Так, зокрема, ООН запропонувала найбільш узагальнену схему дослідження кібербезпеки, яку зосереджено на двох ключових аспектах:

– кібербезпека та тероризм (в основному ці питання належать до сфери повноважень Комітету з боротьби з тероризмом Ради Безпеки ООН);

– кібербезпека як соціально-культурне явище.

ОЕСР відіграє допоміжну роль у розробці інструкцій, визначенні передових практик і допомозі у розробці політики кібербезпеки. У правоохоронній сфері Інтерпол відіграє все більшу роль у заохоченні обміну інформацією, навчальних курсів і координації міжнародних операцій [434]. Також він надає допомогу країнам-учасницям у випадку кібератак, надає підтримку у слідчих діях, розробляє стратегічні партнерства разом з іншими міжнародними організаціями і акторами з приватного сектору, а також виявляє нові загрози. У Європейському Союзі виконавча відповідальність закріплена за Європолом і недавно створеному Європейському центрі кіберзлочинності (ЄС3).

Деякі інші міжнародні організації створили свої робочі групи по кібербезпеці з метою зміцнення своїх інформаційних можливостей, хоч ці спроби є нерівномірними.

Метою підгрупи з боротьби зі злочинами в області високих технологій у «Великій сімці» є запобігання, розслідування та притягнення до відповідальності за кіберзлочини та злочини в сфері технологій. Недавно їх новим обов'язком стала боротьба з тероризмом. Група є організатором контактної мережі і директорій захисту ключової інформаційної інфраструктури для сприяння реагування та підтримки у випадку надзвичайних ситуацій [243].

Модель кібербезпеки Африканського Союзу досі перебуває на ранній стадії розвитку. Щоправда, останнім часом цей процес активізувався, особливо під керівництвом ООН. У 2009 р. Надзвичайна конференція міністрів Африканського Союзу з питань комунікаційних та інформаційних технологій визнала необхідність посилювати кібербезпеку [405]. Враховуючи обмежені ресурси деяких країн-учасниць, на конференції було сформовано прохання до Комісії Африканського Союзу про розробку конвенції про законодавство у сфері інформаційних технологій спільно з Економічною комісією ООН для Африки. Таким чином, економічна комісія ООН для Африки розглядає питання кібербезпеки в межах Ініціативи зі створення

африканського інформаційного суспільства спільно з Африканським Союзом. Метою спільних зусиль є створити стандартну нормативно-правову базу в сфері кіберзлочинності, визначити ключові терміни і розробити загальні принципи міжнародної співпраці. Більш того, буде впроваджено стандарти захисту персональних даних, електронних транзакцій і сертифікації.

Проте, незважаючи на численні спроби створити дійову міжнародну системи щодо боротьби із кіберзлочинністю, й досі залишилося вирішити декілька проблем.

По-перше, у кожній країні застосовуються закриті підходи, коли різні державні служби на національному рівні не діляться інформацією з приводу конкретної загрози з іншими країнами. З метою забезпечення захисту ключових об'єктів інфраструктури та кібербезпеки, міжурядовим організаціям необхідно ділитися знаннями, досягати взаємодії та отримувати вичерпний аналіз існуючих ризиків та шляхів їх вирішення. Також не слід нехтувати програмами місцевого та регіонального рівня.

Безумовно, за останні роки, для того, щоб об'єднати зусилля різних національних органів, які займаються кібербезпекою, було засновано деякі міжнародні організації, створені робочі групи. Між тим, їх поки що важко назвати ефективними.

По-друге, міждержавні об'єднання відіграють важливу роль в процесі узгодження зусиль державних та приватних акторів принаймні у двох сферах - стратегічні наукові дослідження та розробка і управління міжнародним співробітництвом. Ці партнерства допоможуть інтегрувати стратегічний рівень формування політики і тактичний/індивідуальний рівень управління технологіями. Однак швидке розповсюдження суспільно-державних об'єднань у сфері кібербезпеки також може призвести до непотрібного дублювання вжитих заходів і плутанини в обміні інформації по кібербезпеці. Відкритим залишається питання, якій моделі міжнародної співпраці необхідно віддавати перевагу у майбутньому.

По-третє невирішеною є проблема у створенні системи безперервного професійного навчання і освіти у сфері інформаційних технологій для органів державної і місцевої влади, а також для великих приватних компаній. Основною вимогою до такою системи є зміцнення освітніх можливостей у сфері інформаційних технологій не лише в школах та університетах, а й впродовж всього життя. Відділи кадрів повинні включити інформаційну компетенцію у план підбору персоналу і організувати навчання у площині кібербезпеки. Зокрема, вище керівництво повинно демонструвати важливість кібербезпеки як у публічному, так і у приватному секторі. У більшості випадків існуючі інформаційні технології в першу чергу розроблялися з метою забезпечення ефективності, а не безпеки.

Таким чином, в результаті швидкого огляду існуючих досліджень і політики протидії кіберзагрозам можна зробити висновок про відсутність міжнародної системи протидії кіберзагрозам, яка б включала всіх зацікавлених сторін: державних управлінців, компаній, дослідників або відповідних міжнародних суб’єктів. В результаті знання про кібербезпеку і майбутнє кіберпростору залишаються досить розсіяними. Зазначене обумовлює потребу у більш комплексному підході до кібербезпеки, який буде виходити за межі існуючих інституційних або понятійних меж. Це єдиний підхід, який може використовуватися у розробці більш стратегічного процесу формування політики і дозволятиме державам не тільки відставати від рівня кіберзагроз, які швидко еволюціонують, а й випереджати їх.

2.2. Основні підходи до забезпечення кібербезпеки у публічному секторі

Кіберзагрози здійснили революцію в розумінні людьми безпеки, а також правил та методів підтримання національної безпеки [474]. Сьогодні кібербезпека все частіше розглядається як питання національного масштабу, що стосується усіх рівнів суспільства [321]. Відповідно, підтримання безпеки

кіберпростору стало невід'ємною частиною державних стратегій національної безпеки багатьох країн світу. Різні країни мають свої визначення кіберзагроз, але майже всі погоджуються з тим, що загрози і ризики для кіберпростору повинні належним чином представлені у стратегіях національної безпеки.

Часто через низький рівень усвідомлення наявних проблем трапляються випадки тероризму, який також може мати значний вплив на стан кібербезпеки держави. Як заявляють Салієч та ін. у сучасних умовах тероризм набирає нових форм та нового змісту [456]. При цьому вони зазначають, що держави, що розвиваються, повинні краще співпрацювати з метою боротьби із сучасними формами злочинності [там само].

У відповідь на наявні загрози держави у всьому світі розробляють стратегії кібербезпеки, зазвичай – шляхом створення певного національного правого акту або програми для реагування на кіберзагрози та захисту найважливіших мереж [498]. Однак пріоритети стратегій національної безпеки різних держав відрізняються. Деякі держави мають чітке уявлення про кіберсередовище та його головні референтні об'єкти, такі як критична інфраструктура, і, відповідно, сформували комплексний підхід до сприйняття проблем, що становлять загрозу для кібербезпеки та національної безпеки, та визначили найважливіші джерела цих загроз. Унаслідок цього, ключовою умовою для реалізації ефективних стратегій кібербезпеки у цих країнах є призначення державних відомств відповідальними за управління кібербезпекою. З іншого боку, держави, в яких переважає цивільний підхід до кібербезпеки, зосереджуються переважно на боротьбі з кіберзлочинністю. Потенційні джерела загроз кіберзлочинності не визначені чітко і пов'язані, переважно, з приватною власністю і належним функціонуванням сектору економіки.

Причини використання різних підходів до питання кібербезпеки можна пояснити з теоретичної точки зору. Так, зокрема, сьогодні існує багато конкуруючих доктрин для розгляду питань кібербезпеки.

Першою є так звана *державницька (військова) парадигма національної безпеки*, яка відображає традиційну роль держави в захисті кордонів та забезпеченні верховенства права [424]. Харкнетт і Стівер висловлюють думку, що питання кібербезпеки є унікальним і багатогранним, а її забезпечення вимагає зі сторони держави підтримання безпеки кібердіяльності на публічному, приватному та економічному рівнях [346]. У межах цієї парадигми кібербезпека вважається фундаментальним фактором воєнної та економічної безпеки держави, і тому до неї застосовуються традиційні аргументи національної безпеки, що базуються на захисті батьківщини. Інакше кажучи, цей підхід підкреслює зв'язок між захистом критичної інфраструктури і тих державних та приватних систем, що є важливими для функціонування держави. Державницька парадигма національної безпеки відноситься до традиційного підходу до управління та запобігання ризикам з кіберпростору у спосіб, що може спричинити зростання впливу військових сил у сфері стратегій кібербезпеки [301]. Таким чином, концепцію мілітаризації кіберпростору можна проаналізувати крізь призму державницької парадигми національної безпеки.

Другою є *економічна парадигма*, яка відображає зростання впливу інтернету на економічний добробут держави [424]. Тим часом як державницька парадигма національної безпеки виключає з процесів формування стратегій кіберпростору усі сектори, крім військового, економічна парадигма наголошує на важливості участі інших секторів та відомств у процесі формування стратегій кібербезпеки. За Мур [419], економічна парадигма передбачає дві необхідні умови для реалізації стратегії національної кібербезпеки:

1) інтернет-провайдери повинні бути відповідальними за видалення комп'ютерів, уражених шкідливим програмним забезпеченням, з їхніх систем;

2) компанії та інші агенції повинні мати зобов'язання виявляти витоки інформації та втручання в систему.

Економічна парадигма наголошує на децентралізованому підході в групах відомств та суб'єктів, відповідальних за управління кібербезпекою. Згідно з цим підходом тягар вжиття заходів щодо захисту систем розподіляється між окремими особами, надавачами послуг (провайдерами) та керівництвом держави.

Обидві парадигми – державницька та економічна – пропонують основи для теоретичного аналізу процесу створення і реалізації стратегій кібербезпеки. Між тим, на практиці, обидва підходи доповнюють один одного і не існують у «чистому вигляді». У цьому можна пересвідчитися на результатах кваліативного дослідження чотирьох держав Вишеградської групи (Польща, Чехія, Словаччина і Угорщина) і трьох Балтійських держав (Литва, Латвія і Естонія). Під час порівняльного аналізу буде поставлене дві основні задачі:

1) дослідити як співвідносяться державницька та економічна парадигма з реальним процесом реалізації стратегій кібербезпеки;

2) визначити основні відмінності в діяльності держав в кіберпросторі.

Але перед аналізом сучасних практик звернемо увагу на те, що ще на початку 1990-х років теоретики у сфері національної безпеки, серед яких представники Копенгагенської школи Б.Бузан, О.Вівер і Дж. Вільде, не вбачали у кібербезпеці важливого питання. Однак, в результаті зростання залежності суспільств від цифрових мереж, вони звернули увагу на зростання значущості кіберзагроз і розробили теорію сек'юритизації (securitizationtheory), Згідно з цією теорію, проблема кіберзагроз набуває міжнародного масштабу і повинна стати об'єктом невідкладної уваги політиків усього світу за допомогою проголошення її значущості і реалізації надзвичайних заходів для ідентифікації та профілактики імовірних загроз. Ідентифікована загроза, на їх думку, повинна бути обов'язково десекьюритизована (desecuritization).

У 2000-х роках ця теорія отримала міжнародне визнання, про що свідчить наголошування на важливості десекьюритизації під час аналізу

стратегій розвитку багатьох країн світу [399]. Тому важливо проаналізувати як держави усвідомлюють ризики від кібератак і як розробляють відповідний план дій для протистояння загрозам.

Першим пунктом, як зазначають представники Копенгагенської школи, є *інституціоналізація* процесу секьюритизації, що передбачає визначення суб‘єктів відповідальності за цю сферу та наділення їх відповідними повноваженнями.

Згідно з твердженням Бузана, безпека повинна, певною мірою, бути інституціолізованою, і тому «деякі суб’єкти займають позицію при владі і мають повноваження проводити державну політику у сфері безпеки» [263]. Таким чином, державна стратегія кібербезпеки є ідеальним засобом для мобілізації та, імовірно, легітимізації процесу сек’юритизації. Стратегія відображає офіційну позицію керівництва в питанні, яке розглядається як проблема, і пропонує рішення, що базується на технічних знаннях та дослідженнях. З цього погляду стратегії кібербезпеки відображають в стратегічних документах (таких як стратегія національної безпеки і стратегія кібербезпеки) процеси визначення кіберпростору як сфери, що потребує реалізації відповідних заходів безпеки.

З урахуванням цього використовуються як державна, так і так і економічна парадигма до кібербезпеки. Так, в державах з державницьким підходом референтним об’єктом є критична інфраструктура та державні цифрові ресурси. Країни, що реалізують такий підхід, зазвичай є технологічно просунутими, мають потужну економіку і значною мірою покладаються на кіберпростір. З цією залежністю пов’язані вразливість і підтримання безпеки критичної кіберінфраструктури, що вважається основною умовою підтримання національної безпеки. На противагу цим країнам, держави з економічним підходом не мають конкретного референтного об’єкта. У цих країнах вважається, що кіберзловмисники намагаються одразу отримати фінансову вигоду або заволодіти секретною чи провокативною інформацією. Оскільки кіберзагрози тісно пов’язані зі

злочинними діями, основним референтним об'єктом можуть бути як персональні дані, так і інформація щодо функціонування інформаційного, економічного, соціального та інших секторів.

Наступний пункт, на який звертає увагу Копенгагенська школа, полягає в тому, що концепція безпеки охоплює не лише воєнний, але також політичний, економічний та соціальний аспекти. Відповідно, важливим стає *усвідомлення загроз*. При цьому держави з державницькою парадигмою через їхню високу залежність від критичної інфраструктури вважають питання кібербезпеки одним із аспектів національної безпеки та вносять питання ведення кібервійни до військового планування та організації. З цього погляду держави з економічним підходом розглядають конкретні проблеми кібербезпеки як ризики для безпеки лише конкретного сектору, фінансового, соціального або приватного.

Відповідно до даних Копенгагенської школи, дискурс безпеки полягає у *визначенні головного джерела загрози.* Хоч архітектура кіберпростору ускладнює процес визначення ініціатора кібератаки, державницький підхід зазвичай вважає джерелами загроз іноземні держави, а цивільний підхід звертає увагу на та шахрайські недержавні суб'єкти, хакерів тощо. Відповідно, держави з економічним підходом з меншою ймовірністю передбачать зовнішні загрози для кібербезпеки. Найбільшу загрозу в державах з економічним підходом становлять суб'єкти, що викрадають персональні дані з метою шантажу – злочину, що у взаємопов'язаному світі кіберпростору може бути вчинений стосовно будь-кого.

Наступним етапом процесу сек'юритизації є прийняття та легітимізація *надзвичайних заходів,* запропонованих суб'єктом сек'юритизації. Тому за такою логікою активна участь військових структур в процесі розробки та реалізації стратегії кібербезпеки може розглядатись як надзвичайний захід, до якого вдаються держави, що практикують державницький підхід. Так звана мілітаризація кіберпростору пов'язана зі зростанням тиску на владу з метою створення можливості ведення воєн у цій сфері та перемоги в них

[292]. Отже, мілітаризацію кіберпростору слід вважати результатом процесу сек'юритизації. Якщо кіберпростір розглядається як джерело загроз для національної безпеки, уряди укріплюють свій потенціал для ведення наступальної боротьби з цими загрозами. Водночас держави з економічним підходом з більшою ймовірністю реагуватимуть на загрози для кібербезпеки, використовуючи для цього громадський потенціал, структури та інструменти, оскільки питання кібербезпеки в кінцевому підсумку є компетенцією міністерств внутрішніх справ та цивільних відомств (економіки, цифрової трансформації тощо).

Порівняння державницького та економічного підходів в процесі реалізації державної політики щодо боротьби з кіберзагрозами представлені в табл. 2.1.

Таблиця 2.1.

Порівняння особливостей застосування державницького та економічного підходів в процесі реалізації державної політики щодо боротьби з кіберзагрозами

№	*Підходи*	*Економічний підхід*	*Державницький підхід*
1	Сприйняття кіберзагроз	Приватна безпека, інформаційно-комунікаційні технології (ІКТ)	Критична інфраструктура, ІКТ
2	Джерела кіберзагроз	Злочинці, недержавні суб'єкти, кіберзлочинці, хакери	Іноземні держави, шантажисти, терористи
3	Відомства, відповідальні за управління кібербезпекою	Міністерства внутрішніх справ, цивільні відомства та ін.	Міністерства оборони, інші військові відомства

Нижче узагальнимо практики боротьби з кіберзагрозами у різних

країнах світу.

Естонія.

Стратегічні документи Естонії щодо кібербезпеки та її організаційні структури з управління кібербезпекою сприяли формуванню зрілої і всеосяжної культури і стратегії кібербезпеки. В Естонії стратегічне планування знаходиться на першому місці, забезпечуючи єдність усієї системи кібербезпеки. Відповідаючи на серію масштабних хакерських атак в 2007 р., в 2008 р. Естонія стала однією з перших країн світу, що прийняла стратегію національної кібербезпеки. Хакерський випадок, з яким Естонія стикнулась в 2007 р., вважається першою кібервійною і політично-вмотивованим нападом на цифрову інфраструктуру держави за своєю суттю. Після цієї «Першої кібервійни» в Міністерстві оборони Естонії розробили план стратегії національної кібербезпеки. Також було опубліковано і запущено План дій у сфері цифрових технологій до 2020 р. з метою створення середовища, сприятливого для застосування ІКТ та розвитку ефективних рішень.

На сьогодні Естонія володіє найширшим спектром відомчих стратегій у сфері кібербезпеки серед Балтійських країн. В 2011 р. відповідальність за координування політики Естонії у сфері кібербезпеки була передана від Міністерства оборони Міністерству економіки та зв'язку. Як міжвідомчий орган, Рада з питань кібербезпеки при Комітеті Уряду Естонії з питань безпеки підтримує стратегічну міжвідомчу співпрацю і здійснює нагляд за реалізацією цілей стратегії національної кібербезпеки. Міністерство оборони є координуючим органом у питаннях кібероборони у сфері національної безпеки. Додатково, крім Міністерства оборони підтриманням національної кібероборони займається Підрозділ кібероборони у складі Ліги оборони Естонії, до складу якого входять спеціалісти з питань кібербезпеки від державних та приватних структур. З 2008 р. на базі Збройних сил Естонії діє Об'єднаний центр передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defense Centre of Excellence) – міжнародна військова

організація, діяльність якої направлена на поліпшення можливостей кіберзахисту НАТО та держав-спонсорів.

Латвія.

У 2014 р. було прийнято Стратегію кібербезпеки Латвії на 2014-2018 рр. [498]. В ній наголошувалося на наявності істотних проблем у сфері безпеки ІКТ у кіберпросторі Латвії, а також прогнозувалося, що в майбутньому перед кібербезпекою держави може постати чимало ризиків. У межах реалізації стратегії було ухвалено Закон про безпеку інформаційних технологій, що визначав основні вимоги до безпеки держави, муніципальних організацій, надавачів публічних послуг електронної комунікації та наглядачів за критичною ІКТ-інфраструктурою. Обидва документи відображають комплексний підхід до підтримання кібербезпеки та національної безпеки Латвії з пріоритетом критичної інфраструктури і державних послуг.

Розроблена і ефективно інституціолізована стратегія кібербезпеки Латвії є майже зразковою. Її реалізацію координує Національна Рада Латвії з питань безпеки інформаційних технологій. Ця Рада є центральним національним органом для обміну інформацією та співпраці між державним і приватним секторами. При цьому Міністерство оборони координує розвиток та реалізацію безпеки інформаційних технологій та стратегій захисту кіберпростору. На додаток до цього, в країні діють і інші структури, такі як Комп'ютерна група реагування на надзвичайні ситуації (Computer emergency response team, CERT), що також реалізують стратегію кібербезпеки Латвії.

Литва.

Система управління загрозами для кібербезпеки Литви розвивалась протягом тривалого часу, починаючи від створення перших організацій з питань кібербезпеки до недавнього прийняття загального закону про кібербезпеку [262]. При цьому Литва – єдина держава Балтійського регіону, що не затвердила стратегії національної кібербезпеки. Однак литовський Сейм (парламент) затвердив стратегію національної безпеки, в якій

кібербезпека проголошується пріоритетом національних інтересів. Для підтримання безпеки кіберпростору держави, уряд Литви затвердив Програму розвитку безпеки у сфері електронної інформації на 2011-2019 рр. Програма має три основні цілі:

1) укріплення безпеки державних інформаційних ресурсів;

2) забезпечення ефективного функціонування критичної інформаційної інфраструктури;

3) підтримання кібербезпеки громадян і жителів Литви, а також осіб, що перебувають в Литві [262].

Ці цілі були перенесені і далі розвинені в Законі Литви про кібербезпеку, що був затверджений в 2014 р. Серед важливих наслідків цього закону – передача функції координування стратегією національної кібербезпеки Міністерству національної оборони, створення нового оперативного Національного центру кібербезпеки, а також створення Дорадчого комітету з питань кібербезпеки, підзвітного Міністерству національної оборони.

Польща.

Польща провела багато комплексних змін в системі оборони кіберпростору та розробила власну стратегію кібербезпеки. Крім цього, кібербезпека стала невід'ємною частиною зусиль Польщі у сфері національної безпеки і часто згадується в інших національних стратегічних документах.

Питання кібербезпеки в стратегічних документах Польщі було вперше згадано в Стратегії національної безпеки Республіки Польща в 2007 р. Документ визначав прямий зв'язок між кібербезпекою та здатністю держави до належного функціонування. Пізніше, у Стратегії розвитку системи національної оборони Республіки Польща на 2011-2022 рр. було детально описано і розроблено питання, пов'язані з захистом кіберпростору Польщі [498]. Однак перший документ, присвячений виключно питанням кібербезпеки – Стратегія захисту кіберпростору – був виданий лише в

2013 р.. В 2015 р. Бюро національної безпеки Польщі (Biuro Bezpieczeństwa Narodowego, BBN) опубліковало доктрину кібербезпеки. Документ описує завдання, які необхідно завершити для покращення стану національної кібербезпеки. Доктрина також описує завдання державних органів, зокрема органів безпеки, збройних сил, приватного сектору та недержавних організацій у цій сфері [474]. Бюро національної безпеки, як головний орган, разом з Міністерством адміністрації і цифризації, Агентством внутрішньої безпеки та Комп'ютерною групою реагування на надзвичайні ситуації Польщі (Computer Emergency Response Team, CERT) є відповідальними за досягнення цілей у сфері кібербезпеки.

Чеська Республіка.

Національна стратегія інформаційної безпеки Чехії, затверджена в 2005 р., є першою спробою держави щодо регулювання кіберпростору. При цьому у 2011 р., Стратегія національної безпеки проголосила кібербезпеку одним із пріоритетів уряду, а кіберзагрози були віднесені за важливістю до рівня регіональних конфліктів, тероризму і зброї масового знищення [321]. Також у 2011 р. було затверджено стратегію кібербезпеки і план дій на 2011-2015 рр. Ця стратегія направлена, перш за все, на захист систем ІКТ та мінімізацію збитків, завданих кібератаками [там само]. У 2015 р. уряд Чехії затвердив оновлену стратегію національної кібербезпеки на 2015-2020 рр. Ця стратегія на другу половину десятиліття містила більш широкий комплекс заходів, спрямованих на досягнення якнайвищого рівня кібербезпеки.

Відповідальними за реалізацію стратегії кібербезпеки в Чеській Республіці є цивільні відомства. Загальна відповідальність за національну кібербезпеку покладається на Бюро національної безпеки. Національний центр з питань кібербезпеки у складі Бюро національної безпеки є частиною державної і міжнародної системи раннього попередження. Додатково, Міністерство внутрішніх справ просуває питання кібербезпеки на політичному рівні, тоді як Міністерство оборони займається питаннями кібербезпеки лише спільно з НАТО.

Словаччина.

Словаччина розробила правову основу для кібербезпеки, прийнявши в 2008 р. Національну стратегію інформаційної безпеки Словацької Республіки на 2009-2013 роки [456]. Проєкт стратегії був створений Міністерством фінансів – відомством, відповідальним за безпеку незасекреченої інформації державної адміністрації. У 2012 р. Словаччина розпочала реалізацію Стратегії національної кібербезпеки. До стратегії додавались план дій та звітом із завдань Національної стратегії інформаційної безпеки.

Управління національної безпеки Словаччини займається засекреченою інформацією, рештою питань займається Міністерство фінансів. Взаємну комунікацію забезпечує Комітет з питань інформаційної безпеки при Міністерстві фінансів: комітет виконує дорадчу та координаційну функції, готує стратегічні і технічні матеріали щодо інформаційної безпеки. Деякі питання вирішують Рада безпеки, Міністерство внутрішніх справ та Міністерство оборони. Таким чином, Міністерство оборони безпосередньо не займається управлінням національною кібербезпекою.

Угорщина.

У 2013 р. Угорщина прийняла стратегію національної кібербезпеки, яка чітко визначає, що захист суверенітету держави в кіберпросторі є національним інтересом. Усвідомлюючи те, що загрози та атаки із кіберпростору можуть зрости до рівня, що вимагатиме допомоги іноземних держав, Угорщина вважає, що кібербезпека має бути питанням колективної безпеки відповідно до Статті 5 установчого договору НАТО. Також варто зазначити, що кіберзагрози є пріоритетом стратегії національної безпеки Угорщини, прийнятої в 2012 р. [455].

Основним органом, відповідальним за координацію та реалізацію стратегії у сфері кіберпростору в Угорщині є Рада з питань управління національною кібербезпекою. Іншими органами, відповідальними за окремі аспекти кібербезпеки, є Управління кібербезпеки (відомство у складі Міністерства національного розвитку), Управління національної безпеки

(відомство у складі Міністерства державної адміністрації і справедливості) та Комп'ютерна група реагування на надзвичайні ситуації.

Цей огляд стратегій національної кібербезпеки семи країн демонструє, що стратегії кібербезпеки в регіоні стають комплексними і всеосяжними. Стратегії трактують кібербезпеку комплексно і охоплюють економічний, соціальний, правовий, правоохоронний, воєнний та дослідницький аспекти кібербезпеки. Деякі стратегії, як, в Словаччині або Чеській Республіці, підтримують більш гнучкий підхід та надають особливої уваги економічному та персональному (індивідуальному) аспектам стратегії кібербезпеки. Крім цього, Чеська Республіка, Словаччина та Угорщина належать до групи держав, в яких відповідальність за підтримку кібербезпеки несуть головно цивільні відомства. З цього погляду кібербезпеку цих держав можна назвати цивільно-орієнтованою. Більш активно координують та реалізують стратегії кібербезпеки військові відомства в Естонії, Литві, Латвії та Польщі.

Нижче розглянемо як відрізняються стратегії кібербезпеки різних держав залежно від визначення референтних об'єктів, сприйняття основних загроз та ризиків та визначенню їх джерел.

Визначення референтних об'єктів

Незалежно від обраного підходу, усі країни визнають, що одним з найбільш референтних об'єктів (об'єкт, що знаходиться під загрозою) є критична інфраструктура. При цьому, як зазначають Хансен і Ніссенбаум, наукові, політичні та інші дискусії про кібербезпеку йдуть навколо основних референтних об'єктів кібербезпеки [344]. Згідно з ними, ключем до розуміння потенційних масштабів кіберзагроз є розуміння і прийняття того, наскільки розвиненими та пов'язаними стали комп'ютерні системи. Мережі обслуговують критичну цифрову інфраструктуру: регулюють енергозабезпечення, фінансову діяльність, енергоспоживання і навіть структуру трафіку. Ці мережі розглядаються як колективний референтний об'єкт, що підлягає першочерговій сек'юритизації, оскільки їх пошкодження становитиме загрозу для національної безпеки будь-якої країни.

Економічний сектор також має багато референтних об’єктів, включно з побоюваннями приватного сектору щодо можливості викрадення великих сум грошей хакерами, а також власників інтелектуальної власності щодо того, що обмін файлами ставить під загрозу їхні права та прибутки. З цього погляду бере свій початок індивідуальний підхід до кібербезпеки, що наголошує на першочерговій значущості персональної (індивідуальної) безпеки. Як стверджують Хансен і Ніззенбаум, в дискурсі приватної безпеки індивід не є референтним об’єктом, але є пов’язаним з соціальними та політичними референтними об’єктами [344, с. 1163]. Інакше кажучи, захист приватності у кіберсфері повинен бути опосередкованим через колективний референтний об’єкт: чи то політико-ідеологічний, що піднімає питання щодо належного балансу між індивідом та державою, чи то національно-соціальний, що мобілізує цінності, ключові для ідентичності суспільства. Так само захист критичної інфраструктури не може зводитись лише до самої інфраструктури; наслідки краху мережі стосуються також інших референтних об’єктів: суспільства, державного устрою та економіки (прибутки). Нижче зробимо аналіз референтних об’єктів, визначених самими державами, які обрані нами як об‘єкт для аналізу.

Усі сім держав визнають зв’язок між секторами кібербезпеки та національної безпеки та те, що питання кібербезпеки – такі, як руйнування систем ІКТ або критичної інфраструктури – може зашкодити національній безпеці, вплинути на життя громадян і поставити під загрозу активи та функціонування національної економіки та державних служб. Тому у стратегічних документах усіх семи країн домінує дискурс колективної безпеки. Однак такі держави, як Естонія, Польща, Литва, Латвія та певною мірою Чеська Республіка, що демонструють високу необхідність інтенсивного захисту їхнього кіберпростору, демонструють також більш широке і чітке бачення своїх основних референтних об’єктів. Наприклад, стратегія національної безпеки Литви наголошує на важливості підтримання безпеки інформаційної, економічної та соціальної інфраструктур як на

основних завданнях стратегії національної безпеки. Водночас стратегія національної кібербезпеки Чеської Республіки наголошує на захисті інформаційної інфраструктури, що є важливою для економічних та соціальних інтересів держави; вона також звертає увагу на важливість захисту прав інтернет-користувачів. Однак стратегія національної безпеки Чеської Республіки має більш всеохоплюючу концепцію критичної інфраструктури та її вразливостей, що походять з кіберпростору, ніж стратегія національної кібербезпеки. У документі з національної безпеки вказано, що критична інфраструктура загалом має велику кількість загроз натурального, технологічного та асиметричного характеру. Серед таких: кібератаки, економічна злочинність та диверсії. Інакше кажучи, держави, які намагаються підтримувати високий рівень безпеки свого кіберпростору, схильні пріоретизувати питання безпеки елементів критичної інфраструктури як ключової умови національної безпеки.

Оскільки національна безпека пов’язана з критичною інфраструктурою як референтним об’єктом, суб’єкти, які мають право визначати об’єкти, що потребують захисту та оборони, можуть претендувати на право застосування надзвичайних заходів. Наприклад, доктрина кібербезпеки Польщі наголошує на важливості критичної інфраструктури та прямому зв’язку між кібербезпекою та належним функціонуванням держави, включно з її економічним розвитком та здатністю ефективно діяти у воєнній сфері. Крім того, Польща є єдиною країною, що прагне розвивати не лише оборонний, але також наступальний потенціал з метою стримування потенційних противників у кіберпросторі. Отже, підхід Польщі показує, що чим чіткіше сформульовано процес виявлення і захисту від кіберзагроз, тим більш мілітаризованим він стає.

З іншого боку, такі держави, як Угорщина і Словаччина також вважають критичну інфраструктуру референтним об’єктом. Однак ці країни не розглядають потенційні атаки на критичну інфраструктуру як загрозу національному існуванню, оскільки кібербезпека у цих двох країнах

вважається лише одним із декількох секторів національної безпеки. Угорщина та Словаччина фокусуються головно на інформаційній безпеці. Цілі стратегії інформаційної безпеки Словаччини зосереджені навколо захисту прав та свободи людини, покращення управління інформаційною безпекою та захисту державних ІКТ для підтримки критичної інфраструктури держави [Національна стратегія інформаційної безпеки Словацької Республіки, 2008]. Концепція референтних об'єктів стратегії кібербезпеки Угорщини залишається ще більш амбівалентною: її бракує прямих посилань до головних референтних об'єктів. В стратегії згадується лише захист національних баз (активів) даних та «операційна безпека елементів критичної інфраструктури, пов'язаних з кіберпростором». Ні Словаччина, ні Угорщина не виділяють конкретних референтних об'єктів, які повинні бути захищені першочергово в рамках кібербезпеки; внаслідок цього обидві країни мають головно економічний підхід до кібербезпеки.

Основні загрози та ризики.

При цьому відзначимо, що питання кібербезпеки зазвичай актуалізуються тоді, коли суб'єкти, такі, як керівництва інших держав або недержавні суб'єкти, шляхом шахрайства намагаються отримати доступ до фінансової, енергетичної сфери або сфери публічної безпеки, а перспектива кібератак розглядається як загроза, що потребує термінової відповіді. Сприйняття і подання кібератак у такий спосіб веде до прийняття інтенсивних заходів безпеки.

Однак загрози для кібер- та національної безпеки не виникають лише із зовнішніх джерел. Кібератаки також можуть виникати із систематичних загроз. Ці системні загрози зумовлені властивою непередбачуваністю комп'ютерів та інформаційних систем, що створюють ненавмисні (потенційно або дійсно) небезпечні ситуації для самих себе або ж для людей і фізичного середовища, до якого вони вбудовані [234]. Більш поширеною проблемою, однак, є навмисне спровокована системна загроза, яку застосовують кримінальні синдикати або окремі особи. З цього погляду

технічний дискурс супроводжується кримінальним. У цьому дискурсі кібербезпека може, простіше кажучи, розглядатися як захист комп'ютерів від кримінальних дій, а кібератаки сприймаються не як загрози для національної безпеки, а як загальні ризики у кіберпросторі. Відповідно держави, що сприймають потенційні кібератаки як ризик для конкретного сектору, менш схильні вважати питання кібербезпеки питаннями національної безпеки і можуть називатись державами з економічним підходом.

Між тим, узагальнюючи, можна зазначити, що Польща, Латвія, Литва, Естонія і Чеська Республіка мають багаторівневий підхід до кібератак. По-перше, вони оцінюють ризики для національної безпеки і дають завдання державним органам щодо запобігання кібератакам. По-друге, вони ідентифікують виклики у сфері кібератак для невід'ємних компонентів їхньої національної безпеки: економічного, фінансового та приватного секторів. Такий комплексний підхід до кібератак найбільш показова відображений в стратегії кібербезпеки Естонії.

Естонія декларує зростання кількості державних суб'єктів, що отримали доручення з протидії кібершпигунству та захисту підключених до Інтернету і закритих мереж, а також додаткову ціль – збір інформації про безпеку та економічні інтереси. Національна безпека також є домінуючим дискурсом доктрини кібербезпеки Польщі. До кіберзагроз, як вони описані в доктрині, відносяться атаки на телекомунікаційні системи, важливі для національної безпеки та протидії кіберзлочинності; до специфічних кіберзлочинів, згаданих в доктрині, відносяться «кібернасилля, деструктивні кіберпротести і кібердемонстрації», викрадення даних, зокрема особистих, а також викрадення приватних комп'ютерів. Той самий підхід міститься також в стратегічних документах Литви та Латвії. Наприклад, концепція національного захисту Литви визначає кібератаки як національну загрозу поряд із тероризмом та організованою злочинністю. Варто згадати також те, що остання концепція національної оборони Латвії називає кібератаки однією з восьми основних загроз для національної безпеки.

Згадані вище чотири країни (Естонія, Литва, Латвія, Польща) мають всеосяжний підхід до кібербезпеки, що базується на точних оцінках потенційного впливу кібератак на різні сектори та на національну безпеку загалом. Оскільки кібератаки сприймаються головно як загрози для національної безпеки, ці країни реагують на це, використовуючи державницький підхід.

Оновлена концепція кібербезпеки Словаччини на 2015-2020 рр. також представляє комплексне уявлення про кібербезпеку. Словаччина стверджує, що кібербезпека не повинна розглядатись як окрема проблема держави, або як проблема, що стосується одного чи декількох секторів, і що з огляду на свою глобальну суть, кібербезпека є загальносуспільним явищем.

Документ також описує основну проблему стратегії кібербезпеки Словаччини: кіберзагрози не розглядаються як термінова проблема. Хоча документ пропонує модель управління стратегіями кібербезпеки, в ньому немає повного бачення викликів у сфері кібербезпеки. У результаті цього потенційні кібератаки розглядаються переважно як ризики для безіменних (конкретно не визначених) цілей.

У стратегії Чеської Республіки згадуються такі ризики як кібершпигунство (промислове, воєнне, політичне або інше), організована злочинність в кіберпросторі, хактивізм, міжнародні дезінформаційні кампанії з політичними або воєнними цілями і навіть, у майбутньому, кібертероризм. Ці ризики розглядаються загалом як небезпечні тенденції глобального кіберпростору, які ще однак не торкнулися чеського суспільства. Безпековий дискурс, що домінує в стратегічних документах Чеської Республіки, переважно відноситься до систематичних загроз та «комп'ютерної безпеки». З цього погляду стратегія кібербезпеки Чеської Республіки фокусується здебільшого на побудові надійної інформаційної спільноти шляхом захисту доступу до послуг, цілісності даних і покращення конфіденційності кіберпростору Чеської Республіки. Угорщина, натомість, особливо наголошує на кримінальній складовій кібератак, стверджуючи, що

динамічний розвиток нових технологій, на кшталт хмарних обчислень та мобільного інтернету, веде до постійного виникнення нових загроз, таких як незаконне заволодіння критичною інформацією та персональними даними. Крім цього, Угорщина не ідентифікує виклики для кібербезпеки з загрозами – у державі надають перевагу називанню кіберзагроз ризиками для кіберсектору.

Отже, аналіз сприйняття кіберзагроз та кібербезпеки загалом дозволяє стверджувати про застосування економічного підходу до управління кібербезпекою, що домінує в Чеській Республіці, Словаччині та Угорщині.

Джерела кіберзагроз.

Між тим, сучасна архітектура кіберпростору забезпечує високий рівень анонімності та перешкоджає спробам відслідковування *джерел кібератак*, що є додатковим фактором небезпеки. Утім, сучасні технології дозволяють можна аналізувати джерела кібератак та кіберзловмисників, серед яких виділяють два основних: внутрішні та зовнішні. У воєнно-цивільній дихотомії зовнішні кіберзагрози, такі як іноземні держави або недержавні суб'єкти, включно з кібертерористами та суб'єктами кібершпигунства, стикаються з внутрішніми суб'єктами: хактивістами, кіберзлочинцями, авторами шкідливих програм, кібершахраями та подібними організаціями. Як згадувалось раніше, держави, що активно захищають свій кіберпростір, наголошують на політичних мотивах кібератак та зовнішніх кіберзагроз. Таке відношення розглядає державницький підхід до управління кібербезпекою як найбільш ефективний. І навпаки, фокусування переважно на внутрішніх кіберзагрозах означає те, що головним референтним об'єктом є сектор економіки або персональні дані. Економічний підхід до стратегій кібербезпеки вважається у такому разі найбільш ефективним для боротьби з такими загрозами.

Подальший аналіз того, як окремі держави розуміють джерела кіберзагроз, приводить нас до висновку про те, що усі вони визнають те, що у кіберпросторі є багато суб'єктів; однак, лише декілька держав розрізняють їх

природу, цілі та методи діяльності. Наприклад, Естонія у своїй стратегії кібербезпеки декларує, що на національну кібербезпеку впливають суб'єкти з різними навичками, цілями та мотиваціями, і що показник кібершпигунства з метою отримання інформації з секторів національної безпеки та економіки зростає. В стратегії Естонії також наголошується на зростанні кількості держав, здатних до початку кібератак. Такий розподіл внутрішніх та зовнішніх загроз наявний також у доктрині Польщі. Зовнішні загрози, перераховані в доктрині, включають кіберкризи, кіберконфлікти, кібервійни та кібершпигунство за участі держав та інших суб'єктів; «загрози (для Польщі) з кіберпростору походять від екстремістських, терористичних та міжнародних кримінальних організацій, чиї атаки у кіберпросторі можуть бути ідеологічно, політично, релігійно, бізнесово або кримінально вмотивованими».

Литва і Латвія, навпаки, не виділяють специфічні кібератаки, а їхні стратегічні документи відносяться в основному до зовнішніх загроз, таких як сусідні держави. Водночас Словаччина і Угорщина мають розмите і фрагментарне бачення джерел кіберзагроз. Угорщина фокусується на технічних (внутрішніх) вразливостях і їх впливі на належне функціонування державної економіки, не вдаючись до глибшого аналізу їхніх причин та суб'єктів цього процесу.

В стратегії кібербезпеки Угорщини стверджується, що додатково до шкоди, завданої зовнішніми факторами, ще одним ризиком є невідповідне регулювання операційної безпеки інформаційної та комунікаційної систем, що формують кіберпростір. «Динамічний розвиток нових технологій, на кшталт хмарних обчислень та мобільного інтернету, веде до постійного виникнення нових загроз для безпеки».

Цивільний підхід до джерел кіберзагроз застосовується також у Чеській Республіці. Стратегія національної кібербезпеки Чеської Республіки представляє великий перелік потенційних викликів для кіберпростору, однак майже всі вони є кримінальними або технологічними за своєю природою.

Такими вважаються хакерські атаки з метою заволодіння персональними або конфіденційною інформацією, технічні збої, ботнет-мережі, DDoS/DoS-атаки (розподілені атаки на відмову в обслуговуванні) та ін.

Сприйняття кіберзагроз тісно пов'язане з джерелами сприйнятих загроз. Переважання сек'юритизованого погляду на кіберзагрози сприяє більш точному визначенню джерела загрози. Крім того, держави, що сек'юритизують кіберзагрози, такі як Естонія, Польща, Литва та Латвія, розрізняють зовнішні та внутрішні суб'єкти кіберпростору. Водночас держави, що підкреслюють кримінальний елемент кіберзагроз, розглядають їх переважно як внутрішні виклики та обмеження для кіберпростору. Варто зазначити, що більшість представлених держав розрізняють внутрішні та зовнішні джерела кіберзагроз у своїх стратегічних документах. Однак країни з економічним підходом не зацікавлені в подальшому розвитку цього розрізнення і фокусуються здебільшого на внутрішніх джерелах загроз як на найбільш поширених та ймовірних у їхньому середовищі безпеки.

Отже, компаративний аналіз стратегій кіберзагроз чотирьох країн Вишеградської групи і трьох Балтійських країн демонструє, що кожна з них має власні стратегії кібербезпеки і відповідне законодавство для вирішення проблем кібербезпеки. Усі проаналізовані документи посилаються на стратегії національної безпеки та оборони високого рівня та представляють законодавче середовище, незважаючи на значні відмінності у їхній глибині. В документах також розглядаються різні суб'єкти кіберпростору та потенційні загрози, що походять від цих суб'єктів. В більшості національних стратегій кібербезпеки загрози для критичної інфраструктури та кіберзлочинність відіграють важливу роль і вказують на зростання шкоди для економіки, завданої кібератаками. У формальному сенсі, сфера кіберпростору вже включена до порядку денного з питань безпеки всіх держав і може бути названа «сек'юритизованою».

Однак, між сек'юритизацією цих держав є також відмінності. Кібербезпека відрізняється за тим, як держави, по-перше, визначають

референтний об’єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики. Відповідно до цих відмінностей їх можна віднести до двох категорій. Перша категорія – держави, що мілітаризують питання кібербезпеки: Польща, Естонія, Литва, і певною мірою Латвія. Ці держави більш точно визначають конкретні референтні об’єкти та називають захист цих об’єктів національним пріоритетом. Ця тенденція піднімає кібербезпеку на найвищий рівень національної безпеки та зосереджує увагу на захисті ІКТ та державних інформаційних ресурсів. Польща, Естонія і Литва схильні трактувати виклики кібербезпеки як загрозу для належного функціонування держави та вважати атаки зі сторони іноземних держав найбільшими джерелами загроз. Відповідно, відповідальність за реагування на кіберзагрози у цих державах передана воєнним та оборонним органам.

Друга категорія держав за дискурсом сек’юритизації пов’язана з криміналізацією питань кібербезпеки. Чеська Республіка, Словаччина та Угорщина покладаються на економічний підхід в управлінні кібербезпекою. Їхні референтні об’єкти відрізняються і здебільшого стосуються належного функціонування системи національної економіки та приватної власності. ІКТ та державні цифрові ресурси не мають переваги над іншими законними референтними об’єктами. Унаслідок цього держави з домінуючим економічним підходом зосереджуються на кримінальній діяльності у кіберпросторі, а проблеми кібербезпеки розглядають як «ризики». Перелік потенційних джерел таких ризиків також фрагментований і включає не лише зовнішні міжнародні суб’єкти, але також внутрішні суб’єкти – хакерів, хактивістів, кримінальні організації і навіть ненавмисні злами мереж. Цивільні відомства Чеської Республіки, Словаччини та Угорщини відповідають за відслідковування ризиків для кібербезпеки та координування відповіддю держави на виклики у цій сфері.

Таким чином, поділ підходів до кібербезпеки, може сприяти кращому розумінню кібербезпеки як явища і допомогти пояснити перешкоди для

співпраці держав, що займаються питаннями кібербезпеки на міжнародному рівні. Крім цього, визначення особливостей різних підходів до кібербезпеки може пояснити конкретні дії держав у кіберпросторі. Розуміння відмінностей в сприйнятті державами кіберзагроз, референтних об'єктів і потенційних противників становить основу для обговорення так званої кіберідентичності держав та недержавних суб'єктів. Це може бути корисним теоретичним знаряддям для аналізу потенційних кіберконфліктів та моделей співпраці в цій сфері.

2.3. Національні стратегії кібербезпеки: основні складові

Як показує аналіз, стратегії кібербезпеки більшості держав зосереджують увагу на п'яти основних сферах: 1) військові кібероперації; 2) розвідка і контррозвідка; 3) боротьба з кіберзлочинністю; 4) захист критичної інфраструктури та врегулювання кризових ситуацій; 5) кібердипломатія та управління Інтернетом. Для того, щоб краще зрозуміти сутність національних стратегій кібербезпеки стосовно зазначених сфер нижче у даному параграфі розглянемо особливості цих стратегій, розроблених у таких країнах як США, Великобританія, Німеччина, Франція, Нідерланди, Туреччина, Індія.

Військові кібероперації.

Одночасно з виникненням кіберзагроз протягом останніх десятиліть відбулись фундаментальні зміни у сприйнятті безпеки військовими силами. Зростання залежності від інтернет-технологій означає також зростання вразливості мереж і ймовірності атак, спрямованих на об'єкти критичної інфраструктури. Ці зміни змусили керівництва країн переглянути власні підходи до сприйняття загроз та механізми підтримки безпеки для боротьби з кіберзагрозами. Протягом останніх чотирьох років спостерігається тенденція з боку керівних органів до публікації стратегій кібербезпеки, котрі становлять основне джерело інформації про те, як військові сили трактують

кіберпростір і як формують стратегії кібербезпеки.

Вага, що надається воєнному підходу до кіберпростору в стратегічних документах, проаналізованих в цьому дослідженні, значно відрізняється в кожній державі. В деяких державах для вирішення головних питань, пов'язаних з кіберпростором, застосовується воєнний підхід, тоді як в деяких інших державах найбільше уваги отримують інші питання, наприклад – боротьба з кіберзлочинністю.

Можна із впевненістю сказати, що у стратегії безпеки кіберпростору *США* переважає військовий підхід, оскільки влада у Вашингтоні все частіше називає кіберзагрози проблемою національної безпеки. У Стратегії національної безпеки, опублікованій Білим домом у 2010 р., «масштабні кібератаки» вважають загрозою для США нарівні з тероризмом, стихійними лихами і пандеміями, наголошуючи на їхньому асиметричному характері. Ще одним пунктом, що демонструє сприйняття кіберзагроз розробниками стратегії в США, є внесення цифрової інфраструктури до списку стратегічних активів, що повинні бути захищеними.

«Наша цифрова інфраструктура, таким чином, є національним стратегічним активом, а її захист — так само як захист приватної та цивільної свободи — є одним із пріоритетів національної безпеки» [488, с. 27)

Широкомасштабні кібератаки – не єдиний вимір кіберзагроз. Можливості, що надає інтернет, активно використовують транснаціональні терористичні групи, для яких кіберпростір є середовищем не лише для пропаганди, вербування чи хакерства, але також для викрадання коштів, фінансування терористичних атак та отримання конфіденційної інформації про безпеку. У Стратегії звернено увагу на використання терористами кіберпростору з метою підриву глобальної довіри до міжнародних фінансових систем як на основну складову ланцюга «злочин-тероризм» [там само, с. 49]

Для більш детального вивчення воєнного підходу США до кіберпростору варто поглянути ближче на Стратегію кібербезпеки

Міністерства оборони США, частина якої була оприлюднена в 2011 р. На самому початку документу вказано, що Міністерство оборони розглядає кіберпростір як операційний простір «для організації, тренування та оснащення» [503]. З цього документа можна зробити висновок, що основною причиною воєнного підходу США до кіберпростору, згідно з яким кіберзагрози вважаються загрозами для національної безпеки, є залежність критичної інфраструктури держави від мереж. Описуючи критичну інфраструктуру США, у Міністерстві оборони виокремлюють п’ять послуг, надавачі яких є стратегічно важливими для національної безпеки: енергетика, банківська справа і фінанси, система транспортування, система комунікацій і оборонна промисловість [там само]. Важливо зазначити, що об’єкти критичної інфраструктури, визначені Міністерством оборони, контролюються переважно приватним сектором. Оскільки питання підтримки безпеки мереж, що належать приватному сектору, є темою для окремої дискусії, очевидною є необхідність створення нової структурної організації між державою та приватним сектором, що підтримуватиме хиткий баланс між безпекою і конфіденційністю з повагою до ліберальних цінностей.

Хоч в стратегічних документах США не згадується інституційна основа стратегій кібербезпеки, варто відзначити створення у 2010 р. Кіберкомандування США – спеціального підрозділу у складі Стратегічного командування Збройних сил США, що спеціалізується на протидії кіберзагрозам. Створення Кіберкомандування дало початок ще одній важливій дискусії в контексті стратегії кібербезпеки США: яку позицію займають США в контексті захисту кіберпростору – оборонну чи наступальну?

В сухопутних, військово-повітряних і військово-морських силах можна простежити більш чіткий розподіл між наступальними та оборонними силами. Однак проведення такого ж чіткого розподілу між цими сферами в кіберпросторі є більш складним завданням. Незважаючи на те, що в

документах з питань кібербезпеки основним завданням визначено оборону, існують конкретні практики, які вказують на те, що США розглядають саме «активну оборону». Ті, хто вважають, що в основі стратегії кібербезпеки повинен бути наступальний підхід, стверджують, що вища вартість забезпечення стійкості є одним з перших факторів, які повинні мотивувати керівництво держави до вибору наступальних засобів.

За словами Гілі, «кібербезпека є надзвичайно дорогою; вона передбачає величезні інвестиції фінансових і людських ресурсів для налаштування організацій, технологій та процесів (навіть базових рис людської поведінки) відповідно до процедур інформаційної безпеки» [350].

Наголошуючи на обов'язковому передбаченні наступальних заходів в стратегії кібербезпеки, Гілі вказує, що самих лише оборонних заходів недостатньо для підтримки мережевої безпеки: «Наприкінці 1990-х у Міністерстві оборони США чітко визначили оборону одним із пріоритетів, вважаючи, що традиційні військові сили здатні стримати будь-якого потенційного противника без застосування наступального потенціалу. Однак якби власні кіберсистеми Міністерства оборони зазнали вторгнення, усі ці традиційні військові сили залишились би глухими і сліпими» [там само].

У стратегічних документах США немає прямих посилань на наступальний потенціал у сфері кібербезпеки, однак на практиці число доказів свідчить про те, що Вашингтон вбачає у військових засобах для підтримки кібербезпеки ефективний стримувальний актив для досягнення зовнішньополітичних цілей. Інцидент з вірусом Stuxnet, незважаючи на відкритість питання його дипломатичної ефективності, показав, що кіберзброя може бути використана для атаки на стратегічні об'єкти. Варто також мати на увазі те, що трансформація американської воєнної стратегії після подій 11 вересня 2001 р. призвела до того, що американські лідери обирають превентивні операції, ймовірність чого є також досить високою в умовах кібервійни з ускладненою атрибуцією.

Безсумнівно, США – не єдина держава, що прагне використовувати

власний кіберпотенціал для захисту мереж шляхом здійснення наступальних заходів. *Великобританія* є ще однією державою, що висловлюється на підтримку наступальних заходів. Пріоритетом «Стратегії кібербезпеки Великобританії» [485] визначено боротьбу з кіберзлочинністю, в результаті чого країна має стати найбезпечнішим середовищем для ведення бізнесу (тобто економічно-орієнтований підхід), однак Міністерство оборони Великобританії водночас має у своєму активі наступальні кіберзасоби.

З метою покращення стану кібербезпеки у сфері воєнних поставок, Великобританія сформувала Партнерство з питань кібероборони і захисту (Defence Cyber Protection Partnership, DCPP) і продовжує зосереджуватись на найкращих практиках, усвідомленні і пропорційних стандартах. В 2015 р. було офіційно запущено модель кібербезпеки для оборони (Кабінет Міністрів Великобританії, 2014), однак її реалізація затрималась і відбулась у другому кварталі 2016 р. (Міністерство оборони Великобританії, 2016). Для ведення кібервійни було сформовано підрозділ збройних сил під назвою 77-а Бригада (77^{th} Brigade) (Міністерство оборони Великобританії, 2016).

Як вказано у звітах, одним із основних кроків Великобританії на шляху до активної кібероборони є співпраця з окремими хакерами, навіть якщо деякі з них були ув'язнені. Стверджується, що держава планує залучити таких комп'ютерних хакерів до створеного нещодавно підрозділу з питань кіберзахисту – Об'єднаної резервної групи з питань кібербезпеки (Joint Cyber Reserve Unit, JCRU), про що уряд Великобританії оголосив у вересні 2012 р. Міністерство оборони розробило ініціативу вартістю 500 млн. фунтів для набору до резерву сотень комп'ютерних експертів для забезпечення оборони держави поряд із з регулярними військовими силами. Діяльність Об'єднаної резервної групи спрямована на зміцнення національної безпеки шляхом захисту комп'ютерних мереж і критичних даних, а також на здійснення превентивних наступальних операцій в кіберпросторі [483].

У свою чергу, на думку представників *Німеччини*, кібератака – це атака на ІТ-систему держави, ціллю якої є доступність, конфіденційність та

цілісність інформаційних систем. Німеччина не згадує про воєнний потенціал у своїй стратегії, але водночас працює над завершенням створення спеціального Кіберінформаційного командування з центром кібероперацій, а також Центру з питань кібербезпеки Збройних сил Німеччини (Bundeswehr cyber-security centre) на 13800 працівників [259].

Індія ще не сформувала власне кіберкомандування, але за наказом Кабінету Міністрів (Cabinet Note) формуванням Командування керує Генерал Інтегрованого оборонного штабу (Integrated Defence Staff, IDS). Станом на сьогодні визначені агентства – Розвідувальне управління Міністерства оборони (англ. Defence Intelligence Agency, DIA) і Національна організація технічних досліджень (National Technical Research Organization, NTRO) – проводять наступальні кібероперації за потребою. У Національній організації технічних досліджень Індії згадується, що одним із компонентів її місії є реакція на кіберзагрози, однак не говориться про захист кіберкордонів шляхом активного кіберзахисту, як це вказано в документах Великобританії, США і Німеччини. США і Німеччина говорять про кібервійну, натомість Індія окрім кібервійни враховує також ризики, пов’язані з хмарними обчисленнями.

Розвідка і контррозвідка.

Збір розвідувальної інформації в кіберпросторі не вимагає втручання до іноземного територіального суверенітету шляхом відправлення агентів за кордон, агенти, як правило, залишаються у своїх країнах. Оскільки така ситуація не порушує норм міжнародного законодавства, збирання розвідувальної інформації в кіберпросторі рідко викликає занепокоєння у сфері міжнародного права. Більше того, міжнародне право не забороняє країнам шпигувати за кордоном або карати шпигунів на своїй території.

Однак, слід зазначити, що чіткого розподілу між кіберзлочином, кіберкрадіжкою і кібершпигунством досі немає. Протиріччя також спостерігається в розрізненні військової кіберактивності, кіберзлочинності і кібершпигунства. Що станеться, якщо група хакерів за певної допомоги від

держави А здійснить кібероперацію проти комп'ютерних мереж держави Б, спрямовану на заволодіння конфіденційною інформацією про військові таємниці держави Б? Чи такі дії можна вважати кіберзлочином, за котрий слід карати хакерів, військовою діяльністю чи кібершпигунством?

Не говорячи вже про невизначені сірі зони, кібершпигунство є найбільш небезпечною частиною діяльності, спрямованої проти кібербезпеки, що вражає як приватний, так і публічний сектори. Велика кількість викраденої інтелектуальної власності та пов'язані з цим проблеми спонукали багато організацій вжити додаткових заходів безпеки. Окрім організацій, особливу увагу кібершпигунству приділяють також самі держави, фіксуючи це у планах дій щодо підтримки безпеки. Викрадена інформація є не лише значною втратою в аспекті наукових досліджень і розвитку, але також чинником, що значно підриває довіру до відповідного відомства.

У кіберстратегії *США* немає конкретних згадок про кібершпигунство. Однак право власності, промислове шпигунство, а також захист конфіденційних даних, що належать сфері бізнесу і державі – ці питання розглядаються у відповідних стратегічних документах [489]. Крім цього, стратегія кібербезпеки Міністерства оборони США пов'язує діяльність по боротьбі з кібершпигунством із зусиллями по встановленню особистостей нападників і хакерів. Вирішення складних завдань атрибуції кібератак покладається на особливі підрозділи кіберрозвідки.

Міністерство оборони *Великобританії* спільно з Агентствами безпеки та розвідки і Центром урядового зв'язку (Government Communications Headquarters, GCHQ) відіграють головну роль у виявленні кіберзагроз і нівелюванні ризиків, пов'язаних з ними. Кіберстратегії також передбачають певні бюджетні асигнування, виділені для цих агентств. Так, у 2018 році на виявлення кіберзагроз було заплановано виділити 157 млн. фунтів [420].

Зменшення вразливості до кібершпигунства є одним із перших кроків, до яких вдалось керівництво *Нідерландів*. У Стратегії кібербезпеки цієї

держави зазначено, що розвиток технічного потенціалу йтиме поруч з корегуванням правових процедур в аспекті контркіберрозвідки. Стратегія також містить заклик, звернений до публічних організацій, до тісної співпраці з метою протидії кібершпигунству, особливо тому, що виникає з-за кордону [481].

У стратегії кібербезпеки *Німеччини* кібершпигунству надається такої ж ваги як в інших стратегіях. Окрема частина документу присвячена цьому питанню [259].

Національне агентство розвідки *Туреччини* (Turkey's National Intelligence Agency) широко залучене до процесу збору доказів для врегулювання інцидентів у кіберпросторі. Однак у стратегії Туреччини не вказано безпосередньо на те, як протидіяти комп'ютерному шпигунству в кіберпросторі.

В *Індії* розвідка і контррозвідка була важливим елементом геополітичної стратегії з найдавніших часів. Тому не дивно, що Індія у своїх стратегічних документах, пов'язаних з кібербезпекою, згадує про глобальну співпрацю між агентствами безпеки різних держав та проводить постійні діалоги для ефективного обміну інформацією.

Боротьба з кіберзлочинністю.

Кіберзлочинність – вид кримінальної діяльності, що здійснюється за допомогою комп'ютерів чи Інтернету [442]. Як і в багатьох інших сферах кіберпростору, тут бракує чіткого окреслення деталей, яке могло б нас задовольнити. Так, кіберзлочини можна розділити на дві основних групи. Дуже поширеними є злочини, спрямовані на заволодіння персональною інформацією головно з метою крадіжки грошей за допомогою експлойтів і проґалин в безпеці. Основна частина злочинів цієї групи зосереджена на ідентичності – крадіжки і фішинг. Зловмисники, за допомогою шкідливого програмного забезпечення, що створює копії усіх натиснень клавіш, можуть отримати паролі і втрутитись у фінансові зв'язки, створюючи проблеми не лише для індивідуальних користувачів, а й для великих компаній.

В інших сферах здійснюються більш поважні злочини – це стосується кібератак з конкретними інституційними цілями, спрямованими на затримку надання послуг державних установ. DDoS/DoS-атаки (розподілені атаки на відмову в обслуговуванні), спрямовані проти адміністраційних мереж, можуть також бути спрямованими проти відомств, що є критично важливими для підтримки повсякденного життя людей – транспортна система, енергетика, банківська сфера.

Боротьба з кіберзлочинністю є багатовимірним завданням. Цілями кіберзлочинців є різноманітні мережі – від воєнних до університетських. Кожне відомство має власні проблеми у сфері кібербезпеки, але через брак комплексного підходу в багатьох державах та транснаціональний характер кіберзлочинів, різні відомства вживають власних заходів безпеки для протидії кіберзлочинам. Втім, зі зростанням числа кіберзлочинів, що становить загрозу для національної безпеки, керівники різних публічних організацій розпочали брати участь у спільній боротьбі з кіберзлочинністю., у тому числі, на міжнародному рівні. І першим міжнародним договором стала Будапештська конвенція про кіберзлочинність (також: Конвенція про кіберзлочинність), ціллю якої є гармонізація національного законодавства, оновлення методів розслідування і розвиток міжнародної співпраці для більш ефективної протидії кіберзлочинності [285]. Крім того, боротьба з кіберзлочинністю є однією зі сфер, що має велику потребу у публічно-приватній співпраці, тому активна підтримка приватних компаній у сфері кібербезпеки зі сторони держави набуває стратегічного значення [383].

Великобританію можна справедливо назвати державою, що докладає багато зусиль для боротьби з кіберзлочинами. Середня сума збитків від кіберзлочинності для великих організацій Великобританії становить у середньому 4,1 млн. фунтів/рік [450]. Тому свого часу для підтримки безпечного бізнес-кіберсередовища керівництво Великобританії виділило 860 млн. фунтів на Національну програму кібербезпеки, яка тривала з квітня 2011 р. по березень 2016 р..

Більше того, першою і головною метою Стратегії кібербезпеки Великобританії є саме підтримка безпеки бізнесу. Для досягнення цього у документі передбачено певні законодавчі поправки, розвиток кіберпотенціалу і нарощення потенціалу правоохоронних органів [485] Також Стратегія містила три конкретних кроки для розвитку потенціалу кібербезпеки:

- запуск Національного агентства з питань кіберзлочинності – нового органу для боротьби з кіберзлочинністю;
- дотримання плану дій, затвердженого під час Лондонської конференції 2012 року з питань кібербезпеки, для впровадження схваленої міжнародною групою «дорожньої карти» стосовно користування кіберпростором;
- створення єдиної системи звітування для громадян і малого бізнесу для повідомлення про кіберзлочини, так щоб злочинну дію було зафіксовано і правоохоронні органи могли визначити масштаб кіберзлочину (включно з впливом злочину на окремих осіб, організації та економіку в цілому).

Але зрозуміло й те, що самостійна боротьба з кіберзлочинністю не принесе користі жодній державі, так само як боротьба одного солдата проти цілої армії. Гарантія цілковитої кібербезпеки в національному кіберпросторі при існуванні небезпечного глобального кіберпростору є неправдивою обіцянкою. Це схоже на обіцянки політиків будувати мости там, де не течуть річки.

Саме тому такі держави як Великобританія та США голосно і однозначно говорять про необхідність розробки плану дій для покращення глобальної співпраці і боротьби з кіберзагрозами і тероризмом. У *США* доклали величезних зусиль для створення міжнародної основи з метою відділення її від стратегій кібербезпеки для запобігання кіберзлочинам. Не зупиняючись на цьому, США також працювали і продовжують працювати над створенням правової системи для пристосування до швидких змін і видозмін кіберзлочинів. Додатково, у Стратегії кібербезпеки США

оголошено про намір вести міжнародну війну проти кіберзлочинності. До речі, загальна сума збитків, завданих американській економіці кіберзлочинами за останні десять років, становить у середньому 15 млрд. дол./рік [449].

Натомість із Стратегії кібербезпеки *Німеччини* можна побачити, що кіберзлочинність не вважається найважливішим питанням, адже боротьба з кіберзлочинністю є однією з десяти цілей, перерахованих наприкінці стратегічного документу. Німеччина прагне найняти кращих спеціалістів до правоохоронних відомств і створити сприятливу платформу для того, щоб Федеральне управління з питань інформаційної безпеки могло діяти спільно з представниками приватного сектору для отримання високих результатів для країни у боротьбі з кіберзагрозами; цим держава показує свій намір виробити ширшу національну перспективу. Одночасно ведеться боротьба з кібершпигунством і робота з використанням отриманих розвідданих. Керівництво Німеччини також виразило готовність тісно співпрацювати з міжнародними структурами, включно з Радою Європи і ООН, зокрема у сфері обміну інформацією (Федеральне міністерство внутрішніх справ Німеччини, 2011). Тому попри всі зусилля та ініціативи, можна із впевненістю сказати, що Німеччина не працює над питанням загроз кіберзлочинності як над одним із пріоритетів кіберстратегії. І це дещо дивно, оскільки Німеччина посідає другу позицію після США за збитками, завданими кіберзлочинністю – у середньому 5,950 млрд. дол./рік за останні десять років [449].

Нідерланди у своїй національній стратегії мають тенденцію до застосування правового підходу. В контексті кіберзлочинності, стратегія Нідерландів стосується головно розробки сумісних законів, вдосконалення методів розслідування і деяких додаткових аспектів для підтримки попередніх кроків. Розвиток потенціалу правоохоронних органів для боротьби із кіберзлочинністю також входить до переліку заходів, передбачених стратегічним документом [481].

Франція, надаючи меншого значення кіберзлочинності, єдиним засобом для боротьби з нею вважає посилення законодавчих заходів. Стратегія кібербезпеки Франції передбачає також міжнародну співпрацю у сфері протидії кіберзлочинності [330].

Окрім широкомасштабних заходів безпеки, описаних у стратегіях інших держав, *Туреччина* з метою стимулювання ефективних зусиль для запобігання кіберзлочинам вдається до певних специфічних дій. Так, двома головними завданнями Міністерства внутрішніх справ і Міністерства транспорту та інфраструктури є, відповідно, встановлення основних стандартів щодо збору доказів при виникненні інцидентів у сфері кібербезпеки та створення найбільш сучасної технологічної інфраструктури. Завдяки цьому керівництво Туреччини будує власну стратегію боротьби з кіберзлочинністю на основі постійного оновлення даних про інциденти. За умови збереження такого підходу Туреччина, ймовірно, зможе краще визначати основні характеристики кіберзлочинців і передбачати їхні наступні кроки [494].

Індія суттєво потерпає від шахрайства у сфері інтернет-банкінгу та кредитних карток, наприклад, Індійська комп'ютерна команда з реагування на надзвичайні ситуації (Indian Computer Emergency Readiness Team, CERT-In) повідомила про 49455 інцидентів у сфері кібербезпеки лише за один 2016 р. [508]. У Стратегії кібербезпеки Індії зазначається про ефективні механізми підтримки верховенства права, що впроваджуються законодавчим шляхом, а також про те, що усвідомлення небезпечності кіберзлочинів залишається найкращим засобом їх попередження.

Захист критичної інфраструктури та врегулювання кризових ситуацій на національному рівні.

Питання підтримки безпеки критичної інфраструктури є справою національної безпеки – з чи без урахування кіберскладової. Однак мережі, що використовуються в об'єктах критичної інфраструктури, не застраховані від зростання залежності від інтернет-технологій. Тому можна стверджувати, що

кібербезпека поєднується з національною безпекою в основному в критичній інфраструктурі. І хоч держави не мають одностайності у визначенні того, які об'єкти слід вважати критичною інфраструктурою, загальне бачення вказує на те, що такими є об'єктами є надавачі найважливіших послуг всередині держави в рамках національної безпеки.

Крім цього, одним з найскладніших завдань у сфері підтримки кібербезпеки полягає у тому, що значною частиною об'єктів критичної інфраструктури в державах з ліберальною ринковою економікою керують суб'єкти приватного сектору, а не держава, незважаючи на те, що ці об'єкти вважаються невід'ємною частиною національної безпеки. Крім того, надання приватному сектору можливості пропонувати більш безпечні та стабільні послуги пов'язане з наданням приватним надавачам послуг державної допомоги [383].

Розробники Стратегії кібербезпеки *США* і відповідальні за прийняття рішень у сфері кібербезпеки створили новий інституційний механізм реалізації процесу обміну інформацією між зацікавленими сторонами приватного і публічного секторів шляхом запуску нової Національної команди реагування на комп'ютерні надзвичайні події (National computer emergency response team, CERT). Але при цьому останнє слово залишається завжди за президентом США, рішення котрого дає право застосувати кіберзброю. І це є певним недоліком, оскільки безпрецедентна швидкість кібератак здійснює суттєвий тиск на такий механізм прийняття рішень.

Операційний центр з питань безпеки інформаційних систем *Франції* (Operational Center of the Security of Information Systems, COSSI), головний орган Франції для координації ініціатив у сфері кібербезпеки, несе основну відповідальність за врегулювання кризових ситуацій на національному рівні, а також за приготування та реалізацію плану дій щодо врегулювання кризових ситуацій у кіберпросторі. Наголошуючи на великому значенні критичної інфраструктури, Франція у Стратегії національної безпеки звертає особливу увагу на заходи безпеки стосовно цього середовища [330].

Слідом за боротьбою з кіберзлочинністю, другою за важливістю ціллю стратегії національної безпеки *Великобританія* визначає захист об'єктів критичної інфраструктури. Її Стратегія кібербезпеки спрямована на розвиток публічно-приватного партнерства та заохочення обох сторін до подальшої співпраці. Наприклад, у 2018 р. уряд Великобританії виділив 14,2 млрд. фунтів для 20 найбільших приватних постачальників послуг, а державні служби мали найменший персонал після Другої світової війни (Уряд Великобританії, 2019).

Необхідність співпраці описана так: «Велика частина інфраструктури, котру ми повинні захищати, знаходиться у приватній власності та керується приватним сектором. Досвід та інновації, необхідні для адекватної відповіді на загрози, будуть орієнтовані на бізнес» [485]. Саме з метою активізувати публічно-приватне партнерство та заохотити обидві сторони до кращого співробітництва Великобританія внесла кардинальні зміни до своєї Стратегії кібербезпеки. Ще однією важливою метою Стратегії кібербезпеки Великобританії є захист міжнародної критичної інфраструктури. Перша і головна причина цього – боротьба, яку держава веде з кіберзлочинністю.

За показник, який демонструє намір керівництва *Нідерландів* мати комплексний підхід, що поєднує усі суб'єкти у сфері кібербезпеки, в Стратегії кібербезпеки Нідерландів взято налагодження відповідного рівня співпраці усіх зацікавлених сторін держави та міжнародних суб'єктів; цей показник включений до найважливіших принципів реалізації Стратегії. На цьому етапі надзвичайно важливо зазначити, що стратегія Нідерландів задіяє як публічні, так і приватні міжнародні суб'єкти до вирішення питань національної безпеки. Загалом, ця частина Стратегії є, ймовірно, конструктивним зразком в аспекті заходів зі зміцнення довіри, котрі є визначальними для міжнародних кіберальянсів.

У Стратегії кібербезпеки *Німеччини* захист критичної інфраструктури посідає центральне місце. Існує 10-кроковий план дій щодо захисту кіберпростору, з якого три кроки присвячені захисту саме критичної

інфраструктури. При цьому публічно-приватне партнерство у плані назване обов'язковою умовою досягнення цих цілей [259]. Також було створено Раду національної кібербезпеки Німеччини, завданням якої є координування співпраці правоохоронних органів, Конституційного суду, агентств розвідки, Федерального агентства новин і окремих міністерств. Це був крок Німеччини до створення ефективної системи врегулювання кризових ситуацій у випадку виникнення інцидентів у національному кіберпросторі, а також щоб вирішити питання того, яка владна структура має право вимагати реалізації плану дій у разі кібератаки та інших пов'язаних з цим проблем.

Як вже згадувалось раніше, визначення критичної інфраструктури відрізняються залежно від рівня процвітання держави. В зв'язку з цим у *Туреччині* створено чіткий перелік об'єктів, що надають критично важливі послуги [494]. При цьому відповідно до плану дій Туреччини у сфері кіберпростору, що містить галузевий аналіз ризиків для критичної інфраструктури, перевагу у сфері захисту критичної інфраструктури мають публічні організації, відповідальні за регулювання і аудит критичних секторів, а також за розробку галузевих планів дій в надзвичайних ситуаціях і для безперервного ведення бізнесу. Туреччина також досягла значного прогресу в інституціоналізації кібербезпеки, утворивши національну Команду реагування на комп'ютерні надзвичайні події (USOM) та плануючи створити подібні команди реагування для окремих секторів. Один із найважливіших пунктів стратегічного підходу Туреччини до захисту критичної інфраструктури пов'язаний з визначенням правових санкцій у відповідь на порушення безпеки критичної інфраструктури.

Індія у свою чергу створила Національний центр захисту критичної інформаційної інфраструктури (National Critical Information Infrastructure Protection Centre, NCIIPC), який має повноваження для підвищення рівня захисту та стійкості цієї сфери. Але при цьому Індія у своїх стратегічних документах не визначає чітко найважливіші об'єкти інфраструктури.

Кібердипломатія та управління інтернетом

Кібердипломатія, відома також як *публічна дипломатія 2.0,* в основному сконцентрована на впровадженні технічних інновацій зі сфери комунікації і інформаційних технологій до сфери дипломатії [412]. Загалом, вона пов'язана зі зв'язками з громадськістю і відкриває новий вимір для традиційної дипломатії, інтегруючи нові засоби, що дозволяють державам взаємодіяти не лише з високоповажними представниками, але також з пересічними громадянами з різних країн. Ймовірно через слабкий і неконтрольований зв'язок зі сферою безпеки багато стратегічних документів не містять окремої частини, присвяченої кібердипломатії.

Держави зазвичай вбачають у кібердипломатії основу для формування міждержавних зв'язків і налагодження міжнародної співпраці з питань кібербезпеки. *Нідерланди* у Стратегії кібербезпеки підкреслюють потребу міждержавної співпраці і обіцяють брати активну участь в Форумі з управління інтернетом від ООН (UN Forum of Internet Governance). *Німеччина* так само підкреслює важливість міжнародної співпраці і обіцяє активно підтримувати такі організації як ООН, НАТО і G-7.

В контексті глобальної інтернет-спільноти набір механізмів для управління інтернетом складається з громадських організацій включно з представниками приватного сектору. На даний час двома найвпливовішими організаціями у сфері управління Інтернетом є Рада з архітектури Інтернету (Internet Architecture Board, IAB) та Інженерна рада Інтернету (Internet Engineering Task Force, IETF). Втручання держав у діяльність цих організацій є суттєво обмеженим. Втім низка держав надає суттєвої уваги питанням, пов'язаним з кібердипломатією та управлінням Інтернетом як складовим кібербезпеки.

Так, Підрозділ з питань міжнародної кібербезпеки є інструментом управління Інтернетом у *Великобританії*, що був сформований під керівництвом міністра закордонних справ у 2011 році. При цьому Стратегія кібербезпеки Великобританії в основному зосереджена навколо міжнародної

співпраці з метою створення основи для міжнародного кіберзаконодавства, а також для розвитку двосторонніх відносин з впливовими суб'єктами кіберпростору. У Лондоні вважають, що більш активна участь ЄС у дискусіях з питань кібербезпеки могла б сприяти формуванню більш активної стратегії у цій сфері.

На відміну від Великобританії з її міжнародним орієнтуванням, *Франція* наполягає на пристосуванні національної правової бази до найновіших напрацювань у сфері кібербезпеки.

Сама назва Стратегії кібербезпеки *США* – «Міжнародна стратегія дій у кіберпросторі» – вказує на те, що США вважають кіберпростір сферою, до якої повинен застосовуватись міжнародний підхід. Через це кібердипломатія набуває важливого значення для американської кіберстратегії. Наочним прикладом стратегічних змін є стратегічний документ, опублікований ще у 2003 р. під назвою «Національна стратегія підтримки безпеки кіберпростору», у якому зазначається, що США надають вирішального значення укріпленню міжнародних зв'язків і наголошують на важливості збереження свободи слова та правових санкцій щодо управління інтернетом за ліберальним зразком.

Аналіз стратегічних документів *Німеччини* в галузі кібердипломатії показує, що у її стратегії пропонується ефективна координація для підтримки кібербезпеки в усьому світі. Німецькі стратеги розуміють кіберпростір як «простір свободи, безпеки та справедливості». Під час головування в ОБСЄ в 2016 р. Німеччина визначила три пріоритети для кібердипломатії: безпека, економічне співробітництво та права людини.

Індія у своїй стратегії чітко говорить про налагодження двосторонніх та багатосторонніх відносин, а також про співпрацю з питань кібербезпеки з іншими країнами. Керівництво держави проводить двосторонні діалоги з питань кібербезпеки з Великобританією, США та Німеччиною. Це поєднується із запуском ініціативи Цифрова Індія (Digital India) – для її реалізації створюються багатосторонні зв'язки. «Кібердипломатія – це сфера,

що надалі розвивається. Це вимагає складних знань з технологій, права, політики тощо. Уряд Індії зосереджується на цьому» [412].

Отже, виклики кібербезпеки стосуються усіх країн, і жодна з них не стикається з абсолютно однаковими проблемами, але більшість з них є подібними, що дає можливість виробляти спільні універсальні рішення, які потім можна адаптувати до умов конкретних держав. При цьому кіберпростір є невід'ємною частиною розвитку будь-якої сучасної держави, тому потужний кіберпотенціал має вирішальне значення для прогресу та розвитку держав в економічній, політичній та соціальній сферах.

Це зумовлює необхідність розробки та реалізації національних стратегій кібербезпеки, які б висували на перший план і підкреслювали необхідність підвищення рівня обізнаності щодо питань кіберсфери всередині гетерогенних категорій, таких як публічні службовці, політики, бізнесмени IT-спеціалісти, представники третього сектору та ін.

І залежно від використаних підходів, кібербезпеку можна сприймати або як відповідальність приватного сектору, або як відповідальність окремих органів публічної влади – від правоохоронних органів до військових відомств, або як поєднання обох. І саме останній підхід, на нашу думку, має бути застосований в Україні.

2.4. Національні стратегії кібербезпеки: порівняльний аналіз

Отже, як було зазначено вище, низка країн уже розробили і опублікували свої НСК , які мають різні назви (національні стратегії інформаційної безпеки, стратегії захисту інформаційного простору, стратегії протидії інформаційним загрозам тощо. Нижче проаналізуємо і порівняємо документи 18 країн світу:

– з одного боку, найбільш розвинених країн світу, зокрема Австралії (AUS), Канади (CAN), Франції (FRA), Німеччини (DEU), Японії (JPN), Люксембургу (LUX), Нідерландів (NLD), Нової Зеландії (NZL), Іспанії (ESP),

Великобританії (GBR) і США (USA).

– з іншого боку, країн, що швидко розвиваються, Індії (IND), ПАР (ZAF), Уганди (UGA).

Загальновідомо, що стратегія – це «план дій, метою якого є досягнення певної візії (довгострокової мети)» [442]. Інші визначення стратегії включають такі аспекти як напрям або шлях до візії та (ближчих) цілей, бажане майбутнє і комплекс дій для досягнення довгострокових цілей тощо [524].

Таким чином національні стратегії кібербезпеки представляють собою національний план дій на основі національної візії, яка має на меті досягнення певних довгострокових цілей щодо підвищення рівню безпеки у інформаційній сфері. Узагальнення змісту розроблених документів, дозволяє стверджувати, що національні стратегії включають три групи цілей:

- систематизація державної політики в інформаційній сфері;
- координація дій різних суб‘єктів в сфері кібербезпеки та розподіл відповідальності між усіма зацікавленими сторонами;
- донесення національних намірів в сфері кібербезпеки до інших держав та зацікавлених сторін.

Прикладами третьої цілі є демонстрація сили та позиціонування стратегії у якості засобу затвердження лідерства у сфері кібербезпеки). Зацікавленими сторонами в контексті НСК є уряд, урядові органи з цивільних справ, військові, контролюючі органи, оператори об’єктів ключової інфраструктури, великі, середні та малі підприємства, науково-дослідні організації, університети, окремі громадяни та населення в цілому.

Оскільки у держави може бути більше національних стратегій, НСК повинна описувати її зв’язок з іншими стратегіями. Аудиторія НСК повинна зрозуміти, яким чином візія та план дій НСК пов’язані з іншими стратегіями (вищого порядку) такими як стратегія національної безпеки і оборони, національна стратегія захисту ключових об’єктів інфраструктури, національна установка по електронним засобам комунікації, національна

стратегія економічного розвитку і міжнародними стратегіями [309].

Візія НСК та напрям її стратегічних цілей повинні бути максимально чіткими з метою стимулювання зацікавлених сторін до об'єднаних дій, прописаних у НСК. Якщо є можливість, національна стратегія повинна виходити за територіальні кордони відповідної держави і ураховувати вплив зовнішніх чинників (протидію йому).

Далі порівняємо НСК різних країн за низкою ключових ознак.

1. Визначення кібербезпеки

Як зазначено у таблиці 3.1, лише вісім з чотирнадцяти держав чітко визначили поняття «*кібербезпека»*. Дві держави (GBR і CAN) описово характеризують поняття кібербезпеки. Уганда і США дають визначення поняттю «інформаційна безпека», не згадуючи про «кібербезпеку». Три з чотирнадцяти держав (ESP, JPN і LUX) говорять кібербезпеку на стратегічному рівні без визначення самого поняття.

Більш того, десять держав, які визначили або описали поняття кібербезпеки, розуміють його зовсім по-різному. Деякі держави визначають кібербезпеку як колегіальний підхід до захисту і гарантій прав фізичних та юридичних осіб у сфері інформаційної безпеки. Інші держави застосовують державницький підхід і акцентують на захисті від загроз у кіберпросторі (табл. 2.2).

Відсутність спільних узгоджених визначень понять, пов'язаних з кіберпростором, прийнятих декількома державами ймовірно є причиною непорозумінь між державами під час обговорення міжнародних підходів до міжнародних загроз у кіберпросторі.

На початку 2011 р. двостороння російсько-американська робоча група Інституту досліджень у сфері безпеки Захід-Схід та МГУ підготувала чорновий варіант моделі міжнародної термінології. Вони визначили кібербезпеку як «властивість кіберпростору до опору навмисним і ненавмисним загрозам, реагування на них та відновлення» [452, с. 31].

Таблиця 2.2

Розуміння «кібербезпеки» у стратегіях різних країн

Країна	Визначення	Кібербезпека
AUS	є	Заходи, пов'язані з конфіденційністю, доступністю і цілісністю інформації, яка обробляється, зберігається і передається за допомогою електронних та аналогічних засобів.
CAN	опис	Відповідний рівень реагування та/або пом'якшення дії кібератак (навмисного чи ненавмисного доступу, використання, маніпуляцій, переривання або знищення (за допомогою електронних засобів) цифрової інформації та/або цифрової і фізичної інфраструктури, яка використовується для обробки, передачі та/або зберігання такої інформації.
DEU	є	Бажана ситуація у сфері інформаційної безпеки, у якій ризики в (міжнародному) кіберпросторі було знижено до прийнятного мінімального рівня. Примітка: цивільну та військову кібербезпеку визначено у схожому формулюванні.
FRA	є	Інформаційна система, яка забезпечує опір ймовірним випадкам у кіберпросторі, які можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, оброблюються або передаються, а також пов'язаних сервісів, які надаються за допомогою систем інформаційно-комунікаційних технологій (ІКТ).
GBR	опис	Охоплює як захист національних інтересів у кіберпросторі а також переслідує мету розширення політики національної безпеки шляхом використання багатьох можливостей, запропонованих кіберпростором.
IND	є	Діяльність із захисту інформації та інформаційних систем (мереж, комп'ютерів, баз даних, дата-центрів та застосунків) за допомогою відповідних процесуальних і технологічних заходів безпеки.
NLD	є	Відсутність загрози або шкоди, завданої порушенням або знищенням ІКТ або через їх злочинне використання.
NZL	є	Практика максимального захисту мереж, що складають кіберпростір, від втручань, підтримка конфіденційності, доступності та цілісності інформації, виявлення вторгнень та інцидентів, реагування на них та відновлення в результаті таких вторгнень та інцидентів.
ROU	є	Нормальний стан в результаті комплексу превентивних та зворотних заходів, які забезпечують конфіденційність, цілісність, доступність, достовірність та відмовостійкість інформації у електронній формі, а також державних і приватних ресурсів та послуг у кіберпросторі.
UGA	не визначено	Посилання на «інформаційну безпеку»: захист інформації та інформаційних систем від неавторизованого доступу, використання, розкриття, порушення, змін або знищення.
ZAF	є	Набір інструментів, політик, концепцій безпеки, захисних механізмів, підходів до управління ризиками, дій, навчальних матеріалів, передових практик, гарантій і технологій, які можуть використовуватися для захисту кіберпростору, організації і активів користувача.

Незважаючи на безперервну академічну дискусію більшості визначень термінології у кіберпросторі, визначення Раушера-Ященко може стати заміною більшості національних визначень та розуміння кібербезпеки, відображених у таблиці 2.2. Щоправда, канадське бачення кібербезпеки не збігається з визначенням Раушера-Ященко, оскільки Канада лише зосереджується на зловмисних атаках у кіберпросторі. Дві інші держави розширили бачення Раушера-Ященко. Визначення, сформульоване Великобританією, включає фізичні загрози та загрозу електромагнітних завад у кіберпросторі [280]. Німеччина включає поняття прийняття ризику у своє визначення [249]. 15 з 18 держав обговорюють поняття кіберзлочину без його визначення, як і поняття кібербезпеки. Румунія — це єдина країна, яка у НСК дає визначення всім поняттям, пов'язаним з кіберпростором [421].

2. Загальна інформація

Далі порівняємо базову інформацію про НСК, зокрема, таку, як кількість редакцій, сфера регулювання, зв'язок з іншими нормативними документами, а також обсяг та зміст. Останнє включає зв'язок між іншими національними та міжнародними стратегіями, усвідомлення наявних загроз і засобів протидії ним.

2.1. Кількість редакцій

Дванадцять з чотирнадцяти держав один раз ухвалювали свою НСК; Японія та Великобританія мають вже другу редакцію НСК.

2.2. Сфера регулювання

Більшість НСК передбачають комплексний підхід до регулювання кіберпростору. Щоправда, у німецькій НСК прямо вказано, що сферою її регулювання є лише інформаційно-комунікаційні технології (ІКТ), підключені до Інтернету. Формулювання австралійської, канадської, іспанської та новозеландської НСК пропонує таке ж вузьке бачення кіберзагроз. У голландській НСК прямо зазначено, що вона зосереджена на широкому діапазоні ІКТ, який, на відміну від ІКТ, підключених до Інтернету, включає, наприклад, смарт-карти, автомобільні систем та засоби передачі

інформації. Франція та ПАР також мають аналогічне бачення. У інших НСК ця тема менш виражена, але вони не зосереджуються безпосередньо «лише на Інтернеті».

2.3. Зв'язок з іншими нормативними документами

НСК восьми країн безпосередньо пов'язано зі стратегіями національної безпеки у їхніх державах. Іспанська НСК є фактично частиною іспанської стратегії національної безпеки. Низка держав розробила НСК в результаті минулих оцінки національних загроз та ризиків, а в деяких випадках НСК навіть включає оцінку національних загроз та ризиків. Цікаво, що Уганда застосовує SWOT-аналіз (аналіз сильних і слабких сторін, можливостей та загроз) на національному рівні для створення плану стратегічних і пов'язаних дій. Нідерланди запровадили зовнішній циклічний процес: один з напрямів реалізації НСК – проведення щорічної оцінки національних кіберзагроз та ризиків для включення у реєстр оцінки національних ризиків (NRB). В свою чергу, процес оцінки NRB може викликати потребу у оновленні самої НСК.

У більшості НСК прямо зазначається загроза кібербезпеці ключових об'єктів інфраструктури. Щоправда, зв'язок НСК зі стратегією національного захисту ключових об'єктів інфраструктури обговорюється не так прямо. Цікаво, що дев'ять з десяти країн-членів ЄС не пов'язують з НСК з Європейською Директивою Захисту Ключових Об'єктів Інфраструктури [283].

Більшість з НСК охоплюють питання економічного благополуччя сфери кіберпростору. Кібербезпека вважається основою для підвищення благополуччя населення та економічного добробуту.

Між тим, аналіз НСК більшості держав свідчить про те, що в урядах відповідних країн триває дискусія про те, яка урядова установа або орган відіграє ключову роль у разі масштабної кібератаки проти держави або порушення роботи ІКТ. У якості стратегії національної оборони деякі держави розробляють військові кібероперації/засоби для оборони у

інформаційні сфері. У НСК Великобританії з 2009 р. [279] підвищення військового та розвідувального потенціалу у сфері кібербезпеки прописано чіткіше, аніж у пізнішій редакції 2011 р. [280]. Французька НСК посилається на свою стратегію національної оборони та безпеки, яка підкреслює потребу у (військовій) обороні та стримування у сфері кібербезпеки [463]. Німецька [249] та нідерландська [415] НСК посилаються на свої напрацювання у сфері військових кібероперацій.

2.4. Суб'єкти загроз та цілі суб'єктів загрози.

У своїх НСК всі держави зосереджуються на кіберзагрозах для своїх ключових об'єктів (інформаційної) інфраструктури. Переважна більшість країн прямо вказують на ці загрози, називаючи кіберзагрози важливим ризиком для своєї національної безпеки. Франція непрямо зазначає кіберзагрози значущим чинником для оборонної сфери, посилаючись на свою «Білу книгу» з питань оборони та національної безпеки [462].

У своїх НСК Німеччина, Індія та Японія зосереджуються на загрози зростання глобалізаційних факторів (і міжнародних суб'єктів) у сфері кібербезпеки. З цими загрозами вони пов'язують ризики зростання соціальної напруженості, а також порушень особистих прав та свобод громадян. Шість держав прямо вказують на цю загрозу. Вісім держав взагалі не згадують цей тип загрози у своїх НСК, незважаючи на визнання певних ризиків, пов'язаних із швидким розвитком інформаційного суспільства.

Всі держави, окрім США та Японії, прямо називають окремих осіб, злочинців та організовану злочинність суб'єктами зловмисної загрози. Кібершпигунство (електронне шпигунство) прямо зазначено у НСК десяти держав. Тринадцять держав визначили загрозу ворожих дій з боку іноземних держав (наприклад, кібервійна) у своїх НСК. Незважаючи на низку атак у кіберпросторі з боку таких угрупувань як Anonymous та LulzSec, лише Нідерланди, Нова Зеландія та Великобританія [280] прямо визнають хакерів та екстремістів суб'єктами зловмисної загрози.

Тринадцять держав визнають загрозу (потенційних) терористичних

кібератак на ключові об’єкти (інформаційної) інфраструктури, хоч таких випадків ще не було [401]. Більш того, Канада, Франція, Нова Зеландія та Великобританія у своїх НСК зазначають, що терористи можуть використовувати кіберпростір для пропаганди, залучення коштів, спілкування та планування терактів. Окрім того, Великобританія зазначила, що кіберпростір використовується для збору розвідданих про терористів [279].

Німеччина, Японія та Великобританія прямо вказують на загрозу широкомасштабних кібератак на свої ключові об’єкти (інформаційної) інфраструктури. У випадку з Японією це не дивно, оскільки ця країна пережила кілька широкомасштабних (і широко відомих) кібератак на урядові та комерційні системи у недалекому минулому. Щоправда, на момент публікації НСК інші дві держави не стикалися з широкомасштабними кібератаками.

Японська і німецька НСК посилаються на загрозу невідповідностей між існуючими розробками в сфері ІКТ та необхідним рівнем кібербезпеки, пов’язаним з цими розробками. Цікаво, що жодна з інших держав не піднімає тему загроз, викликаних інноваціями в сфері ІКТ, та ризиків, які вони несуть.

Кіберзагрози, які охоплює НСК Великобританії за 2009 р., включають заглушення сигналу GPS та його модифікацію, передачу радіочастот великої потужності за допомогою НВЧ-випромінювання високої потужності, пошкодження незахищеної електроніки [280]. Ці загрози можуть мати нецифровий характер, але вони призводять до пошкодження цифрових активів. Жодна з НСК не посилається на ці загрози, незважаючи на те, що світом шириться проблема, пов’язана з тим, що злочинці використовують ці технології. Таким чином, дуже дивно, що більшість країн не виносять ці загрози та виклики на перший план.

3. Візії, цілі та принципи

Згідно з визначенням НСК, наведеним вище, вона повинна містити точку фокусу «на горизонті», тобто візію (табл. 2.3).

Таблиця 2.3

Національні візії кібербезпеки

Країна	**Особливість визначення**	**Визначення**
AUS	Пряме	Підтримка безпечного, стійкого та надійного цифрового робочого середовища, яке підтримує національну безпеку та примножує переваги цифрової економіки.
CAN	Пряме	Підвищення безпеки кіберпростору для всіх канадців.
DEU	Пряме	Федеральний уряд має намір зробити суттєвий внесок у безпеку кіберпростору одночасно підтримуючи і підвищуючи соціально-економічне благополуччя у Німеччині.
ESP	Пряме	Підтримка безпеки Іспанії, її громадян та жителів у кіберпросторі.
FRA	Не виражене прямо	Збереження меж своєї суверенності, зосереджуючись на можливостях, необхідних для підтримки стратегічної і політичної автономії держави: {...} а кібербезпека є одним з пріоритетних напрямів.
GBR	Пряме	Досягнення високих соціально-економічних показників завдяки здоровому, стійкому та надійному кіберпростору, де ми зможемо підвищити рівень благополуччя і національної безпеки та зробити суспільство сильнішим, керуючись нашими ключовими цінностями такими як свобода, справедливість, прозорість та верховенство права.
IND	Не виражене прямо	Правильне зосередження на надійному обчислювальному середовищі та достатньому рівні довірі до цифрових транзакцій стає одним з вимушених пріоритетів для країни, враховуючи розвиток IT-сфери в Індії та важливу роль країни на світовому ринку інформаційних технологій.
JPN	Не виражене прямо	Уряд відповідає за подолання ризиків використання ІКТ завдяки заходам з укріплення безпеки ключових об’єктів інфраструктури, які слугують на підтримку соціально-економічної діяльності, тісно пов’язані з щоденним життям держави і також повинні вживати організованих та негайних дій задля підвищення рівня національної безпеки та ефективного регулювання кризових ситуацій.
LUX	Пряме	Підвищення рівня кібербезпеки та стійкості інфраструктур і внесок у захист громадян, спеціалістів та суспільства.
NLD	Пряме	Безпека і впевненість у відкритому і вільному цифровому суспільстві.
NZL	Не виражене прямо	Окреслення реакції уряду на зростання кіберзагрози та ініціатив для окремих осіб, компаній і уряду з метою зміцнення стану кібербезпеки Нової Зеландії.
UGA	Пряме	Стратегічний напрям національної інформаційної безпеки з метою завоювання довіри та забезпечення комерційного зростання і економічного розвитку.
USA	Пряме	Заохочення американців і надання їм повноважень із забезпечення надійності тих частин кібербезпеки, якими вони володіють, керують, контролюють або з якими вони взаємодіють.
ZAF	Пряме	Створити середовище, в якому буде забезпечуватися надійність та довіра до безпечного використання ІКТ.

У табл. 2.4 викладено стратегічні цілі кібербезпеки держав. Щоправда, у [249] Німеччина презентує набір стратегічних пріоритетів, які в інших НСК представлені як напрями дії. Більшість НСК містять 3-4 стратегічних цілі. Такі держави як Німеччина, Уганда і ПАР, які мають більше чотирьох цілей, об'єднують свої стратегічні цілі з напрямами дії (наприклад, Люксембург) або презентують власні основні напрями дій.

Таблиця 2.4

Стратегічні цілі НСК

Країна	**Стратегічні цілі**
AUS	Всі австралійці знають про ризики у кіберпросторі, захищають свої комп'ютери і вживають всіх належних заходів для захисту своєї особи, недоторканості особистого життя і коштів в мережі.
	Австралійські компанії керують надійними і стійкими ІКТ з метою захисту цілісності транзакцій, особи та недоторканості особистого життя клієнтів.
	Австралійський уряд забезпечує свої транзакції, особи та недоторканості особистого життя своїх клієнтів.
CAN	Забезпечення надійності урядових систем.
	Встановлення партнерських відносин життєво важливих систем у інформаційній сфері, які не відносяться до федерального уряду.
	Забезпечення надійності діяльності канадців в мережі.
DEU	Захист ключових об'єктів інфраструктури.
	Забезпечення надійності ІТ-систем в Німеччині.
	Підвищення рівню інформаційної безпеки у сфері публічного управління.
	Національний центр реагування на кіберзагрози.
	Національна рада кібербезпеки.
	Ефективна боротьба зі злочинністю з кіберпростором.
	Ефективні координовані дії з метою забезпечення кібербезпеки у Європі та в світі.
	Використання надійних ІТ-технологій.
	Підвищення кваліфікації персоналу, який працює у федеральних органах.
	Інструменти для реагування на кібератаки.
ESP	Іспанська НСК є невід'ємною частиною іспанської стратегії національної безпеки і має на меті захищати іспанських ключових і стратегічних інтересів та цінностей.
FRA	Стати світовим лідером у сфері кібербезпеки.
	Гарантувати французам свободу прийняття рішень на національному рівні шляхом захисту інформації про громадян.
	Підвищувати рівень кібербезпеки ключових об'єктів інфраструктури.
	Гарантувати безпеку у кіберпросторі.
GBR	Боротися з кіберзлочинами і стати одним з найбезпечніших місць у світі для бізнесу у кіберпросторі.
	Бути більш стійкими до кібератак та краще захищати свої інтереси у кіберпросторі.

Продовження таблиці 2.4

GBR	Допомагати формувати відкритий, стабільний та здоровий кіберпростір, який наше населення може безпечно використовувати і яке підкреслює відкрите суспільство.
USA	Запобігання кібератакам проти ключових об'єктів інфраструктури США
	Зниження вразливості держави до кібератак
	Мінімізація шкоди та скорочення часу на відновлення від реальних кібератак
ZAF	Розбудова дієвих структур кібербезпеки
	Мінімізація кіберзагроз та вразливостей
	Розвиток співпраці державного та приватного секторів та їх координація
	Заохочення та зміцнення міжнародної співпраці у сфері кібербезпеки
	Розвиток потенціалу та поширення культури кібербезпеки
	Підтримка дотримання відповідних робочих та технічних стандартів кібербезпеки
IND	Розвивати ІКТ в Індії у якості рушійної сили для економічного росту та благополуччя
	Створити модель безпеки для забезпечення надійності кіберпростору
JPN	Покращена політика боротьби з кібератаками
	Політика адаптації до змін у середовищі кібербезпеки
	Активні/динамічні заходи з кібербезпеки
LUX	Забезпечити експлуатаційний захист інфраструктури та систем ІКТ
	Модернізувати правову базу
	Розвивати національну та міжнародну співпрацю
	Інформувати, навчати та підвищувати обізнаність про ризики, пов'язані з кібербезпекою
	Ухвалити обов'язкові норми і стандарти
NLD	Покращити безпеку цифрового суспільства з метою підвищення довіри громадян, компаній та уряду до ІКТ, щоб стимулювати голландську економіку та підвищити рівень благополуччя та добробуту громадян.
	Гарантія належного правового захисту у цифровій сфері та запобігання дестабілізації суспільства.
	Вживання достатніх заходів у випадку проблем.
NZL	Підвищення обізнаності та рівня інформаційної безпеки приватних осіб та суб'єктів малого бізнесу
	Захист урядових систем
	Розбудова стратегічних відносин з метою підвищення рівню кібербезпеки ключових об'єктів інфраструктури та інших компаній.
UGA	Систематизація впровадження інформаційної безпеки на національному та міжнародному рівні
	Систематизація, класифікація та захист ключових об'єктів інфраструктури від порушень
	Розробка моделі моніторингу інформаційної безпеки
	Поширення інформації про надійну е-комерцію, послуги електронного уряду та інші національні ІТ-проєкти
	Гарантія прав громадян на недоторканість особистого життя завдяки якісному управлінню інформаційною безпекою
	Розвиток культури обізнаності у сфері кібербезпеки на національному рівні та зміцнення потенціалу у сфері людських ресурсів
	Підтримка управління ризиками, пов'язаними з інформаційною безпекою, та забезпечення зрілого рівня інформаційної безпеки

Велика різниця між цілями національної стратегії викликана різними відправними точками та різними за змістом візіями, зокрема, такими, як безпечне, надійне та стійке ІКТ-середовище, економічне благополуччя, національна безпека та оборона, захист законних прав та інтересів громадян. Австралія, Канада та Нова Зеландія будують свої цілі навколо аналогічної схеми зацікавлених сторін: уряду, ключових об'єктів інфраструктури, компаній та громадян/ приватних осіб (використовуючи економічний підхід). У своєму наборі стратегічних цілей Японія прямо визнає потребу у швидкому пристосуванні до нових та майбутніх загроз кібербезпеці. Німеччина також піднімає цю тему, але не вказує на жодні пов'язані з цим дії.

У Франції інший підхід: вона висловлює свої амбіції в тому, щоб стати світовим лідером у кібербезпеці та зберігати свій статус інформаційної переваги у національній кібербезпеці. До речі, Франція – єдина держава, яка чітко слідує цим шляхом, хоча в деяких інших НСК у певному вигляді підтримується концепція демонстрації сили. Наприклад, Великобританія має законне право збирати розвіддані про злочинців, терористів та інших небезпечних суб'єктів у кіберпросторі та використовує цю інформацію для боротьби з кіберзлочинами та зниження мотивації і можливостей ворога діяти у кіберпросторі. Згідно з публікацією Дерріка [295], MI6 здійснив хакерську атаку на Інтернет-журнал терористичної організації Аль-Каїда «Інспайр». Згідно з цією публікацією, Інтернет-стаття «Зроби бомбу на кухні твоєї матусі» було замінено на рецепти кращих американських капкейків. Це наочний приклад впровадження цієї стратегії. При цьому НСК Великобританії містить посилання на можливості використання кіберпростору, які можна віднести до «деяких дій, що були ініційовані урядом і які не підлягають розголошенню» [280, с.9].

4. Керівні принципи та базові умови.

Згідно з табл. 2.5, більшість держав пов'язують зміст своїх НСК з базовими принципами національної безпеки. У НСК Франції, Японії, Литви,

Люксембургу, Нової Зеландії, Уганди та ПАР відсутні посилання на жодні керівні принципи. Деякі держави посилаються на захист громадянських свобод та інших основних національних (міжнародних) демократичних цінностей. У НСК Німеччини відсутні посилання на такі цінності. Вісім держав у якості базових умов кібербезпеки вказують співпрацю та суспільно-державні об'єднання. США (як і інші держави, які не вказали керівні принципи) не згадували громадські об'єднання у якості ключового суб'єкту реалізації НСК.

Таблиця 2.5.

Керівні принципи НСК (за наявності опису)

AUS	1	Національне лідерство.
	2	Розподіл відповідальності.
	3	Партнерства.
	4	Активна участь міжнародної спільноти.
	5	Управління ризиками
	6	Захист австралійських цінностей
CAN		Чіткі керівні принципи, відсутні, але є посилання на НСК США, Великобританії і Австралії. «Більшість керівних принципів та першочергових завдань, викладених у цих звітах нагадують нам ті, що є у нас» [451, с.8].
DEU		Всі зацікавлені сторони повинні діяти як партнери і разом виконувати задачі з забезпечення захисту. Необхідно дотримуватися міжнародних правил поведінки, норм і стандартів.
ESP	1	Комплексний підхід.
	2	Координація.
	3	Ефективне використання ресурсів.
	4	Попередження та профілактика.
	5	Стійкість.
	6	Взаємозалежна відповідальність.
GBR	1	Підхід на основі оцінки ризиків.
	2	Партнерська співпраця.
	3	Рівновага між безпекою і свободою та недоторканістю особистого життя.
NLD	1	Зв'язок між існуючими ініціативами кібербезпеки і їх зміцнення.
	2	Суспільно-державні об'єднання та чітка відповідальність, повноваження та гарантії.
	3	Особиста відповідальність за гарантію безпеки кіберпростору (громадян, компаній, органи і установи державного управління).
	4	Активна міжнародна співпраця.
	5	Заходи безпеки повинні бути урівноважені і пропорційні у відношенні між державною та національною безпекою і гарантією основних прав людини.
	6	При можливості, необхідно впроваджувати принципи саморегулювання, і у разі необхідності застосовувати законодавчий і нормативний контроль.
USA	Необхідно захищати недоторканість особистого життя і громадянські свободи.	

5. Зацікавлені сторони НСК

У табл. 2.6 відображається класифікація зацікавлених сторін, пов'язаних з кібербезпекою і визнаних такими у НСК. Як видно з наведеного, більшість країн очікують, що громадяни братимуть активну роль у кібербезпеці. Однак, Японія, Люксембург, Іспанія та ПАР лише згадують про громадян у зв'язку з підвищенням рівня їх обізнаності в інформаційній сфері. НСК ПАР та Японії зосереджено на відповідних урядах і ключових об'єктах інфраструктури.

Таблиця 2.6

Зацікавлені суб'єкти відносно реалізації НСК

	Громадяни	*Середній та малий бізнес*	*Інтернет-провайдери*	*Великі організації*	*Оператори ключових об'єктів інфраструктури*	*Держава*	*Міжнародні організації*
AUS	■	■	■	■	■	■	□
CAN	■	□	□	■	■	■	□
DEU	■	■	■	□	■	■	■
ESP	□	□	□	□	■	■	
FRA	■	■	□	■	■	■	□
GBR	■	■	■	■	■	■	■
IND	■	■	□	■	■	■	
JPN	□	□		□	■	■	□
LUX	□	□	□	□	■	■	
NLD	■	■	□	■	■	■	□
NZL	■	■	■	■	■	■	
UGA	■	■		■	□	■	
USA	■	■	□	■	■	■	■
ZAF	□	□		□	■	■	

Примітки: □ = якщо згадувалося у НСК, але містить обмежений набір відповідних заходів/дій

Інтернет-провайдери прямо вказані лише у НСК Австралії, Німеччини, Нової Зеландії та Великобританії. Хоча Секретаріат Кабінету Міністрів Великої Британії не вказував Інтернет-провайдерів у НСК в редакції 2009 р. [279], у редакції за 2011 р. згадуються Інтернет-провайдери, «які допомогли приватним особам виявити, чи існує загроза для їх комп'ютерів і що вони можуть зробити для вирішення цієї загрози і захиститися від атак у майбутньому» [280, с. 31]. Інтернет-провайдери Австралії, які мають

підтримку австралійського уряду, вжили низку спільних заходів з метою підвищення рівня кібербезпеки їх операцій та клієнтів. Згідно з австралійським НСК [232], такі заходи включають практичну інструкцію для Інтернет-провайдерів та визначення систем клієнтів, для яких існує загроза.

Німеччина, Великобританія і США прямо вказали міжнародні інформаційні інфраструктури у якості сторін, зацікавлених у кібербезпеці. Однак, варто відзначити, що ці зацікавлені сторони (наприклад, основні провайдери) працюють за межами сфери прямого впливу національних держав.

6. Плани дій на тактичному/функціональному рівні

Проведене дослідження свідчить про те, що всі держави розробили тактичні напрями дій і часто визначали комплекс детальних функціональних заходів на підтримку своїх стратегічних цілей кібербезпеки. Оскільки у більшості НСК виражено нагальну потребу у діях, можна констатувати наявність у них конкретного, вимірюваного, досяжного, реалістичного і прогнозованого (SMART) формулювання таких заходів. Загалом, SMART-підхід дозволяє національних парламентам виконувати наглядову роль, а також дозволяє іншим суб'єктам, відповідальним за кібербезпеку, моніторити хід впровадження напрямів дій, викладених у НСК. Він дозволяє виявляти недостатній прогрес, про який можна вчасно повідомити з метою успішної реалізації НСК в цілому. Найбільш відповідає SMART-критеріям НСК Японії через те, що вона безпосередньо пов'язана з підходом щодо управління якістю, по-друге, містить додаток, у якому вказано відповідальну(-і) зацікавлену(-і) сторону(-и) та набір критеріїв досяжності для кожного запланованого завдання, зазначені проміжні та кінцеві результати. При цьому Японія стала єдиною державою, яка у якості стратегічної цілі вказала швидку адаптацію до нових кіберзагроз і запланувала комплекс пов'язаних тактичних і функціональних заходів. Це свідчить про те, що японський підхід до питань кібербезпеки є найбільш раціональним в контексті динамічної перспективи безпеки у порівнянні з

іншими державами. Детальний аналіз заходів наведено у табл. 2.7.

Таблиця 2.7.

Ключові напрямі дій (пріоритети) та заплановані в НСК заходи

Ключові заходи та напрями дій	**AUS**	**CAN**	**DEU**	**ESP**
Активні/динамічні заходи безпеки	–	–	–	–
Навчально-освітня кампанія/кампанія з інформаційної безпеки	■	■ (ціль 3)	Захід 2	■
Політика, яка пристосовується до нових ризиків у сфері ІКТ Плани безперервної роботи і плани дій на випадок позаштатних ситуацій	–	–	□	■
Захист ключових об’єктів інфраструктури	■	■	Захід 1	■
Криптографічний захист	–	–	(Захід 8)	■
Контроль кіберзброї	–	–	–	■
Оборонні операції у сфері кібербезпеки/оперативні заходи і практичне навчання	–	■	■	□
Розробка та обмін передовими практиками	–	–	–	■
Економічне зростання	■	■	–	■
Освіта і навчання	■	■	(Захід 9)	■
Практичне навчання	■	■	■	
Пряме комплексне бачення Використання з метою подолання загроз Покращений рівень безпеки ІКТ-продуктів Обмін інформацією	■	■	Захід 4	□
Збір розвідданих про суб’єктів загроз	■	■		■
Міжнародна співпраця	■	■	Захід 7	■
Законодавча/правова база			–	■
Санкціонування стандартів безпеки Потенціал виявлення загроз на національному рівні	■	■	–	□
Потенціал реагування на загрози/регулювання кризових ситуацій у сфері ІКТ	■	■	Захід 4	
Захист недоторканості особистого життя	■	■	–	–
Поширення конвенції по кіберзлочинам	–	□	Захід 6	
Захист об’єктів інфраструктури другорядного значення	■	■	–	–
Суспільно-державні об’єднання	■	(Ціль 2)	–	■
Зниження ворожої мотивації і потенціалу			–	
Науково-дослідницька діяльність	■	■	–	–
Стійкість до порушень/зниження кількості загроз та вразливостей	■	–	–	–
Захищені протоколи та ПЗ	–	–	Захід 2	–
Захищені джерела отримання продуктів	–	–	Захід 8	■
Самозахист уряду	■	(Ціль 1)	Захід 3	■
Стратегічна рада кібербезпеки	–	–	Захід 5	–
Аналіз загроз і вразливостей	■	■	Захід 4	–
Відслідковування злочинців та їх притягнення до відповідальності	■	■	Захід 6	–

Продовження табл. 2.7

Ключові заходи та напрями дій	**FRA**	**GBR**	**IND**	**JPN**	**LUX**
Активні/динамічні заходи безпеки			■	(ціль 3)	
Навчально-освітня кампанія/кампанія з інформаційної безпеки	Захід 7	■	■	■	■
Політика, яка пристосовується до нових ризиків, пов'язаних з ІКТ	–	–	–	(ціль 2)	–
Плани безперервної роботи і плани дій на випадок позаштатних ситуацій	–	■	■	■	■
Захист ключових об'єктів інфраструктури	Захід 4 (ціль 3)	■	■	Напрям дій 1	■
Криптографічний захист Контроль кіберзброї	■	–	–	■	–
Оборонні операції у сфері кібербезпеки/оперативні заходи і практичне навчання	□	■	–	–	–
Розробка та обмін передовими практиками	–	–	–	–	□
Економічне зростання	–	□ (ціль)	■	Напрям дій 4 (ціль)	■
Освіта і навчання	■	■	■	–	■
Практичне навчання	–	□	■	–	■
Пряме комплексне бачення Використання з метою подолання загроз	–	■		Напрям дій 3	
Покращений рівень безпеки ІКТ-продуктів Обмін інформацією	–	■	■	–	■
Збір розвідданих про суб'єктів загроз	–	■	■	–	–
Міжнародна співпраця	Захід 6	■	■	Напрям дій 5	■
Законодавча/правова база	–	■	■	–	■
Санкціонування стандартів безпеки Потенціал виявлення загроз на національному рівні	Захід 2	□	–	–	■
Потенціал реагування на загрози/регулювання кризових ситуацій у сфері ІКТ	Захід 2	–	■	Напрям дій 2	■
Захист недоторканості особистого життя Поширення конвенції по кіберзлочинам	□	■	■	■	–
Захист другорядних об'єктів інфраструктури	–	□	□	□	□
Суспільно-державні об'єднання	–	■	■	■	■
Зниження ворожої мотивації і потенціалу	–	■			
Науково-дослідницька діяльність	Захід 3	■	■		■
Стійкість до порушень/зниження кількості загроз та вразливостей	Захід 4	■	□	Напрям дій 1	■
Захищені протоколи та ПЗ	■	–	■	–	–
Захищені джерела отримання продуктів	■	■	–	–	–
Самозахист уряду	■	■	□	■	■
Стратегічна рада кібербезпеки	–	Лише уряд	–	–	■
Аналіз загроз і вразливостей	Захід 1	■	■	–	■
Відслідковування злочинців та їх притягнення до відповідальності	Захід 5		■	■	–

Продовження табл. 2.7

Ключові заходи та напрями дій	**NLD**	**NZL**	**UGA**	**USA**	**ZAF**
Активні/динамічні заходи безпеки	–	–	–	■	–
Навчально-освітня кампанія/кампанія з інформаційної безпеки	–	■	■	Пріо-ритет 3	–
Політика, яка пристосовується до нових ризиків у сфері ІКТ Плани безперервної роботи і плани дій на випадок позаштатних ситуацій	–	–	■	□	–
Захист ключових об'єктів інфраструктури Криптографічний захист Контроль кіберзброї	–	■	□	–	■
Оборонні операції у сфері кібербезпеки/оперативні заходи і практичне навчання	■	–	–	■	
Розробка та обмін передовими практиками	–	–	■		■
Економічне зростання	(ціль)	–	■	□	■
Освіта і навчання	Напрям дій 6	–	■	□	□
Практичне навчання	■	■		□	■
Пряме комплексне бачення Використання з метою подолання загроз Покращений рівень безпеки ІКТ-продуктів	■	–	–	Пріорит ет 5	□
Обмін інформацією	■	–	■	■	–
Збір розвідданих про суб'єктів загроз	■	–	–	–	–
Міжнародна співпраця	■	□	■	Пріо-ритет 5	■
Законодавча/правова база	Аналіз		■	–	□
Санкціонування стандартів безпеки Потенціал виявлення загроз на національному рівні	–	–	–	–	–□
Потенціал реагування на загрози/регулювання кризових ситуацій у сфері ІКТ	Напрям дій 4	■	–	Пріо-ритет 1	■
Захист недоторканості особистого життя	■		–	–	–
Поширення конвенції по кіберзлочинам	■	Р		■	–
Захист другорядних об'єктів інфраструктури	□–	–	–	–	–
Громадські об'єднання	Напрям дій 1		■	–	■
Зниження ворожої мотивації і потенціалу	–	–	–	–	–
Науково-дослідницька діяльність	Напрям дій 6	■	■	■	□
Стійкість до порушень/зниження кількості загроз та вразливостей	Напрям дій 3	■	–	Пріо-ритет 2	
Захищені протоколи та ПЗ Захищені джерела отримання продуктів	–	–	–	■	■
Самозахист уряду	■	■	■	Пріо-ритет 4	■
Стратегічна рада кібербезпеки	Всі актори	–	–	–	–
Аналіз загроз і вразливостей	Напрям дій 2	–	–	■	■
Відслідковування злочинців та їх притягнення до відповідальності	Напрям дій 5	–	–	■	

Примітки: ■ *= конкретні заходи;* □ *непрямо вказані заходи; - відсутність інформації*

Наприклад, Японія розглядає безпеку IPv6, кібербезпеку побутової, яка відіграє активну роль у інтелектуальних енергосистемах. Говорячи про зміст запланованих заходів інших країн звернемо увагу, що всі держави (окрім Уганди) прямо зазначають необхідність захисту своїх ключових об'єктів інфраструктури (в том числі сервісів «електронного уряду»).

Як видно з табл. 2.7, п'ять держав (Канада, Німеччина, Великобританія, Нідерланди та США) прямо посилаються на свій військовий потенціал і плани у сфері кібербезпеки; французька НСК пропонує аналогічний підхід. У нідерландській НСК зазначено структури операцій в інформаційній сфері та заходи Міністерства оборони. Аналогічно, в німецькій НСК вказуються заплановані операції Німецьких Збройних Сил (Бундесверу) в інформаційній сфері.

Всі держави (окрім ПАР) зазначили, що вони планували розвиток програми обізнаності з кібербезпекою. Окрім суспільних програм, Німеччина, Нідерланди, ПАР, Великобританія і США розробляли програми з навчання з роботи у кіберпросторі для певних груп держслужбовців (наприклад, для службовців в оборонній сфері та спеціалістів, які працюють у правоохоронних органах).

Більшість держав (крім Іспанії, Уганди та Великобританії) зміцнюють заходи з регулювання кризових ситуацій і реагування у сфері ІКТ з метою вирішити серйозні проблеми в інформаційній сфері. Практичне навчання на національному і вузькоспеціалізованому рівні часто пов'язують з такою діяльністю, хоча згідно з табл. 2.7, лише десять держав вказують навчання на національному рівні у своїх НСК. Австралія, Канада, Франція і Великобританія зазначили важливість розвитку потенціалу виявлення кіберзагроз на національному рівні.

Всі держави (окрім Нової Зеландії) вказували міжнародну співпрацю у якості напряму дій або пріоритетного напряму. Нова Зеландія лише вказала своїх поточних партнерів з міжнародної безпеки та боротьби з кіберзлочинністю. Щоправда, у більшості НСК відсутнє детальне пояснення

передбачених дій з міжнародної співпраці, окрім обміну інформацією (наприклад, через національні Групи реагування на комп'ютерні надзвичайні ситуації).

Стосовно боротьби з міжнародної кіберзлочинністю Німеччина, Нідерланди та США висловили свої наміри поширити конвенцію по кіберзлочинам серед інших держав. Канада має намір ратифікувати договір про конвенцію по кіберзлочинам, а Великобританія вже зробила це у травні 2011 р.

Чотири держави (Франція, Німеччина, Іспанія та Великобританія) прямо зазначили необхідність захисту урядового апаратного і програмного забезпечення, яке є частиною ключових і стратегічно важливих об'єктів урядової інфраструктури.

7. Інституціоналізація НСК

Велика кількість країн з метою створення умов для максимально ефективної реалізації НСК створили відповідні організаційні структури, які не тільки відслідковують хід виконання НСК, а й вживають заходи, спрямовані на реалізацію її окремих положень. Так, Німеччина, Японія, Люксембург і Нідерланди задля реалізації НСК створили комітет і раду кібербезпеки. Японія також заснувала подібний міжвідомчий комітет. Німецька рада кібербезпеки є міжвідомчою радою, але зацікавленим сторонам у приватному секторі дозволено брати участь у якості спостерігачів. У голландській раді кібербезпеки є члени державних і приватних організацій, а також науково-дослідних інститутів/академічних організацій. Аналогічно, ПАР заснувала Національну консультаційну раду кібербезпеки (NCAC).

На функціональному рівні у своїх НСК більшість держав зазначають, що вони будуть зміцнювати свої національні Групи реагування на комп'ютерні надзвичайні ситуації (за наявності); інші планують створити національні Групи реагування на комп'ютерні надзвичайні ситуації. Декілька держав вказали на необхідність зміцнення потенціалу кіберполіції і

комп’ютерної криміналістики.

8. Співпраця з питань розробки міжнародної стратегії

У 2011 р. у США було розроблено міжнародну стратегію для кіберпростору, яка передбачала створення інформаційного середовища, яке «сповна використовує інновації та надасть приватним особам більше повноважень; встановить зв’язки між приватними особами і зміцнить громади; покращить уряди та зробить їх більш підзвітними; гарантує забезпечення основних свобод і підвисить рівень національної та міжнародної безпеки» [495, с. 8]. За допомогою такої стратегії США мала намір уніфікувати процес залучення декількох відомств разом з міжнародними партнерами для вирішення широкого діапазону проблем, пов’язаних із загальносвітовим кіберпростором. Міжнародна стратегія посилається на набір «ключових зобов’язань: основні свободи, недоторканість особистого життя громадян і вільний потік інформації» [495, с. 5] у США. Згідно з цією стратегією, США повинна відігравати передову роль у майбутньому загальносвітовому кіберпросторі. Там обговорюються три цілі національної політики: зміцнення партнерських відносин, оборона (стримування) і технічно-економічний розвиток (інновації). У розділі про пріоритети політики подано набір напрямів дій для реалізації органами публічної влади.

Зазначена стратегія була спрямована на розвиток відкритого, надійного і захищеного кіберпростору, який слугуватиме для «підтримки міжнародної торгівлі, зміцнення міжнародної безпеки та розвитку свободу слова та інновацій» [там само, с. 8]. Також там пропонувався набір керівних принципів або «правил кіберпростору». Він включав як традиційні принципи (підтримка основних свобод, приватної власності, недоторканості особистого життя, захист від злочинів та право на самооборону), так і нові інформаційні принципи (міжнародна інтероперабельність, стабільність мережі, надійний доступ, участь декількох зацікавлених сторін в управлінні та ретельна перевірка стану кібербезпеки).

У межах цієї Стратегії передбачалося, що інші держави та міжнародні зацікавлені сторони повинні узгодити власні стратегії кібербезпеки для ефективного розвитку загальносвітового кіберпростору. Але такого узгодження досі не відбулося. Як і підписання такого документу в цілому.

Між тим, на основі аналізу наведених НСК можна запропонувати наступну структуру НСК, яка може стати основою як для національних, так і для міжнародних документів з цієї проблематики.

1. Резюме.
2. Вступ.
3. Стратегічна візії кібербезпеки
4. Зв’язок НСК з іншими стратегіями (національними і міжнародними) та існуючою правовою базою.
5. Керівні принципи.
6. Пріоритетні напрями діяльності у сфері кібербезпеки (бажано 1-4).
7. Короткий опис тактичних напрямів дій.
8. Глосарій (на основі міжнародного узгодженого набору визначень).
9. Додатки, що включатимуть передбачені функціональні заходи, визначені за допомогою SMART-підходу.

Залежно від цільової аудиторії та національних традицій, розділи НСК можуть містити описи інцидентів, статистику та супутні цитати ключових політичних діячів та лідерів індустрії. Це дозволяє підвищити рівень підтримки населення та підкреслити важливість питання. Якщо держава вирішила включити оцінку загроз та ризиків в SWOT-аналіз, його можна розмістити або між вступом та стратегічною візією кібербезпеки або у якості окремого додатку.

Щодо висновків. Проведений аналіз НСК 14 країн дозволив виявити основні відмінності між ними, залежно від обраних пріоритетів: національна економіка (економічний підхід), національна безпека або оборона (державницький підхід). При цьому показано, що у більшості НСК зв’язки та існуючою національною та міжнародною політикою (наприклад, стратегією

національного захисту ключових об’єктів інфраструктури, європейською установкою по електронним засобам комунікації і політикою національної політики) прописані нечітко.

Лише вісім держав дали визначення поняттю «кібербезпеки». Інші десять держав або роблять це описово у НСК або дають загальне розуміння. Це може призводити до непорозумінь на національному та міжнародному рівнях. Оскільки державам бракує узгодженої термінології, пов’язаної з кіберпростором, це може призводити до затримки зі спільним визначенням міжнародних загроз у кіберпросторі. Більш того, держави можуть по-різному розуміти сферу, яку повинна охоплювати кібербезпека: лише системи, підключені до Інтернету, чи всі ІКТ. Перший підхід, на нашу думку, є обмеженим, оскільки держави, зосереджені на Інтернет-безпеці несвідомо нехтують захистом ІКТ, які (ще) не підключено до Інтернету, але які є частиною інших публічних мереж (наприклад, системи управління процесами у ключових об’єктах інфраструктури та об’єктах інфраструктури другорядного значення, а також медичні системи).

У своїх НСК всі держави вказують на міжнародні загрози та ризики у кіберпросторі. Між тим, щодо опису детальних планів дій з «міжнародної співпраці» більшість розглянутих НСК представляються доволі слабкими. Міжнародні аспекти такі як узгодження між різними країнами, спільне прискорення заходів з міжнародного реагування на кіберзлочини та інші порушення, відслідковування кіберзлочинців не входять до пріоритетних завдань значної кількості країн. Більшості НСК також бракує динамічного підходу до (технологічних) кіберзагроз та викликів у кіберпросторі.

У той же час, у більшості НСК визнається потреба залучення до її реалізації широких верств населення: громадян, компаній, публічного сектору та уряду. Щоправда, комплекси заходів, спрямованих на громадян, часто обмежуються навчальними кампаніями і уроками інформаційної безпеки в школах.

Комплексну програму, яка охоплює громадян та національні

інструменти кібербезпеки, було впроваджено лише в Австралії. Це також свідчить про те, що більшість держав недооцінюють ризик втрати довіри громадськості до ІКТ, що, у свою чергу, може призвести до серйозних затримок у економічному розвитку та реалізації планів електронного уряду. Саме це, на наш погляд, слід враховувати під час розробки та реалізації національної стратегії кібербезпеки України.

Висновки до другого розділу

Аналіз і узагальнення сучасних тенденцій і підходів до забезпечення кібербезпеки у публічному секторі дали можливість зробити такі висновки:

1. З’ясовано, що проблема зростання кількості кібератак на мережі та ускладнення їх характеру робить питання кібербезпеки все більш актуальнішим. Нові агресивніші форми кіберактивності та поява неурядових акторів у якості активних учасників процесів визначення внутрішньої та зовнішньої політики викликають численні запитання про майбутнє публічного сектору з точки зору забезпечення національного суверенітету та незалежності. Широкий діапазон потенційних загроз створює серйозні виклики існуючим міжнародним структурам, які часто не встигають за кіберпростором, що динамічно розвивається. Водночас, політика, яка націлена проти різних загроз у кіберпросторі, зазвичай розвивається ізольовано, що призводить до невідповідностей та відсутності узгодженості рішень, що ухвалюються окремими урядами. Отже, глобальним кіберзагрозам протиставляються локальні рішення, які часто не встигають за технологіями та тенденціями розвитку кіберзлочинності. Таким чином, постає питання визначення цих тенденцій, оцінка їх значення для окремих держав, а також розробка конкретних пропозицій щодо системного протистояння цим загрозам.

2. Встановлено, що у міжнародних наукових та політичних колах протягом останніх років сформувалась певна спільна думка щодо наступних

позицій. По-перше, всі (більшість держав та їх громадян) згодні, що життєдіяльність людства залежить від мережі, а інформаційні технології – це ключ до подальшого соціального та економічного розвитку. По-друге, на практиці це перетікає у зростаюче визнання того, що залежність життя у XXI сторіччі від інформаційної інфраструктури робить всіх (як окремих громадян, так і різноманітні установи, організації, підприємства і навіть цілі країни) надзвичайно вразливими до кіберзагроз. По-третє, потенційні загрози є досить серйозними, враховуючи залежність від мережі та відомих випадків вразливості кіберпростору, проте наразі сучасні державі не готові боротися з кіберзагрозами; атаки трапляються все частіше, а наслідки все триваліші. По-четверте, згідно з дослідженнями конкретних випадків та висновками, всі держави вразливі до переворотів, програми у сфері атомної енергетики вразливі до кібератак, а витоки інформації та революції через «Facebook» можуть нашкодити державам та дипломатичним відносинам між ними. Необхідно вживати певних заходів для того, щоб цифрове життя та інтереси стали безпечнішими. Визнання характеру та масштабу проблеми – це перший крок до її вирішення у майбутньому. По-п’яте, кіберпростір являє собою «справжню», відносно нову сферу взаємодії (як місцевої, так і міжнародної), яка є такою ж важливою, як і взаємодія у повітрі, на морі, на суші та в космосі. Кіберпростір заслуговує на той же рівень взаємодії, захисту і уваги, як і будь-яка інша сфера.

3. Визначено, що серйозним викликом для національних урядів є обмежена кількість ресурсів. З одного боку, варто визнати, що витрати на кібербезпеку у національних бюджетах щороку зростають. З іншого боку – кібербезпека коштує достатньо дорого, а враховуючи, що наразі бюджети на національну оборону підлягають безперервному перегляду, можливості для гідного протистояння кіберзагрозам постійно зменшуються. Таким чином, обґрунтування виділення ресурсів на кібербезпеку, що зазвичай сприймається більшістю науковців та політиків як боротьба з гіпотетичною загрозою, (враховуючи обмежену кількість точних даних про конкретні

результати інвестицій у цю сферу) – представляється достатньо складним завданням. Ускладнює ситуацію і те, що зазвичай через недостатню прозорість уряди і приватні компанії не бажають розкривати всю інформацію про атаки на їх активи. Таким чином, спільна проблема публічного та приватного секторів полягає у пошуку інвестицій, необхідних для покращення стандартів безпеки.

4. З'ясовано, що у відповідь на наявні загрози держави у всьому світі розробляють стратегії кібербезпеки, зазвичай – шляхом створення певного національного правового акту або програми для реагування на кіберзагрози та захисту найважливіших мереж. Однак пріоритети стратегій національної безпеки різних держав відрізняються. Деякі держави мають чітке уявлення про кіберсередовище та його головні референтні об'єкти, такі як критична інфраструктура, і, відповідно, сформували комплексний підхід до сприйняття проблем, що становлять загрозу для кібербезпеки та національної безпеки, та визначили найважливіші джерела цих загроз. Унаслідок цього, ключовою умовою для реалізації ефективних стратегій кібербезпеки у цих країнах є призначення державних відомств відповідальними за управління кібербезпекою. З іншого боку, держави, в яких переважає цивільний підхід до кібербезпеки, зосереджуються переважно на боротьбі з кіберзлочинністю. Потенційні джерела загроз кіберзлочинності не визначені чітко і пов'язані, переважно, з приватною власністю і належним функціонуванням сектору економіки. Але при цьому, як показує аналіз, стратегії кібербезпеки більшості держав зосереджують увагу на п'яти основних сферах: 1) військові кібероперації; 2) розвідка і контррозвідка; 3) боротьба з кіберзлочинністю; 4) захист критичної інфраструктури та врегулювання кризових ситуацій; 5) кібердипломатія та управління Інтернетом.

5. Було визначено дві парадигми, що стосуються забезпечення кібербезпеки у публічному секторі. Першою є так звана *державницька* парадигма, яка відображає традиційну роль держави в захисті кордонів та забезпеченні верховенства права У межах цієї парадигми кібербезпека

вважається фундаментальним фактором воєнної та економічної безпеки держави, і тому до неї застосовуються традиційні аргументи національної безпеки, що базуються на захисті батьківщини. Інакше кажучи, цей підхід підкреслює зв'язок між захистом критичної інфраструктури і тих державних та приватних систем, що є важливими для функціонування держави. Державницька парадигма відноситься до традиційного підходу до управління та запобігання ризикам з кіберпростору у спосіб, що може спричинити зростання впливу військових сил у сфері стратегій кібербезпеки. Другою є *економічна* парадигма, яка відображає зростання впливу інтернету на економічний добробут держави. Тим часом як державницька парадигма національної безпеки виключає з процесів формування стратегій кіберпростору усі сектори, крім військового, економічна парадигма наголошує на важливості участі інших секторів та відомств у процесі формування стратегій кібербезпеки. Економічна парадигма наголошує на децентралізованому підході в групах відомств та суб'єктів, відповідальних за управління кібербезпекою. Згідно з цим підходом тягар вжиття заходів щодо захисту систем розподіляється між окремими особами, надавачами послуг (провайдерами) та керівництвом держави.

РОЗДІЛ 3
ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ПУБЛІЧНОМУ СЕКТОРІ

3.1. Забезпечення кібербезпеки у середовищі Gov 2.0

Електронний уряд, соціальні мережі і Web 2.0 / Gov 2.0 (і, що важливо, все, що прийде після Gov 2.0) стали сьогоднішньої реальністю, і організації публічного сектора на всіх рівнях повинні думати про те, як їх адаптувати, а не як з ними боротися.

Хоча в даному параграфі особлива увага приділяється політиці кібербезпеки, пов'язаної з соціальними мережами і впровадженням Gov 2.0 в публічному секторі, у зв'язку зі сказаним хотілося б згадати те, що було відзначено Федеральною Радою IT-директорів США про ризики, пов'язані із соціальними мережами (курсив наш):

«Рішення використовувати технологію соціальних мереж - це рішення, засноване на ризику, а не рішення, засноване на технології. Подібне рішення має бути прийнято на основі переконливого економічного обґрунтування, підтриманого на відповідному рівні для кожного департаменту або агентства, враховуючи їх місію, загрози, технічні можливості і потенційні вигоди. *Завдання IT-організації повинне полягати не у тому, щоб сказати «Ні» веб-сайтам соціальних мереж і повністю їх заблокувати, а у тому, щоб сказати «Так, слідуючи вказівкам по безпеці» з ефективними і належними засобами забезпечення безпеки і конфіденційності.* Рішення про дозвіл доступу до веб-сайтів соціальних мереж є бізнес-рішенням і ґрунтується на процесі управління ризиками, зробленому командою менеджерів при участі всіх гравців....Використання соціальних мереж і невід'ємні проблеми кібербезпеки створюють складності, які обумовлюють додаткові уразливості організаційної інфраструктури, появу додаткових загроз, які потребують оновлення елементів управління даною організацією» [275, с. 6].

Нижче ми зосередимо увагу на питаннях політики в сфері кібербезпеки, пов'язаних, зокрема, із зусиллями публічних організацій на центральному і на місцевому рівні з підвищенням прозорості своєї діяльності за рахунок використання інструментів Web 2.0 (Gov 2.0) і реалізації ініціатив відкритих даних / відкритого уряду. При цьому ми припускаємо, що практично всі публічні організації вже забезпечили деякий базовий рівень мережевої безпеки, запобігання втрати даних, антивірусного захисту, виявлення вторгнень тощо, і не будемо вдаватися в подробиці по цим аспектам кібербезпеки.

Не підлягає сумніву, що інтеграція цифрового світу в повсякденне життя громадян привела до збільшення їх попиту як користувачів на прозорість публічного управління, доступ до інформації та її доступність, а також на можливість отримання зворотного зв'язку з органами влади та іншими публічними організаціями. Органи влади багатьох країн за останні десять років стали активними учасниками так званого «цифрового руху», який згодом назвали «уряд 2.0» або просто «Gov 2.0», і який було охарактеризовано в 2010 році Марком Дре з O'Reilly Radar, Інтернет-сайту новин та інформації, присвяченого новим технологіям, таким чином:

«Це означає зміну статус-кво органів влади та публічного управління різними способами, але не обов'язково обмежуючись: інноваціями з боку органів влади, прозорістю процесів в них, співпрацею між ними і участю громадян. В цілому, його впровадження призведе до величезної трансформації публічного управління на будь-якому рівні» [299].

Однак по мірі того, як все більше публічних організацій намагаються виправдати ці зростаючі очікування перетворення публічного управління, вони повинні вирішувати важливі питання своєї внутрішньої політики, особливо ті, що стосуються забезпечення безпеки загальнодоступних онлайн-даних й інформації, і все частіше організовувати тісну взаємодію між різними посадовими особами і співробітниками, а також з представниками громадськості. При цьому їм потрібно переступити якийсь поріг і перестати

використовувати загальну загрозу безпеки і конфіденційності в якості причини, щоб нічого не робити і не впроваджувати інновації.

Одним з ключових питань політики кібербезпеки, що стоять перед публічними чиновниками при розгляді рішень про те, як краще за все впровадити соціальні мережі в діяльність публічних організацій, є питання забезпечення належного балансу між управлінням ризиками і створенням дійсно відкритого уряду. Це не дивно, оскільки існує природне протиріччя між характеристиками відкритого уряду, – відкритими даними, відкритим доступом, прозорістю і підзвітністю, – і проблемами забезпечення безпеки.

Досить багато керівників відповідних підрозділів в органах влади вважають саме забезпечення кібербезпеки одним зі своїх головних завдань. Тим не менше, вони також відчувають зростаючий тиск з усіх сторін щодо в впровадження нових і більш ефективних послуг електронного уряду, розробки придатних для використання відкритих ресурсів даних та в цілому підтримки більш прозорого процесу прийняття рішень і комунікації, включаючи реалізацію активних ініціатив в соціальних мережах. Такий тиск особливо сильно присутній на місцевому рівні, де громадяни щодня взаємодіють з різними публічними організаціями, зокрема, з місцевими органами влади і їх різними підрозділами, що відповідальні за ключові публічні послуги, включаючи водопостачання та енергетику, громадський транспорт; з місцевими та регіональними агентствами з планування і розвитку спільнот; з екологічними агентствами; з навчальними закладами та багатьма іншими. У зв’язку з цим тиском як співробітники підрозділів з надання послуг й інформаційних технологій, так і посадові особи змушені буквально щодня боротися за те, щоб врівноважити, з одного боку, прагнення до все більшого доступу до публічної інформації, налагодження реального діалогу з громадянами і виборцями, і, з іншого боку, мінімізацію загроз приватного життя і безпеки. Розвиток Gov 2.0 підвищив ставки по обидві сторони цього балансу.

Кібербезпеку в широкому сенсі можна визначити як перешкоду

вразливості комп’ютерних систем, а також веб-сайтів в Інтернеті, по відношенню до несанкціонованого доступу чи атак, або як заходи політики, прийняті для їх захисту. Ризики кібербезпеки в Gov 2.0 також не можуть бути сфокусовані на одному типі або категорії проблем. Gov 2.0 / Web 2.0 включає в себе ряд факторів, в тому числі людські дії, проблеми, пов’язані з інфраструктурою, соціальні очікування і навіть перехід на кілька платформ і інтерфейсів.

Особливо в соціальних мережах найбільш реальною загрозою безпеки може бути ненавмисне розкриття потенційно компрометуючої інформації або непублічних даних недбалими публічними службовцями. У той же час, більша частина привабливості соціальних мереж полягає в їх здатності «пов’язувати» велику кількість людей в режимі реального часу. Тому в режимі реального часу Gov 2.0 надає великі можливості, в тому числі можливість інформувати учасників про різні деталі по мірі того, як відбуваються події, і надавати відкриті канали, які можуть негайно з’єднати різних акторів. Однак взаємодія в реальному часі також може не давати достатньо часу і концентрації зусиль для надання правильних відповідей, і збільшує ймовірність того, що публічні службовці можуть надати інформацію, яка ще не була перевірена, відповідно, може завдати шкоди безпеці.

Крім того, експонентне щоденне зростання соціальних мереж, сервісів і додатків надає численні нові потенційні точки входу в комп’ютерні мережі. Це одна з найбільш основних і очевидних загроз, яку не можна ігнорувати. Так, фактично всі мобільні телефони, вироблені за останні 10 років, мають технологію GPS (Global Positioning System). Виходячи з цього більшість смартфонів мають можливість передавати геотеги, які надають координати широти і довготи телефону і, отже, показують місце, де знаходиться користувач телефону. Це дозволяє, наприклад, службам екстреної допомоги в надзвичайних ситуаціях знаходити постраждалих в межах 100 метрів від їх фактичного місця розташування.

Ті ж функції реалізуються при вході зі смартфонів в соціальні мережі. Хоча в популярних соціальних мережах Twitter і Facebook передбачені заходи, що дозволяють уникнути публікації геотегів користувачами в разі їх небажання робити це, а в більшості смартфонів передбачена можливість відключення цих налаштувань. Сайти соціальних мереж, спеціально присвячені обміну фотографіями, такі як Flickr і Picasa, організовані в цьому сенсі ще краще, пропонуючи варіанти геотегінгу, але не включаючи їх автоматично.

Тим не менше, одним з основних комбінованих переваг мобільних технологій і соціальних мереж є обмін інформацією про географічне розташування. Це часто обговорюється, перш за все, як проблема конфіденційності в Інтернеті, але в контексті місцевих органів влади це може представляти дуже реальну проблему кібербезпеки, оскільки робить доступним інформацію про місцезнаходження ключових суспільних активів, таких як електростанції та інша важлива інфраструктура, дані про громадський транспорт, переміщення посадових осіб, схеми доступу до публічних організацій тощо.

Це може стати також і потенційною проблемою, оскільки соціальні мережі все частіше використовуються для спільної роботи в організаціях або для розподілених комунікацій і роботи. Деякі нові публічні послуги електронного уряду фактично побудовані навколо цього. Такі служби, як, наприклад, See-Click-Fix, заохочують «активне громадянство», пропонуючи громадянам різні платформи для повідомлень про різноманітні проблеми, включаючи можливість використання для цього мобільних пристроїв і завантаження фотографій. Першими з подібними проблемами стали боротися військові, оскільки багато військовослужбовців, особливо молоді, активно використовували соціальні мережі для спілкування з друзями і сім’єю, не відключаючи при цьому геотегінг, який є процесом додавання географічної ідентифікації до фотографій, відео, веб-сайтів і SMS-повідомлень. Це еквівалентно додаванню 10-значної координатної сітки до усього, що ви

публікуєте в Інтернеті.

Велика сфера уразливості кібербезпеки обертається навколо того, що відомо як «соціальна інженерія». За своєю суттю соціальна інженерія як концепція кібербезпеки включає в себе використання людського елемента довіри, який лежить в основі соціальних мереж. Це особливо проблематично для публічних організацій, оскільки все більше високопоставлені публічні діячі, – виборні посадові особи, міські керівники, члени комісій, генеральні менеджери, співробітники по зв'язках з громадськістю та ін., – використовують соціальні мережі для безпосереднього спілкування і обміну інформацією з громадськістю, часто в режимі реального часу.

Все це призвело до активного розвитку так званого «прослуховування» соціальних мереж. Для маркетингу, брендингу та зв'язків з громадськістю в приватному секторі мета такого прослуховування полягає в колективній оцінці того, що споживачі говорять про ті чи інші продукти, події, конкретні компанії тощо. Будучи обізнаними щодо цих «трендових» розмов, компанії можуть намагатися активно направляти і формувати їх, стимулюючи позитивні по відношенню до себе тенденції і намагаючись пом'якшити негативні. Це все ще залишається швидше мистецтвом, аніж наукою, але розвиток інструментів інтелектуального аналізу даних і бізнес-аналітики, які дозволяють користувачам пов'язувати один з одним окремі дані й інформацію для прогнозного аналізу, створило широкі можливості також і для зловмисників. Ці інструменти можуть використовуватися, наприклад, для так званих «фішингових» атак або для формування широких баз знань про суспільні об'єкти та інфраструктури, внутрішню операційну діяльність органів влади, їх плани і стратегії тощо.

Фішинг-шахрайство стало зростаючою проблемою в Інтернеті: мало хто не стикався із ситуацією, коли намагаються змусити клацнути по посиланню на якийсь сайт для перевірки облікової записи, отримання спеціальної пропозиції, що робиться з метою отримання банківської або іншої фінансової інформації, такої як номери кредитних карт. Хоча багато з

цих фішингових атак межують з безглуздям і легко впізнавані навіть більшістю цифрових неофітів, багато стають все більш витонченими і виглядають дивно схожими на реальні облікові записи та сайти, під які маскуються спеціально зроблені сайти.

З появою соціальних мереж виникла і стала швидко поширюватися ще більш мерзенна афера, яка отримала назву «цільовий фішинг» («spear phishing»). Цільовий фішинг – це атака, націлена на конкретного користувача або групу користувачів. Він намагається обдурити користувача через виконання певної дії, наприклад, відкрити документ або клацнути посилання, що запускає атаку. В цьому випадку фішери покладаються на знання певної конкретної інформації про їхні цілі, такі як події, інтереси, плани поїздок, адреси, поточні проб леми і т. п., тому знаходження сайтів, на яких зареєстрована «жертва», і її бесіди в соціальних мережах стають скарбницею для пошуку цих критичних фрагментів інформації. Популярне використання скорочень URL-адрес у світі соціальних мереж підвищило ефективність фішингу, оскільки користувачі не можуть легко розпізнати модифіковану URL-адресу фірмового веб-сайту.

Веб-додатки також протягом тривалого часу представляють серйозну уразливість для публічних організацій, особливо в зв’язку зі зростанням послуг електронного уряду за останні п’ять-десять років. В контексті Gov 2.0 до цих проблем безпеки додалися дві нові: мобільні додатки і зростання числа відкритих конкурсів на розробку додатків з боку державних установ. Незважаючи на те, що для розробки додатків існують певні стандарти безпеки, такі як керівні принципи Open OWASP, їх відстеження і застосування в динамічному світі Gov 2.0 стає все важчим.

Практично всі прогнози у сфері високих технологій вказують на те, що мобільні підключення до Інтернету за допомогою смартфонів і планшетів все більше будуть витісняти комп’ютерні підключення. Так, Symantec, компанія по забезпеченню безпеки й інші представники даної галузі, вважають, що по мірі того, як мобільні телефони стають «розумнішими» і додаються нові

функції, додатки, доступ до даних і можливості підключення, вони відкривають абсолютно нові можливості для кіберзлочинців. Розробка мобільних додатків, – автономних додатків, зазвичай доступних для завантаження в «магазинах» онлайн-додатків, і мобільних веб-додатків, зазвичай доступних для всіх мобільних користувачів, – є однією з найбільш затребуваних сфер розробки додатків.

Можливості для послуг мобільного електронного уряду і мобільних веб-додатків практично безмежні. Те ж саме стосується і якості розробки мобільних додатків. У комерційному просторі провідні магазини додатків, такі як iTunes для додатків для iPhone і Google Play для додатків на базі Android, роблять скринінг додатків на функціональність, але, згідно з галузевим журналом *Wired,* зазвичай не оцінюють уразливості безпеки або шкідливість програм. Більш гнучкі мобільні веб-додатки, які не повинні поширюватися різними магазинами додатків і, отже, потенційно більш широко доступні, схильні до тих же вразливостей, що і веб-додатки і сервіси електронного уряду, але призводять до ще більшої складності щодо забезпечення безпеки через безліч мобільних телефонів і операційних систем на ринку. Зрозуміло, що моніторинг і управління цими розробками виходять за рамки компетенцій і можливостей IT-персоналу публічних організацій.

Вівек Кундрю, нинішній федеральний директор США по інформаційним технологіям, ще в 2008 році оголосив конкурс «Додатки для демократії», будучи в той час директором по технологіям в окрузі Колумбія. Проста ідея полягала в тому, щоб відкрити ключові набори даних уряду і інструменти для громадськості, і дозволити компаніям і приватним особам розробляти свої власні додатки електронного уряду для їх використання в органах влади [323].

Багато місцевих органів влади США наслідували його прикладу. Так, Нью-Йорк оголосив подібний конкурс «NYC BigApps», в Південній Каліфорнії місто Анахайм провело «Великий конкурс додатків в Анахаймі», а столичне транспортне управління округу Лос-Анджелес (Metro) оголосило

на початку 2011 року свій власний «конкурс розробників метро», присвячений транспортним веб-додаткам і мобільним додаткам, використовуючи набори даних Metro. Подібна практика швидко поширилася і в інших містах і країнах [363].

Хоча деякі з цих конкурсів, наприклад, пропоновані Metro, вказують в своїх правилах і рекомендаціях, що в додатках не повинно бути шкідливих програм, зазвичай ця умова спеціально не обговорюється, що знижує потенційну значимість цієї проблеми і не дає докладних відомостей про те, як додатки можуть бути перевіреними на наявність шкідливих програм. Слід визнати, що чим більше реалізується краудсорсінгових ініціатив Gov 2.0, тим більше ймовірність того, що вони можуть нести загрозу кібербезпеці публічного сектора. Потенціал для шкідливих програм, особливо вбудованих або впроваджуваних в такі «відкриті» додатки, являє собою явну вразливість, особливо якщо конкурси та створені в їх результаті додатки стають все більш популярними серед громадськості та громадських організацій.

Згідно з дослідженням, проведеним Інститутом людського капіталу (США) і компанією Saba, 66% всіх публічних організацій в США і ЄС в даний час використовують ті чи інші форми соціальних мереж. Зокрема, на місцевому рівні соціальні мережі використовуються для забезпечення зовнішніх взаємодій і як більш ефективний засіб залучення стейкхолдерів, особливо для зворотного зв'язку [360].

Symantec, світовий лідер у сфері безпеки, в своєму щорічному звіті про загрози кібербезпеці за 2019 рік стверджує, що зростаюче використання соціальних мереж органами влади підвищує ризик кібератак. У Symantec особливо відзначають, що використання скорочених URL-адрес – міра ефективності, при якій довгі URL-адреси скорочуються, особливо для мікроблогів, таких як Twitter, – є небезпечним, оскільки такі адреси маскують справжні посилання за ними. Symantec особливо наполягає, що подібна ситуація є небезпечною для органів влади на національному рівні і глобальних корпорацій, і назвала зростання цілеспрямованих і витончених

атак на них «кібервійною» [334].

У недавньому дослідженні, проведеному протягом 4 місяців Центром інформаційної безпеки штату Джорджія (2019 р.), у середньому кожен день виявлялося 130 примірників шкідливого ПЗ шляхом простого пошуку контенту по популярним, «актуальним» темам через Twitter, Google, Yahoo! та Bing [334].

Проте, однією з основних рушійних сил все більшого прийняття соціальних мереж в публічному секторі є простота їх використання в якості інструменту зовнішньої комунікації. Платформи Facebook, Twitter і блоги можуть надавати мережеві ідентифікатори, які можуть бути легко визначені і «лайкати» або «слідувати» потенційно великим числом учасників. У свою чергу, контрагенти через одні й ті ж канали можуть давати відповіді, що призводить до потенційно ефективного двостороннього каналу комунікації. Але соціальні медіа як зовнішній інструмент комунікації можуть бути проблематичними через проблем, які можуть виникнути через характер контенту в реальному часі, стислість, прийняту в спілкуванні, а також поділ на публічний / приватний і конфлікти, які може бути важко ідентифікувати, коли публічні службовці й офіційні особи використовують ці інструменти.

Наприклад, згідно з Social Media Today, новинним Інтернет-сайтом соціальних мереж, в Червоному Хресті стався інцидент, коли співробітник випадково написав особистий твіт в своєму офіційному аккаунті [466]. У Червоному Хресті змогли виправити цю помилку з гумором і перетворити потенційно незручну ситуацію на позитив, але такий приклад показує, наскільки легко можуть виникати помилки в спілкуванні, і при використанні інструментів відкритої комунікації, призначених для громадського споживання, можна випадково перетнути якісь «червоні лінії». Це особливо характерно, коли офіційні особи або публічні службовці мають легкодоступні офіційні облікові записи у Facebook або Twitter, в результаті чого вони в режимі реального часу висловлюють свою оцінну думку, яку не було ретельно продумано або сформульовано.

Соціальні мережі також дають додаткові можливості для внутрішньої співпраці через блоги, вікі та гібридні інтерфейси, які включають соціальні мережі. Ефективно використовувані соціальні мережі можуть надати цінні інструменти підвищення продуктивності й ефективності для співробітників, часто по дуже низькій ціні. Однак без належних керівництв моніторинг і навчання цим технологіям можуть відкрити ненавмисні порушення безпеки з боку співробітників або, що ще гірше, зловмисні порушення безпеки.

На доповнення до найбільш важливою лінії захисту, яка пов'язана з людським аспектом, зростає число технологічних інструментів і підходів, які в разі їх впровадження можуть забезпечити всеосяжну систему безпеки. Нижче наведено приблизний список, який був складений на підставі різних керівництв з безпеки як для публічних, так і для приватних організацій.

Фільтрація універсального локатора ресурсів (URL) та Інтернет-протоколу (IP).

Це досить проста технологія, яка блокує певні веб-сайти, частини веб-сайтів або IP-адреси, визначені користувачами або адміністраторами. Це допомагає захистити користувачів, які можуть бути перенаправлені на певні шкідливі сайти.

Крім того, на деяких сайтах соціальних мереж використання URL-фільтрів для блокування сторінок входу для всіх, крім співробітників, яким це потрібно за родом діяльності, дозволяє отримати доступ до загальнодоступної інформації, в той же час запобігаючи доступ до додатків і інструментів обміну повідомленнями, які можуть обходити контрольні заходи безпеки.

Фільтрація шкідливих програм по периметру мережі.

Ця технологія перевіряє трафік до його попадання в мережу об'єкта, щоб переконатися, що він не містить шкідливих програм і блокує будь-які виявлені шкідливі програми. Така фільтрація може бути реалізованою як частина комплексної структури скринінгу і виявлення несанкціонованих вторгнень.

Системи виявлення / запобігання вторгнень.

Ця технологія забезпечує моніторинг в реальному часі й аналіз мережевої активності на предмет можливих атак.

Запобігання втрати даних.

Ця технологія призначена для виявлення і запобігання несанкціонованого використання і передачі конфіденційної інформації. Її слід використовувати як на робочому столі комп'ютера, так і в веб-шлюзі для моніторингу та блокування вихідних конфіденційних даних. Причому зі зростанням використання мобільних даних ця технологія повинна йти в ногу з усім трафіком даних в мережі.

Модерування контенту.

При розміщенні аккаунта публічного суб'єкта в соціальній мережі необхідно запустити процес, який дозволив би хосту модерувати (тобто переглядати, приймати, відхиляти) контент, представлений на сайті соціальної мережі до його публікації (тобто зробити видимим для відвідувачів). Це допомагає хосту блокувати контент, що містить шкідливі посилання, або неприпустимий контент.

Інструменти попереднього перегляду скорочення URL.

Ці інструменти відображають фактичне значення URL-адрес, що маскується скороченими URL-адресами таких служб, як Google, TinyURL і Bit.ly. Попередній перегляд дозволяє користувачам приймати обґрунтовані рішення про посилання до натискання. Крім того, можна створити настроювані фірмові короткі URL-адреси, щоб підвищити легітимність контенту і зв'язати URL-адресу з інформацією про обмін джерелами.

Браузер з обмеженими привілеями.

Якщо ця функція доступна, вона забезпечує роботу браузера і його надбудов з мінімальним набором дозволів, що запобігають встановлення шкідливого коду.

Сервіси Web -репутації.

Ці сервіси перевіряють веб-сайти на наявність спаму, програм-

шпигунів, шахраїв і т.п., та використовують ці тести для оцінки безпеки, допомагаючи користувачам уникнути відвідування небезпечних сайтів. Щоб ця технологія була найбільш ефективною, вона повинна супроводжуватися навчанням кінцевих користувачів того, як інтерпретувати і використовувати рейтинги сайтів, які визначаються даними сервісами.

У цілому ж, враховуючи багато потенційних проблем кібербезпеки, у тому числі, зазначені вище, одним із способів, за допомогою яких органи влади можуть почати вирішувати ці проблеми, є розробка спеціальної політики, що стосується соціальних мереж. Політика щодо соціальних мереж повинна враховувати ряд факторів:

– в яких соціальних мережах повинні бути присутніми органи влади і офіційні особи;

– які технології можуть знадобитися для повноцінної участі в цих соціальних мережах ;

– яким стандартним керівництвам користувача повинні слідувати співробітники органів влади, і кому зі співробітників повинен бути наданий доступ до аккаунтів органів влади в соціальних мережах ;

– які необхідно вживати дії в разі виникнення проблем, будь то поширення дезінформації, несанкціоноване використання облікового запису або проблема, яка виникає в результаті використання тих чи інших технологій;

– який візуальний і текстовий брендинг повинен використовуватися, щоб гарантувати, що громадяни офіційно визнають такі аккаунти в соціальних мережах в якості офіційних каналів інформації.

Можливо, найбільш очевидним з наведеного вище списку, і особливо при обговоренні конкретних питань розробки політики, є те, що необхідно робити основний акцент на людський фактор.

У міру того, як все більше і більше соціальних технологій стають доступними, публічні організації повинні вирішити, як використовувати свої ресурси в цьому відношенні і як спілкуватися зі своєї конкретної аудиторією.

Деякі реалізації можуть бути безкоштовними або недорогими, але існує необхідність у фінансових та часових інвестиціях для створення і підтримки мережевих ідентифікаторів й інформаційних каналів. При цьому великі інвестиції вимагають збільшення уваги, необхідної для спостереження за різними каналами, тому слід розуміти, що саме найкращим чином приверне цільову аудиторію і чи є достатній персонал для належного підтримання функціонування таких каналів.

З огляду на людські ресурси та технології, необхідні для активної участі в соціальних мережах, – для того, щоб не тільки своєчасно поширювати інформацію, але і для взаємодії з користувачами, взаємодіючими з соціальними інструментами, – частина політики повинна включати визначення того, який персонал повинен нести відповідальність за таку взаємодію, і якою повинна бути структура, необхідна для розсилки інформації по каналах. Наприклад, в ситуаціях, коли потрібні відповіді в режимі реального часу, треба заздалегідь визначити, який порядок формулювання цих відповідей, хто саме розміщує відповідну інформацію в соціальних каналах, і наскільки і для кого ця інформація доступна. Наявність такої політики знижує ймовірність непорозуміння.

Крім того, соціальні технології на даний час можуть включати стороннє програмне забезпечення, яке забезпечує доступ до соціальних мереж через настільні додатки і мобільні пристрої. Це програмне забезпечення також може бути безкоштовним або недорогим, що підвищує продуктивність в цих каналах, але з додатковими технологіями зростає кількість можливих проблем безпеки з продуктами і зростає ймовірність помилок, особливо якщо ці інструменти дозволяють користувачам створювати кілька облікових записів, які можуть змішувати особисті та професійні думки й інтереси.

В кінцевому підсумку ряд проблем можна уникнути або зменшити, якщо співробітники публічного сектора будуть належним чином навчені тому, як вони повинні взаємодіяти з третіми особами по цих каналах.

Користувачі сучасних ІКТ часто є найслабшою ланкою в ланцюжку, оскільки окремі дії можуть управлятися, але ніколи не контролюватися повністю. Тому людська помилка і недбалість повинні бути очікуваним фактором при розгляді питання про запровадження будь-якої технології. Так, в опитуванні, в якому взяли участь більше ста технологічних, медійних і телекомунікаційних компаній, проведеному консалтинговою фірмою Deloitte в 2018 році, «людська помилка» була вказана 75% учасників в якості головного чинника загроз безпеки [486]. Однак, як показує практика, навчаючи співробітників, можна знизити деякі потенційні небезпеки. Крім того, шляхом розробки політики, яка включає в себе надання навчальних матеріалів і обов'язковість їх вивчення для співробітників, що працюють зі соціальними мережами, публічні організації та їх співробітники також підвищать обізнаність і розуміння своїх цілей за допомогою соціальних мереж, а також їх позитивні і негативні сторони в міру інтеграції їх використання в діяльності організації.

Говорячи про безпеку, звичайно ж слід враховувати і те, що сайти соціальних мереж стають об'єктами кіберзлочинців, оскільки вони можуть ефективно використовуватися для поширення шкідливого коду для широкої, аудиторії, яка нічого не підозрює. Згідно думки співробітників Websense Security Labs, провідного постачальника рішень веб-безпеки, сайти, які дозволяють створювати користувальницький контент, є одними з найбільш активних розповсюджувачів шкідливого контенту, такого як черв'яки, які можуть відключати мережі, або програми-шпигуни і реєстратори натискань клавіш, які можуть красти дані. Багато публікацій в блогах, чатах і на дошках оголошень є спамом або містять шкідливі посилання [513]. Як вже зазначалося вище, оскільки багато посилань на сайтах соціальних мереж представлені у вигляді скорочених або стислих URL-адрес, користувач не може визначити, куди ведуть ці посилання, що дозволяє злочинцям направляти користувача, який нічого не підозрює, на шкідливі сайти. Причому хибне почуття довіреної спільноти при відвідуванні сайтів

соціальних мереж збільшує ймовірність того, що користувач може стати жертвою такого типу загроз. Якщо співробітник використовує ресурси своєї організації для спілкування в соціальних мережах (наприклад, робочий ПК), ці ресурси мають підвищений ризик зараження.

У такій ситуації введення нових посад, таких як фахівець по цифровій інформації або фахівець по цифрових комунікаціях, є досить правильним рішенням. Надаючи людям повноваження по нагляду за реалізацією політики кібербезпеки і впровадженням веб-рішень, це також забезпечує чітке і публічне розуміння того, що в даній сфері потрібні стандарти і структура, і необхідно приймати рішення для того, щоб діяти відповідально.

Наявність відповідної політики та керівних принципів у сфері кібербезпеки також є позитивним сигналом для громадян, нагадуючи про основоположну природу Gov 2.0 як про рух до відкритої, прозорої та безпечної арени діяльності публічних організацій. Громадяни в світі Web 2.0 очікують інтеграції таких технологій в свої взаємодії з публічними структурами, але як і раніше існують основні проблеми конфіденційності та обміну інформацією. Надання керівництв і політик може пом’якшити такі побоювання і відкрити для обговорення додаткові потреби і очікування громадян щодо ступеня розвитку сфери ІКТ.

Подібно посібникам користувача для персоналу, тобто для внутрішнього користування, публічні комунікації також повинні мати свої власні керівні принципи, щоб гарантувати, що користувачі розуміють, куди направляється їх інформація, що очікується від її вмісту і яким чином цей вміст може бути видалено, показано або змінено. Рекомендації по загальнодоступним комунікаціям допомагають сформувати очікування, полегшують діалог і зменшують потенційні проблеми, які можуть виникнути в результаті видалення / зміни контенту. Слід також визначити правила в відношенні того, яким чином інформація надається для публічного доступу. Це особливо важливо, якщо вже існують норми і правила, пов’язані з публічною документацією, оскільки вони тепер повинні враховувати нові

технології і канали зв’язку.

Таким чином, можна констатувати, що за останній час загрози кібербезпеці в публічному секторі постійно зростають і стають більш складними, і все прогнози вказують на те, що в майбутньому подібна ситуація тільки погіршуватиметься. У публічному секторі ці ризики в деякому сенсі загрожують впровадженню соціальних мереж і Gov 2.0 у діяльність публічних організацій, які намагаються стати більш відкритими і прозорими.

Однак, незважаючи на загрози органи влади на всіх рівнях, і особливо місцеві органи влади, повинні продовжувати впроваджувати і сприяти розробці нових технологій і рішень Gov 2.0, щоб залишатися надійними постачальниками публічних послуг та інформації. Тим не менше, органи влади повинні робити це обережно, стратегічно, маючи відповідну політику, розробляючи необхідні керівні принципи, використовуючи відповідні технологічні інструменти та навчання персоналу для захисту від загроз кібербезпеки.

Частиною цього стратегічного підходу є прийняття чітких управлінських рішень щодо цінності конкретних інструментів та ініціатив Gov 2.0 / соціальних мереж. Оцінюючи потенційні ризики конкретних ініціатив або довгострокових стратегій, можна здійснити належне планування і виділити ресурси для їх реалізації і управління. На рисунку 3.1 представлена відповідна модель для такого роду оцінки.

Хоча реєстрація облікової записи в соціальній мережі та надання користувачам інформації (або запит зворотного зв’язку від них) можуть здатися простими і легкими, рішення публічної організації впроваджувати технології Web 2.0 викликає ряд ризиків і проблем. Відзначимо основні з них.

Високі ризики. Врешті-решт, дії людей – це найбільш великий ризик, який виникає в результаті впровадження технологій і рішень Gov 2.0.

Участь громадськості має підкріплюватися політикою, яка гарантує,

що публічні організації чітко формулюють обов'язки і відповідальність всіх акторів, і механізмами, які дозволяють відстежувати / видаляти контент.

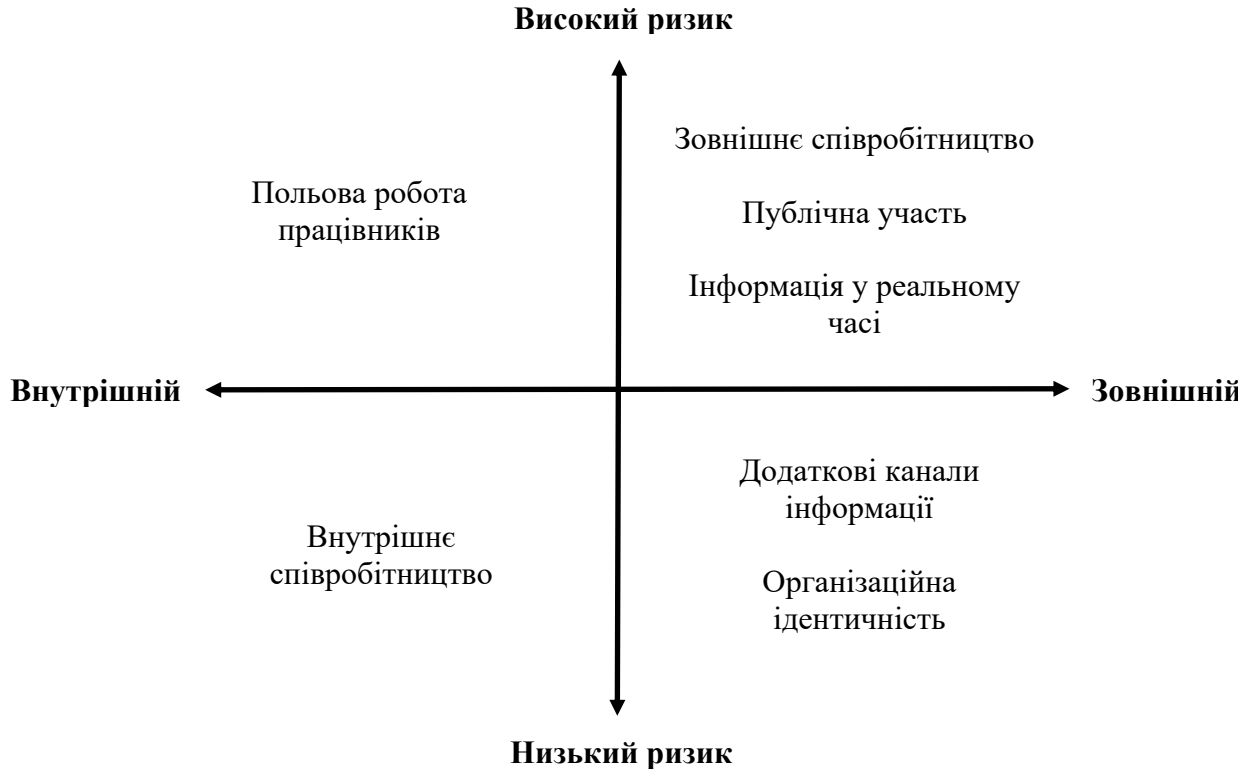

Рис. 3.1. Оцінка ризиків у Gov 2.0 / соціальних мережах

Зовнішнє співробітництво вимагає заходів безпеки для забезпечення того, щоб внесок громадськості адекватно відповідав потребам і бажанням агентств / організацій. Політики, які використовуються для забезпечення участі громадськості, повинні застосовуватися і тут, і те, як різні актори надають інформацію, має оцінюватися й аналізуватися на предмет всіх можливих ризиків і загроз безпеці.

Участь персоналу також має відповідати певним правилам: співробітники повинні розуміти, як вони повинні спілкуватися з громадськістю через соціальні канали. Інформація повинна бути чітко «позначена» для розміщення в загальнодоступних мережах, а її форма і зміст повинні забезпечувати необхідний контекст.

Інформація в реальному часі – це і добре, і погано. Можливість надавати людям актуальну інформацію дуже важлива, але в той же час ця інформація повинна регулярно відслідковуватися і оновлюватися. При цьому ризик того, що зміст оперативної інформації буде доступний навіть тоді, коли це не повинно бути, зростає.

Низькі ризики. Технології та стратегії Gov 2.0 з більш низькими ризиками часто є тими, в яких посилений контроль, перш ніж вони стають відкритими для громадськості:

Фірмовий стиль: від логотипів до угод про імена, фірмовий стиль організації повинен поширюватися по каналах Web 2.0, *перш* ніж він буде доступний для широкої публіки.

Додаткові канали зв'язку: в соціальній мережі існує безліч інструментів, і для Gov 2.0 необхідно приймати зважені рішення про те, які інструменти використовувати. Незважаючи на те, що підписка на облікові записи нічого не коштує або коштує дуже мало, ці канали вимагають наявність відповідного персоналу і витрат його часу, а також існує ризик вибору для комунікації тих каналів, які не будуть вигідні для організації.

Внутрішня спільна робота: Gov 2.0 відкриває безліч можливостей для внутрішньої спільної роботи і спілкування, але ця взаємодія пов'язана з потенційними ризиками, включаючи труднощі, які можуть виникнути при спробі управління багатьма внутрішніми каналами, а також зловживаннями з боку співробітників.

Слід зазначити, що, як і в разі будь-яких нових технологій, моделей робочих процесів і послуг, публічні організації, як правило, значно відстають від приватного сектора в їх впровадженні в свою діяльність. Це також відноситься і до соціальних мереж і Web 2.0.

Однак останніми роками все більше організацій публічного сектора по всьому світу, в тому числі і в Україні, демонструють прагнення прискорити впровадження цих технологій і стратегій та фактично перетворити їх на нову платформу, Gov 2.0, розроблену спеціально для потреб публічного сектора.

Місцеві органи влади можуть бути лідерами в цьому впровадженні, стаючи більш відкритими, прозорими і підзвітними, чого все більше вимагають від них громадяни. І хоча загрози кібербезпеці, нові й старі, завжди супроводжуватимуть нові технології, побоювання перед ними не повинно пригнічувати інновації, а скоріше стимулювати ефективну підготовку до їх безпечного використання, розробку відповідних заходів і нових технологій для захисту суспільного блага.

3.2. Формування глобального підходу до забезпечення кібербезпеки

Інформаційно-комунікаційні технології (ІКТ) трансформують сучасний спосіб життя завдяки глобальному доступу в реальному часі до майже необмеженої кількості інформації. У той же час ці інноваційні інструменти також створюють можливості для різних зловживань.

Як уже неодноразово зазначалося в попередніх розділах, кіберзагрози стали однією з найбільших глобальних проблем нашого часу. Створення постійних інформаційних зв'язків створює глобальну мережу відкритих каналів. Хоча вони приносять незліченні переваги в плані доступу до інформації, вони також призводять до тривожного росту кількості та масштабів кіберзагроз, кіберзлочинців і кібертерористів. Наприклад, згідно International Multistakeholder Partnership Against Cyber Threats (IMPACT), на даний час шкідливе ПЗ в будь-який момент часу зачіпає більше 12 мільйонів систем ІКТ у всьому світі [297].

Інтернет став невід'ємною частиною сучасного суспільства, просуваючи кінцевого користувача на передній край спілкування. Всі види інформації і думок доступні на різних мовах практично на будь-яку тему.

Труднощі з постійно зростаючою безліччю ресурсів полягає в тому, що вони ефективно сортують величезну кількість інформації, доступної в Інтернет. Яка частина цієї інформації є фактичною або навіть справжньою? Реальне занепокоєння пов'язане не тільки з поширенням неточної або такої,

що вводить в оману, інформації, але, перш за все, зі зловмисним контентом. Так, шахрайство і крадіжка існують в Інтернеті так само, як і в реальному світі. Якщо користувачі хочуть скористатися всіма перевагами Інтернету, то довіра до його інфраструктури має першорядне значення.

При цьому кіберзагрози, такі як шкідливе програмне забезпечення, стають надзвичайно складними. Інтернет вже давно перестав бути середовищем для невеликого числа фахівців. Зручне програмне забезпечення та інтерфейси дозволяють всім типам користувачів, включаючи дітей і новачків, легко взаємодіяти в режимі онлайн. Відповідно, кіберпростір містить «золоту жилу» цінної інформації і потенційних жертв, а складна інфраструктура Інтернету ускладнює пошук злочинців.

Але кіберзлочинці це не єдина загроза в Інтернеті. Уразливості ІКТ також поширюються на кібервійну, шпигунство і тероризм, які можуть представляти серйозну загрозу для критично важливою інформаційної інфраструктури.

Незважаючи на те, що багатьма державами вживаються відповідні заходи на національному рівні, кіберзагрози залишаються міжнародною проблемою. Перш за все, зловмисники успішно для себе використовують лазівки в правових нормах. Наприклад, різні закони, що стосуються спаму або фішингу, або закони, які стосуються особистості Інтернет-користувачів, дозволяють кіберзлочинцям ініціювати злочинні дії в тих місцях, де їх неможливо виявити або притягнути до відповідальності. У поєднанні з відсутністю міжнародних організаційних структур і організацій національного рівня, які можуть координувати дії на міжнародному рівні (таких як групи реагування на комп’ютерні інциденти, CIRT), існує справжня проблема в реагуванні на кіберзагрози.

Це без урахування сталого розвитку та складності таких загроз, а також вразливостей в програмному забезпеченні, а останнім часом і в апаратних додатках. З феноменальним зростанням мобільних ІКТ і новими тенденціями, такими як хмарні рішення і віртуалізація, все більш ймовірно,

що кіберзагрози поширяться на нові рівні. Наприклад, ще в 2007 році Міжнародний союз електрозв'язку зазначив, що зростання спаму стало більш серйозною загрозою кібербезпеки, виступаючи в якості платформи для інших протиправних дій, таких як фішинг і злам.

Тому кібербезпека є однією з найбільш важливих проблем епохи інформації. Вона формує наріжний камінь сучасного інформаційного суспільства і так званого «пов'язаного» світу. Це глобальна проблема, яка вимагає дійсно глобального підходу. Через наявність швидкісного зв'язку і численних мереж кіберзлочинцям і кібертерористам не потрібно знаходитися десь поруч з місцем злочину. Тому міжнародне співробітництво – єдина правильна відповідь на кіберзагрози, яку не можна відкладати.

Сила віртуального світу збільшується з кожним днем. Але, на жаль, немає нічого віртуального у небезпеках, які супроводжують сучасні комунікаційні технології. Інтернет може відкрити нам нові можливості, але він також піддає нас пасткам і небезпекам кіберзагроз.

Подібно до багатьох викликів, які стоять сьогодні перед нашою планетою, ці небезпеки не знають кордонів. Так само, як віруси можуть поширюватися з регіону в регіон (що підтвердила остання пандемія COVID-19), комп'ютерні віруси поширюються з комп'ютера на комп'ютер незалежно від їх фізичного розташування.

Необхідність у створенні глобальних рамок для захисту кіберпростору також підкріплюється зростаючим розумінням того, що ІКТ відіграють вирішальну роль в процесі розвитку. За деякими оцінками до 2025 року в кіберпросторі будуть підключені понад п'ять мільярдів чоловік, яким необхідно створити безпечне і надійне кіберсередовище, яке сприятиме соціально-економічному зростанню.

З огляду на глобальний характер кіберзагроз, цю проблему не може вирішити жодна національна держава самотужки. Тому необхідно створювати відповідні глобальні структури, що визначають міжнародні принципи кібербезпеки, і дозволяють забезпечувати швидку координацію

між країнами на регіональному і глобальному рівнях.

У 2000 році світові лідери зібралися в Організації Об'єднаних Націй в Нью-Йорку і пообіцяли собі і своїм країнам досягти восьми цілей в галузі розвитку, сформульованих в Декларації тисячоліття [501], від скорочення масштабів крайньої бідності до припинення поширення ВІЛ/СНІДу та забезпечення загальної початкової освіти. Цілі, викладені в Декларації, стимулювали безпрецедентні зусилля по задоволенню потреб найбідніших людей в світі. Наприклад, мета 8 у сфері розвитку, сформульована в Декларації, передбачає глобальне партнерство, яке ставить перед світовими лідерами завдання співпрацювати з приватним сектором, з тим щоб надавати переваги інформаційних і комунікаційних технологій тим, хто має до них найменший доступ.

З огляду на взаємозалежність, створювану ІКТ, всі держави-члени ООН повинні взяти на себе зобов'язання забезпечити досягнення мети 8 [499], але при цьому забезпечувати необхідний рівень кібербезпеки, оскільки процес розвитку програм та послуг електронної охорони здоров'я, електронної освіти, електронної комерції та електронного уряду буде успішним тільки в тому випадку, якщо інфраструктура ІКТ, яка для цього використовується, буде безпечною.

Перші кроки у вирішенні цього завдання були запропоновані Міжнародним союзом електрозв'язку (МСЕ), який створив Глобальний порядок денний у сфері кібербезпеки (The Global Cybersecurity Agenda – GCA) [297]. На наш погляд, даний порядок денний може служити основою для створення або вдосконалення національних стратегій кібербезпеки, в тому числі і в Україні, тому нижче в даному параграфі докладно проаналізуємо його.

Однак перш хотілося б сказати кілька слів про МСЕ (тут і надалі інформацію про дії та рішення МСЕ взято з офіційного сайту цієї організації [376]). МСЕ займається питаннями безпеки з моменту свого створення в 1865 році: від винаходу телеграфу до епохи радіо і телебачення і до розгортання

супутникових й Інтернет-технологій. Мета, як і раніше полягає у встановленні партнерських відносин і підтримці проектів, метою яких є створення безпечного і надійного середовища, оскільки доступ до зв'язку марний, якщо при цьому не може бути гарантована безпека.

Діяльність МСЕ виходить з визнання того, що безпека інформації та технологій є найважливішим пріоритетом для міжнародної спільноти. Кіберзагрози носять глобальний характер; отже, рішення також повинні бути глобальними. Вкрай важливо, щоб всі країни прийшли до спільного розуміння щодо кібербезпеки, а саме забезпечення захисту від несанкціонованого доступу, маніпулювання і знищення критично важливих ресурсів. Однак будь-яка успішна глобальна стратегія повинна починатися з визначення вже існуючих національних і регіональних ініціатив, з тим щоб знайти точки дотику, які підвищать ймовірність того, що міжнародна стратегія зможе ефективно залучити всіх відповідних учасників і встановити чіткі пріоритети для дій.

Заснований на принципі міжнародного співробітництва між публічним і приватним сектором, МСЕ є унікальний глобальний форум для дій зі сприяння кібербезпеці та боротьби з кіберзлочинністю. Для забезпечення того, щоб переваги інформаційного суспільства поширювалися на всіх громадян світу, МСЕ було запропоновано організувати від імені Організації Об'єднаних Націй Всесвітню зустріч на вищому рівні з питань інформаційного суспільства, що складалась з двох частин – у Женеві (2003 рік) і Тунісі (2005). Саме під час цієї зустрічі лідери і уряди увійшли в МСЕ, щоб очолити координацію міжнародних зусиль у сфері кібербезпеки. Україна брала активну участь в цій зустрічі.

На даній Зустрічі було визначено основну мету: побудова глобального інформаційного суспільства, в якому довіра і безпека при використанні ІКТ є нормою на благо людства. З цієї причини 17 травня 2007 року генеральний секретар МСЕ запустив згаданий вище Глобальний порядок денний у сфері кібербезпеки (GCA), щоб забезпечити структуру, в рамках якої можна

координувати і вирішувати міжнародну відповідь на зростаючі виклики кібербезпеки. GCA є міжнародною основою співпраці і прагне залучити всі зацікавлені сторони, включаючи державні органи, приватний сектор, громадянське суспільство та міжнародні організації, в узгоджені зусилля по зміцненню довіри і безпеки в інформаційному суспільстві. GCA будується на п’яти стовпах зі сімома стратегічними цілями.

П’ять стовпів:

1. Правові заходи.

2. Технічні та процедурні заходи.

3. Організаційні структури.

4. Нарощування потенціалу.

5. Міжнародне співробітництво [376].

Правові, технічні та процедурні заходи й організаційні структури повинні бути зроблені / створені на національному рівні, а також узгоджені на міжнародному рівні в такий спосіб:

– національні закони повинні прийматися там, де їх ще немає, а існуючі закони, а також регіональні та міжнародні угоди повинні ґрунтуватися на загальному розумінні того, що являють собою загрози кібербезпеки;

– технічні рішення повинні бути визначені та розроблені з урахуванням загальноприйнятих стандартів, спрямованих на забезпечення базових показників безпеки апаратного та програмного забезпечення, які можуть бути прийняті виробниками, постачальниками і кінцевими користувачами;

– необхідно на національному рівні створити відповідні організаційні структури, такі як центри та групи координації та реагування (наприклад, групи реагування на комп’ютерні інциденти), щоб швидко реагувати на кібератаки і координувати дії зі своїми колегами на міжнародному рівні.

Останні два стовпи перетинають всі сфери і спрямовані на розробку стратегій, що забезпечують наявність необхідного потенціалу, що дозволяє

фахівцям з ІТ-безпеки належним чином реагувати в разі кібератак, а також будувати партнерські відносини на міжнародному рівні.

Для виконання цієї роботи МСЕ співпрацює як з державами-членами ООН, так і з партнерами з приватного сектора, щоб визначити поточні проблеми, розглянути існуючі та виникаючі загрози і запропонувати глобальні стратегії для досягнення наступних семи стратегічних цілей:

1. Стратегія для розробки типового законодавства про кіберзлочинність, яке стосується глобального масштабу і сумісно з існуючими національними та регіональними законодавчими нормами.

2. Стратегія для створення відповідних національних і регіональних організаційних структур і розробки політики по боротьбі з кіберзагрозами.

3. Стратегія для встановлення загальноприйнятих мінімальних критеріїв безпеки і схем акредитації для апаратних і програмних додатків і систем.

4. Стратегія створення глобальної структури для спостереження, попередження і реагування на інциденти в кіберпросторі для забезпечення транскордонної координації між новими й існуючими ініціативами.

5. Стратегія для створення і схвалення універсальної системи цифрової ідентифікації і необхідних організаційних структур для забезпечення визнання цифрових повноважень поза географічних кордонів.

6. Стратегія щодо сприяння нарощуванню людського та інституційного потенціалу для розширення знань і ноу-хау у всіх секторах.

7. Стратегія міжнародного співробітництва, діалогу та координації у всіх вищезазначених сферах.

Далі зупинимося докладніше на зазначених структурних елементах GCA і діях МСЕ по їх реалізації, які можуть використовуватися в Україні.

Правові заходи.

Кіберзлочинці являють собою постійну загрозу в Інтернеті, в той час як організована злочинність зростає. Це пов’язано з тим, що залишаються відповідні лазівки в національному і міжнародному законодавстві, що

ускладнює ефективне усунення кіберзагроз. Основна проблема тут полягає у відсутності міжнародної гармонізації законодавства про кіберзлочинність, а розслідування кіберзлочинів і судове переслідування кіберзлочинців утруднені, якщо класифікація злочинів відрізняється від країни до країни.

МСЕ сприяє різним державам (за їх бажанням) в розумінні правових аспектів кібербезпеки для того, щоб рухатися в напрямку гармонізації національних нормативно-правових баз. Використовуючи ці ресурси законодавства про кіберзлочинність, МСЕ вирішує одну зі семи стратегічних цілей GCA, яка вимагає вироблення стратегії для розробки законодавства про кіберзлочинність, що застосовується в глобальному масштабі та сумісного з існуючим національним законодавством. При цьому створення відповідних правових інфраструктур є невід'ємним компонентом національної стратегії у сфері кібербезпеки.

Ухвалення всіма країнами відповідного законодавства проти неправомірного використання ІКТ в злочинних або інших зловмисних цілях, включаючи заходи, спрямовані на забезпечення цілісності національних критично важливих інформаційних інфраструктур, має центральне значення для досягнення глобальної кібербезпеки. Оскільки загрози можуть виникати в будь-якій точці земної кулі, ці проблеми за своєю природою носять міжнародний характер і вимагають міжнародного співробітництва, допомоги в проведенні розслідувань і загальних правових і процедурних положень. Таким чином, важливо, щоб країни узгодили свої правові рамки для боротьби з кіберзлочинністю і сприяли міжнародному співробітництву. Ресурси МСЕ за законодавством про кіберзлочинність в даний час складаються з «Розуміння кіберзлочинності: керівництво для країн, що розвиваються» («Understanding Cybercrime: A Guide for Developing Countries») [370] та «Інструментарію МСЕ по законодавству про кіберзлочинність» («ITU Toolkit for Cybercrime Legislation») [371]. Розглянемо їх.

«Розуміння кіберзлочинності: керівництво для країн, що розвиваються». Мета даної публікації – допомогти країнам, що

розвиваються, краще зрозуміти національні та міжнародні наслідки зростаючих кіберзагроз, оцінити вимоги існуючих національних і міжнародних документів, допомогти країнам у створенні надійної правової основи для боротьби з кіберзагрозами.

Керівництво також надає широкий вибір ресурсів для більш глибокого вивчення різних тем, таких як огляд явищ кіберзлочинності, який включає в себе опис того, як скоюються злочини, і аналіз найбільш поширених кіберзлочинів, таких як крадіжка особистих даних і атак типу «відмова в обслуговуванні». У ньому також розглядаються проблеми, пов’язані з розслідуванням і судовим переслідуванням кіберзлочинців, а також короткий огляд заходів, що вживаються міжнародними та регіональними організаціями в боротьбі з кіберзлочинністю. На закінчення наводиться аналіз різних правових підходів, що стосуються кримінального права, процесуального права, міжнародного співробітництва та відповідальності постачальників Інтернет-послуг, і наводяться приклади міжнародних підходів, а також приклади передової практики в різних державах.

«Інструментарій по законодавству про кіберзлочинність». Метою даного набору інструментів є надання країнам прикладів законодавчих формулювань і довідкових матеріалів, які можуть допомогти в розробці гармонізованих законів і процедурних правил щодо кібербезпеки. Цей інструментарій, розроблений міждисциплінарної міжнародною групою експертів, країни можуть використовувати для створення / удосконалення правової бази кібербезпеки і пов’язаних з нею законів.

Даний інструментарій був розроблений після всебічного аналізу найбільш актуальних національних і міжнародних правових основ, що існують в даний час. Мова інструментарію відповідає цим законам і покликана служити керівництвом для країн, що бажають розробити, удосконалити або змінити свої власні закони щодо кіберзлочинності. Інструментарій призначений для просування глобальної гармонізації законів щодо кіберзлочинності, виступаючи в якості центрального ресурсу, який

допомагає законодавцям, адвокатам, урядовцям, політичним експертам та представникам ІТ-галузі в усьому світі підштовхувати свої країни до створення узгодженої правової бази, що захищає від неправомірного використання ІКТ.

Технічні та процедурні заходи.

ІКТ є життєво важливим інструментом в інформаційних суспільствах. Однак вони продовжують експлуатуватися недобросовісними користувачами, і це явище нерозривно пов’язане з організованою злочинністю в Інтернеті. Уразливості в програмних додатках навмисно розшукуються для створення шкідливих програм, які забезпечують несанкціонований доступ, що ставить під загрозу цілісність, справжність і конфіденційність мереж і систем ІКТ. Зі зростанням складності шкідливих програм ці загрози неможливо переоцінити, оскільки вони можуть мати вкрай негативні наслідки, якщо вони торкнуться критично важливої інформаційної інфраструктури.

Сектор стандартизації МСЕ (МСЕ-Т) об’єднує приватний і публічний сектори для спільної роботи із погодження політики і стандартів безпеки в міжнародному масштабі, що має важливе значення для забезпечення кібербезпеки, оскільки гармонізація стандартів не тільки підвищить рівень безпеки, але і скоротить витрати на створення захищених систем.

В даний час існують буквально сотні стандартів МСЕ (Рекомендацій МСЕ-Т) з безпеки, які мають наслідки для кібербезпеки. Це, зокрема, такі:

• Рекомендації серії X.500 по службам каталогів і аутентифікації, включаючи добре відому рекомендацію МСЕ-Т X.509. X.509 є наріжним каменем для розробки додатків, пов’язаних з інфраструктурою відкритих ключів (PKI), і широко використовується в широкому спектрі додатків, починаючи від забезпечення безпеки з’єднання між браузером і сервером в Інтернеті, закінчуючи наданням цифрових підписів, які дозволяють проводити транзакції електронної торгівлі з тією ж упевненістю, як і в традиційній торгівлі. Без широкого впровадження цього стандарту зростання

електронного бізнесу було б неможливим.

• Рекомендації серії X.800 по архітектурі безпеки, зокрема, Рекомендація МСЕ-Т X.805, яка дає операторам і підприємствам телекомунікаційних мереж можливість надати наскрізний опис архітектури з точки зору безпеки. Тим самим, рекомендація дозволяє операторам визначати всі вразливі точки в мережі і знижувати їх вразливість.

• Рекомендація X.1205, «Огляд кібербезпеки», в якій дається визначення кібербезпеки і таксономія загроз безпеки. В рекомендації обговорюється природа середовища і ризиків кібербезпеки, можливі стратегії захисту мережі, методи захищеного зв'язку і дієздатність мережі (навіть під атакою).

Однією з найбільш актуальних сфер діяльності МСЕ в даний час є боротьба з крадіжкою особистих даних, оскільки страх цього найбільшою мірою заважає користувачам довіряти Інтернет. У зв'язку з цим МСЕ були розроблені спеціальні Рекомендації, що стосуються управління ідентифікацією користувачів.

Крім того, активно просувається ініціатива МСЕ з обміну інформацією про кібербезпеку (CYBEX), в рамках якої передбачена можливість імпортувати більше 20 кращих в своєму класі стандартів для платформ, розроблених за останні кілька років урядовими установами та IT-галуззю для підвищення кібербезпеки. Ці платформи збирають і обмінюються інформацією про «стан» безпеки систем і пристроїв, про уразливість, про інциденти, такі як кібератаки, і пов'язану з цим «евристику» знань. Застосовуваний підхід CYBEX об'єднує ці платформи узгодженим чином, щоб забезпечити: 1) «блокування» онлайн-систем для мінімізації вразливостей; 2) збір інформації про інциденти для аналізу при виникненні мережевих шкідливих інцидентів; 3) збір доказів для забезпечення здійснення необхідних дій надалі.

Важливою в цьому сенсі є Рекомендація МСЕ-Т X.1520 «Загальні уразливості (CVE)», яка надає структуровані засоби для обміну

вразливостями інформаційної безпеки в комерційному програмному забезпеченні або програмному забезпеченні з відкритим вихідним кодом, що використовується в мережах зв'язку, пристроях кінцевих користувачів або будь-яких інших типах ІКТ, здатних працювати з програмним забезпеченням.

У свою чергу, Рекомендація МСЕ-Т Х.1521 «Загальна система оцінки вразливостей (CVSS)» забезпечує основу для передачі характеристик і впливів вразливостей інформаційно-комунікаційних технологій в одному і тому ж контексті і дозволяє користувачам цієї Рекомендації використовувати спільну мову для оцінки вразливостей ІКТ .

В Рекомендації Х.1209 «Можливості та їх контекстні сценарії для спільного використання та обміну інформацією про кібербезпеки» описані базові сценарії на високому рівні і визначені допоміжні можливості для спільного використання та обміну інформацією про кібербезпеки. Ці надані можливості важливі для підтримки взаємодії між додатками для спільного використання та обміну інформацією про кібербезпеки.

А в Рекомендації МСЕ-Т Х.1207 зібрані кращі практики і «Керівництва для постачальників телекомунікаційних послуг для усунення ризику шпигунського і потенційно небажаного програмного забезпечення».

В рамках ініціативи CYBEX, МСЕ тісно співпрацює з Форумом груп реагування на інциденти і безпеки (FIRST) – Всесвітньою організацією з координації та співпраці між групами реагування на комп'ютерні інциденти. Результатом цього й інших співробітництв стало створення Глобального центру реагування (GRC), який відіграє ключову роль в реалізації мети забезпечення технічних заходів для боротьби з існуючими та новими кіберзагрозами. Двома основними структурними елементами GRC є NEWS (мережева система раннього оповіщення) і ESCAPE (електронно-безпечна прикладна платформа для спільної роботи експертів).

За задумом його засновників GRC покликаний стати головним ресурсним центром по кіберзагрозам у світі. Працюючи з провідними партнерами, включаючи академічні кола і представників владних структур,

центр прагне до того, щоб надати світовій спільноті в користування агреговану систему раннього попередження в реальному часі. Це допоможе країнам на ранньому етапі виявляти кіберзагрози і швидко визначати, які заходи слід вжити для їх пом'якшення, включаючи реалізацію можливостей спостереження, попередження і реагування на інциденти, створення груп реагування на комп'ютерні інциденти, а також поширення попереджень, технічну допомогу та навчання.

Передбачається, що GRC також надасть державам-членам МСЕ доступ до спеціалізованих інструментів і систем, включаючи недавно розроблену платформу ESCAPE. ESCAPE – це електронний інструмент, який дозволяє кіберекспертам з різних країн об'єднувати ресурси і взаємодіяти один з одним віддалено, але в безпечному та надійному середовищі. Доступ до ESCAPE надається офіційним представникам держав, а також експертам, призначеним партнерами МСЕ IMPACT. Об'єднуючи ресурси і досвід багатьох різних країн в короткі терміни, ESCAPE дозволить окремим країнам і світовій спільноті негайно реагувати на кіберзагрози, особливо в кризових ситуаціях.

Організаційні структури.

Системи моніторингу та оповіщення, а також реагування на інциденти мають важливе значення, коли йдеться про протидію кібератакам, але не менш важливим є вільний обмін інформацією, співробітництво і взаємодія всередині і між національними організаційними структурами.

Співпраця на всіх рівнях публічного управління і з приватним сектором, академічними колами, регіональними та міжнародними організаціями необхідна для підвищення обізнаності про потенційні атаки і вжиття заходів щодо виправлення даної ситуації. Ефективне управління інцидентами також вимагає урахування наявного фінансування, людських ресурсів, можливостей навчання, технологічних можливостей, відносин між публічним і приватним сектором, а також діючої нормативно-правової бази. Все це вимагає, в свою чергу, створення певних організаційних структур і

налагодження їх взаємодії.

Слід зазначити, що за останні двадцять років робляться активні зусилля, щоб налагодити результативну взаємодію організаційних структур, що діють в сфері кібербезпеки, на національному і регіональному рівнях. Однак на глобальному рівні подібних зусиль все ще недостатньо, у зв'язку з чим МСЕ працює з державами-членами над визначенням конкретних потреб в кібербезпеці, які у них є, і на основі цього взаємодіє з відповідними національними, регіональними та міжнародними організаціями для підвищення кібербезпеки в глобальних масштабах.

Тим не менш, у багатьох країнах, особливо в країнах, що розвиваються, рівень комп'ютерної готовності до надзвичайних ситуацій все ще залишається низьким. Але запуск атаки з боку мереж менш підготовлених країн може вплинути на глобальні мережі ІКТ через високий рівень взаємозв'язку. У зв'язку з цим деякі ініціативи МСЕ рекомендують державам-членам створити національні центри реагування на кібербезпеки, такі як групи реагування на комп'ютерні інциденти (CIRT). Наприклад, в Резолюції 58 Всесвітньої асамблеї по стандартам електрозв'язку в 2008 році і Резолюції 69 Всесвітньої конференції з розвитку електрозв'язку в 2009 році підкреслюється, що добре функціонуючі CIRT в країнах, що розвиваються підвищать рівень готовності до реагування на кібератаки і сприятимуть забезпеченню безпеки в національних інфраструктурах ІКТ, а також координації на регіональному і міжнародному рівнях. Крім того, ряд ініціатив спрямований на створення CIRT в тих країнах, де їх немає, з урахуванням вже наявного передового досвіду в цій сфері [297].

Багато зі згаданих ініціатив здійснюються спільно з IMPACT, яке в партнерстві з провідними експертами в сфері ІКТ збирає і розробляє глобальні керівні вказівки з кращої практики, створюючи міжнародний еталон, який особливо актуальний для органів влади. Цей підрозділ проводить за запитом незалежні перевірки безпеки ІКТ в публічних організаціях або компаніях, що займаються критично важливою

інфраструктурою, забезпечуючи тим самим відповідність цих організацій найвищим стандартам безпеки. При цьому відділ забезпечення безпеки IMPACT функціонує як міжнародно визнаний, незалежний, неурядовий орган по сертифікації кібербезпеки.

Нарощування потенціалу.

Нарощування потенціалу необхідно для формування стійкої та активної культури кібербезпеки. Однією з ключових проблем кібербезпеки є ефективне навчання кінцевого користувача. Це питання стосується всіх зацікавлених сторін, від органів влади та великих корпорація до освітніх установ.

З огляду на важливу роль, яку ІКТ відіграють в наданні послуг в таких різних секторах, як охорона здоров'я, освіта, фінанси і комерція, життєво важливо знати про можливості, що надаються безпечним кіберпростором, і про загрози, властиві кіберпростору. Програми, націлені на створення рівних умов для підвищення базової обізнаності та нарощування потенціалу на всіх рівнях, мають важливе значення, і їх також необхідно здійснювати як на міжнародному, так і на національному рівні.

МСЕ розробило і випустило практичне керівництво по наданню допомоги країнам, які бажають розробити свій національний підхід до кібербезпеки і до захисту найважливішої інформаційної інфраструктури (CIIP).

Кібербезпека і захист найважливішої інформаційної інфраструктури є загальними обов'язками органів влади, бізнесу, інших організацій і окремих користувачів, які розробляють, надають, керують, обслуговують і використовують інформаційні системи і мережі, тобто всіх відповідних акторів. Управління невід'ємними ризиками безпеки вимагає активної співпраці всіх акторів з урахуванням проблем безпеки, пов'язаних з їх ролями. Колективна мета полягає в тому, щоб готуватися до будь-яких інцидентів, реагувати на них і швидко усувати їх, при цьому зводячи до мінімуму шкоду.

У будь-якій взаємозалежній системі ролі й обов'язки часто перетинаються. Тільки тоді, коли всі актори матимуть спільне розуміння цілей безпеки, того, як їх досягти, і своїх індивідуальних ролей, ця колективна мета може бути досягнута. Крім того, спільне бачення з чітко розмежованими ролями та обов'язками необхідне для створення стратегії управління ризиками, притаманними використанню ІКТ.

Органи влади в змозі очолити національні зусилля по підвищенню кібербезпеки і поліпшенню захисту найважливішої інформаційної інфраструктури. Багато країн, у тому числі й Україна, вже зробили ряд зусиль по захисту критичної (інформаційної) інфраструктури.

Як тільки країна набуває власного цінного досвіду вирішення проблем кібербезпеки і захисту найважливішою інформаційної інфраструктури, вона може зробити більш цінний внесок в глобальні спільні зусилля із забезпечення кібербезпеки. В цьому відношенні Національне керівництво МСЕ з кібербезпеки спрямоване на надання допомоги державам у розробці їх національної стратегії, з урахуванням оцінки їх існуючих можливостей для вирішення проблем кібербезпеки і визначення їх вимог. Даний посібник орієнтований на політичних лідерів і керівників органів влади, надаючи їм вказівки про те, як оцінювати існуючі національні політики, процедури, норми, інститути та відносини в світлі національних потреб для підвищення кібербезпеки і вирішення проблем захисту критично важливої інформаційної інфраструктури. У посібнику також містяться вказівки про те, як розробляти стратегії кібербезпеки після зіставлення кінцевих результатів (цілей), засобів (ресурсів і можливостей) і способів (як використовувати засоби для досягнення цілей) відповідно до загальних цілей і завдань GCA.

МСЕ через свій Сектор розвитку телекомунікацій надає допомогу, необхідну для здійснення цих зусиль, а також надає підтримку країнам, які знаходяться в процесі розробки і переоцінки своїх національних стратегій у сфері кібербезпеки.

МСЕ також працює з експертами над розробкою практичного

комплекту засобів для пом’якшення наслідків функціонування бот-мереж, щоб допомогти, зокрема, країнам, що розвиваються у вирішенні зростаючої проблеми бот-мереж.

Бот-мережа – це набір програмних агентів або роботів, які працюють автономно і автоматично. Цей термін найчастіше асоціюється зі зловмисним програмним забезпеченням, але він також може відноситися до мережі комп’ютерів, що використовують програмне забезпечення розподілених обчислень. Хоча бот-мережі часто називають за назвою їх шкідливого програмного забезпечення, зазвичай функціонують кілька бот-мереж, що використовують одні й ті ж сімейства шкідливих програм.

МСЕ в якості протидії бот-мережам пропонує Botnet Mitigation Toolkit – багатосторонній підхід для відстеження бот-мереж і пом’якшення їх впливу з особливим акцентом на проблемах, характерних для країн з економікою, що розвивається. Підхід надає інформацію і рекомендації про те, як захистити себе від бот-мереж і боротися з ними, а також дає поради про те, як налагоджувати співпрацю в даній сфері між різними стейкхолдерами, включаючи бізнес-структури, правоохоронні органи, Інтернет-провайдерів і організації громадянського суспільства.

Міжнародне співробітництво.

Хоча Інтернет та ІКТ забезпечують безпрецедентний взаємозв’язок, вони також обмежують здатність країн закривати свої кордони для вхідних кіберзагроз та стримувати ті, які виходять зсередини. Спроби вирішити ці проблеми на національному рівні важливі, але їх явно недостатньо.

Кібербезпека так само глобальна і масштабна, як Інтернет. Тому рішення повинні прийматися і впроваджуватися без урахування державних кордонів. Міжнародне співробітництво необхідно не тільки на урядовому рівні, але і з промисловими, неурядовими та міжнародними організаціями. З цієї причини, GCA прагне скористатися наявними можливостями і ресурсами широкого кола стейкхолдерів для розробки і реалізації глобальних стратегій з метою підвищення кібербезпеки.

Найважливішим елементом міжнародної системи партнерства у сфері кібербезпеки є Міжнародне багатостороннє партнерство проти кіберзагроз (IMPACT), що є міжнародною публічно-приватною ініціативою, спрямованою на підвищення здатності світового співтовариства запобігати і реагувати на кіберзагрози. У листопаді 2008 року штаб-квартира IMPACT в Кіберджайя, Малайзія, офіційно стала оперативним, фізичним будинком GCA.

Під керівництвом МСЕ і спільно з ООН, Інтерполом, Радою Європи та Організацією економічного співробітництва та розвитку (ОЕСР), серед іншого, Центр політики та міжнародного співробітництва IMPACT вносить свій внесок в розробку нової політики і узгодження національного законодавства з низки питань, що стосуються кіберзагроз, включаючи кіберзлочинність.

Центр політики та міжнародного співробітництва також надає консультативні послуги зацікавленим державам з питань політики і регулювання кібербезпеки. За підтримки МСЕ центр розвиває міжнародне співробітництво за допомогою конкретних програм, таких як скоординовані навчання з кібертренінгів між країнами.

Також у співпраці з провідними ІКТ-компаніями і установами IMPACT проводить брифінги на високому рівні в інтересах представників держав-членів МСЕ. Багато з ключових партнерів IMPACT надали своїх відповідних технічних керівників, головних дослідників й інших експертів в рамках унікальної програми IMPACT високого рівня, щоб тримати органи влади своїх країн в курсі нинішніх і майбутніх кіберзагроз. Такі міжгалузеві брифінги високого рівня надають країнам неоціненну інформацію і дають приватному сектору уявлення про останні тенденції, потенційні загрози і нові технології.

Метою дослідного відділу IMPACT є напрямок академічної уваги, в тому числі з боку університетів та науково-дослідних інститутів, на проблеми, які в даний час можуть не вирішуватися належним чином. У

співпраці з МСЕ IMPACT робить свою дослідницьку мережу доступною для світового співтовариства. Крім академічної мережі, глобальна штаб-квартира IMPACT надає державам-членам МСЕ доступ до спеціалізованих лабораторій ІКТ, спеціалізованого обладнання, ресурсних центрів та інших засобів.

З цією метою було створено так званий «Шлюз кібербезпеки», який представляє собою інформаційний ресурс з описом відповідних ініціатив у всьому світі, як на національному, так і на міжнародному рівні. У сучасному взаємозалежному світі загрози можуть виникати де завгодно, і, отже, наша колективна кібербезпека залежить від практики забезпечення безпеки кожної країни, організації, бізнесу та громадянина. Через шлюз кібербезпеки МСЕ прагне забезпечити доступ до інформації, її поширення й інтерактивне співробітництво між зацікавленими сторонами, які працюють в сферах, пов'язаних з кібербезпекою і кіберзлочинністю. Він служить платформою для інформування зацікавлених сторін про різних учасників і групи, що працюють в різних сферах кібербезпеки на національному та міжнародному рівнях. МСЕ пропонує всім зацікавленим сторонам вивчити великі ресурси і посилання, доступні через шлюз кібербезпеки (http://www.Itu.int/cybersecurity), і приєднатися до партнерства з МСЕ та іншими організаціями для зміцнення довіри і безпеки при використанні ІКТ.

Важливо і те, що під егідою GCA МСЕ запустив ініціативу «Захист дітей в Інтернеті» (COP) в якості міжнародної спільної мережі для дій з просування онлайн-захисту дітей і молоді, надаючи керівництво по безпечній поведінці в Інтернеті спільно з іншими установами та партнерами ООН. Основними цілями цієї ініціативи є:

– визначення ключових ризиків та вразливості для дітей та молоді в кіберпросторі;

– підвищення обізнаності про ризики і проблеми в кіберпросторі;

– розробка практичних інструментів, щоб допомогти громадським організаціям та освітнім установам мінімізувати ризики для дітей та молоді в

кіберпросторі;

– обмін знаннями та досвідом за сприяння міжнародних стратегічних партнерств для визначення і реалізації конкретних ініціатив.

Ініціатива COP об’єднує ефективний пакет політики і практики, освіти і навчання, інфраструктури і технологій, а також обізнаності та комунікацій. Вона реалізується на основі участі багатьох стейкхолдерів з переконанням, що кожна організація, педагог або законодавець, технічний експерт або галузевий орган можуть зробити свій внесок.

Підіб’ємо підсумки викладеного в цьому параграфі. Можна не сумніватися, що ІКТ стали невід’ємною частиною людського розвитку, але сутність проблеми кібербезпеки полягає в тому, що глобальні мережі ІКТ, які виросли навколо життєво важливих аспектів нашого повсякденного життя, ніколи не призначалися для забезпечення особливої безпеки. Сучасне комп’ютерне середовище кидає виклик багатьом з наших традиційних підходів до безпеки та вимагає унікальних рішень. При цьому кібербезпека є глобальною проблемою, яка може бути вирішена тільки за допомогою глобальних рішень.

Однак, аналізуючи діяльність таких організацій як МСЕ, можна виділити кілька важливих напрямків дій, які повинні бути реалізовані в Україні для підвищення національної кібербезпеки в цілому і публічного сектора зокрема, а саме:

1. Гармонізація національного законодавства в сфері кібербезпеки із законодавством ЄС.

2. Впровадження стандартів і рекомендацій, розроблених МСЕ, які стосуються технічних аспектів забезпечення кібербезпеки.

3. Створення на національному та регіональних рівнях спеціальних організаційних структур і команд протидії кіберзагрозам різного характеру.

4. Реалізація масових освітніх програм, спрямованих на формування безпечної поведінки в кіберпросторі.

5. Розширення міжнародного співробітництва в сфері кібербезпеки,

участь в реалізації різних ініціатив у цій сфері.

Створення глобальної кібербезпеки є багатогранним і складним завданням, але якщо різні держави будуть активно та плідно взаємодіяти для цього, то вигоди, отримані від сучасного інформаційного суспільства, можуть надати людству найкращі шанси для стійкого миру, безпеки і розвитку.

3.3. Комплексний підхід до формування та реалізації державної політики у сфері кібербезпеки

Аналіз національних стратегій кібербезпеки, проведений в попередніх розділах, показав фундаментальну еволюцію в розробці державної політики, відповідно до якої кібербезпека стає одним із пріоритетних завдань уряду й інших органів влади. До таких змін привело розуміння двох важливих факторів, які впливають на всі сучасні держави, в тому числі і на Україну. До цих факторів належать такі:

1) *Інтернет та ІКТ необхідні для економічного та соціального розвитку і утворюють життєво важливу інфраструктуру*. У загальному контексті економічного спаду, що став результатом останньої пандемії, викликаної COVID-19, відкритий Інтернет та ІКТ є новим джерелом зростання і рушійною силою інновацій, соціального благополуччя та індивідуального самовираження. У міру зростання Інтернет-економіки вся економіка і суспільство, включаючи публічний сектор, стають все більш залежними від цієї цифрової інфраструктури для виконання своїх основних функцій.

2) *Кіберзагрози розвиваються і зростають швидкими темпами*. Вони як і раніше ініціюються кримінальними діячами, але також надходять з нових джерел, таких як іноземні держави та політичні групи, і можуть мати інші мотиви, крім заробляння грошей, такі як деякі види «хактивізму» (Anonymous), дестабілізація, кібершпіонаж, саботаж (наприклад, Stuxnet) і

навіть військові дії (наприклад, гібридна війна Росії проти України). Сучасні шкідливі актори стали краще організовані в порівнянні зі своїми попередниками, що, зокрема, дозволяє їм краще приховувати свої сліди, а ступінь складності кіберзагроз значно зросла, демонструючи явні ознаки професіоналізації тих, хто є їх джерелом.

Як наслідок, сфера застосування стратегій кібербезпеки повинна змінитися від захисту окремих осіб та організацій як окремих суб'єктів до захисту суспільства в цілому. Ця зміна є результатом еволюції ролі Інтернету в суспільстві. Коли Інтернет був просто *корисною* платформою для окремих осіб і організацій, наслідки відмов можна було контролювати на рівні кожної окремої особи і організації, і політика органів влади полягала в тому, щоб допомогти їм запобігти таким інцидентам і управляти ними. Оскільки Інтернет став *необхідним* для економіки і суспільства, наслідки невдач можуть безпосередньо впливати на суспільство в цілому. Тому стратегії кібербезпеки повинні бути спрямовані на досягнення двох взаємопов'язаних завдань: 1) зміцнення кібербезпеки для Інтернет-економіки, щоб сприяти економічному та соціальному процвітанню; 2) захист кіберзалежних суспільств від кіберзагроз. Управління складністю паралельного вирішення цих двох завдань при збереженні відкритості Інтернету і відповідних фундаментальних цінностей, ймовірно, є сьогодні головним завданням розробки політики в сфері кібербезпеки.

Критичність Інтернету для сучасної економіки має кілька наслідків для розробки політики в сфері кібербезпеки, основним з яких є прийняття стратегій, які підходять до забезпечення кібербезпеки **комплексним і всеосяжним чином**. Нинішні органи влади повинні визнавати необхідність розглядати всі аспекти кібербезпеки цілісно, а не фрагментарно, як в минулому. Тому нові стратегії кібербезпеки повинні поширюватися на весь публічний сектор і охоплювати економічні, соціальні, освітні, правові, правоохоронні, технічні, дипломатичні, військові та розвідувальні аспекти кібербезпеки. Для реалізації такого комплексного підходу необхідна

наявність політичної волі на рівні глави держави або глави уряду, що має бути сигналом для всіх органів влади про значне підвищення кібербезпеки серед національних пріоритетів.

Проте, як показав аналіз, не у всіх стратегіях використовуються терміни «кіберпростір» і «кібербезпека», а деякі зі стратегій, які використовують ці терміни, також дають визначення, які варіюється в залежності від країни. Хоча більшість країн при цьому включають концепцію критично важливих інформаційних інфраструктур у сферу своєї стратегії, як це визначено в Рекомендації ОЕСР щодо захисту критично важливих інформаційних інфраструктур [431].

Однак, можна виділити і ряд загальних аспектів, які, на наш погляд, повинні бути присутніми в політиці та стратегії кібербезпеки в Україні. До таких аспектів слід віднести:

Посилення координації органів влади на політичному та оперативному рівнях. Оскільки кібербезпека стає питанням національного пріоритету, відповідальність за розробку і реалізацію політики в сфері кібербезпеки чітко розподіляється всередині публічного сектора. Однак жоден з існуючих органів влади не може претендувати на всебічне розуміння і досить широкі повноваження для управління всіма аспектами кібербезпеки. Таким чином, координація між відповідними органами стає важливою. При цьому відповідальність за координацію повинна покладатися на конкретну існуючу або нову установу, і відповідальність інших залучених публічних організацій також повинна бути чітко визначена, щоб сприяти співпраці, заохочувати взаємодію, уникати дублювання і об’єднувати ініціативи. Така модель являє собою *еволюцію від багатовідомчого до міжвідомчого підходу* і вимагає сильного лідерства, щоб забезпечити координацію і співробітництво в рамках існуючих державних механізмів. Причому зрозуміло, що конкретні домовленості розрізнятимуться в різних країнах і відображатимуть політичну культуру, яка має місце.

Зміцнення публічно-приватного співробітництва. Всі стратегії

визнають, що кіберпростір в значній мірі належить приватному сектору і керується ним, і що користувачі також відіграють ключову роль в його функціонуванні та безпеці. Тому політика кібербезпеки повинна ґрунтуватися на інклюзивних партнерських відносинах між публічним, приватним і третім секторами, які можуть включати бізнес, громадянське суспільство, Інтернет-спільноту й академічні кола.

Покращення міжнародного співробітництва. Як показав аналіз, міжнародне співробітництво та необхідність створення більш ефективних альянсів і партнерств з країнами-однодумцями або союзниками, у тому числі сприяння створенню потенціалу в менш розвинених країнах, є основними завданнями більшості стратегій. Більшість проаналізованих стратегій, однак, надають мало подробиць про те, як саме домогтися розширення міжнародного співробітництва. Виняток становлять Сполучені Штати, які розробили спеціальну міжнародну стратегію для кіберпростору [504], і Великобританія, яка ініціювала міжнародний діалог на Лондонській конференції 2011 року з кіберпростору і просуває концепцію міжнародних норм поведінки в кіберпросторі [497]. У зв’язку з цим слід при розробці національної стратегії звернути увагу на необхідність більш високого ступеня гармонізації законодавства проти кіберзлочинності, зокрема, Будапештської конвенції 2001 року про кіберзлочинність, відповідних документів міжнародних і регіональних організацій, такі як Рада Європи, Європейський Союз, Форум з управління Інтернетом, Організація з безпеки і співробітництва в Європі (ОБСЄ) і ООН, включаючи Міжнародний союз телекомунікацій [284].

Повага до фундаментальних цінностей. Всі стратегії роблять сильний акцент на необхідності політики кібербезпеки поважати фундаментальні цінності, які зазвичай включають в себе конфіденційність, свободу слова і вільний обмін інформацією. У декількох стратегіях прямо згадується про необхідність підтримувати відкритість Інтернету, і жодна стратегія не пропонує зменшити відкритість на користь посилення кібербезпеки.

Навпаки, відкритість Інтернету зазвичай описується як вимога для подальшого розвитку Інтернет-економіки.

Аналіз стратегій кібербезпеки й інших подібних документів дозволяє визначити інші ключові принципи, які хоча і не завжди явно позначені, але повинні бути, на наш погляд, обов'язково враховані в стратегії кібербезпеки України. До цих принципів слід віднести такі:

Урахування питань суверенітету при розробці політики в сфері кібербезпеки, тобто комплексне урахування аспектів національної та міжнародної безпеки, розвідки, оборони та військової справи.

Цей принцип є прямим наслідком того, що кібербезпека спрямована на захист суспільства в цілому і вимагає комплексного підходу з боку органів влади. Питання суверенітету виникають на різних рівнях внутрішньої політики:

1) на стратегічному рівні, наприклад, з визнанням кіберзагроз, спрямованих на військових, або ризиків кібершпіонажу з боку іноземних держав;

2) на організаційному рівні, оскільки органи влади і різні їх підрозділи, чия діяльність пов'язана з дипломатією, розвідкою і збройними силами, як правило, включені в міжурядову координацію для вироблення політики, а також в міжвідомчу структуру, що відповідає за координацію діяльності щодо забезпечення національної безпеки , в тому числі, і кібербезпеки;

3) на оперативному рівні, коли, наприклад, розвідувальні органи відіграють ключову роль в якості джерела інформації для обізнаності про поточну ситуацію.

Міркування суверенітету також з'являються на рівні міжнародної політики: по-перше, в стратегіях згадується необхідність міжнародного діалогу щодо «правил участі» в кіберпросторі або «заходів зміцнення довіри»; по-друге, стратегії підкреслюють роль деяких організацій, таких як НАТО і ОБСЄ щодо вирішення різних політичних питань; по-третє, стратегії згадують необхідність оперативного співробітництва щодо обміну

розвідувальною інформацією між союзниками.

Гнучкий підхід до формування та реалізації політики. Інтернет – це динамічне середовище, в якому технології та інструменти постійно розвиваються непередбачуваним чином в інтересах зростання та інновацій, але загрози також знаходяться в постійному розвитку. У зв'язку з цим деякі стратегії просувають гнучку політику кібербезпеки, яка зберігає відкритість Інтернету і вільний потік інформації, а також інші фактори, які дозволяють Інтернету генерувати економічні й соціальні вигоди і пристосовуватися до фундаментально динамічного середовища. Ці стратегії підтримують політики, які забезпечують швидкі й обґрунтовані процеси прийняття рішень, впроваджують механізми швидкого зворотного зв'язку і включають в себе ефективні цикли навчання та покращення для швидкого і ефективного впровадження нових кіберінструментів. Такі стратегії акцентують на саморегулюванні в кіберпросторі і вважають, що законодавче регулювання щодо кіберпростору слід використовувати тільки в тих випадках, коли саморегулювання не є можливим або неефективно.

Важливість економічних аспектів кібербезпеки. У той час як всі стратегії спрямовані на вирішення проблеми кібербезпеки з метою підтримки і подальшого розвитку економічного і соціального процвітання за допомогою безперервного розвитку динамічної Інтернет-економіки, економічні аспекти кібербезпеки стають все більш помітними особливо в декількох стратегіях. Ці стратегії підкреслюють, що більш високий рівень кібербезпеки забезпечить економіці їхньої держави конкурентну перевагу, а також вони визнають, що економічні фактори відіграють ключову роль у підвищенні кібербезпеки. Тому деякі стратегії вимагають більш глибокого розуміння структури стимулів учасників ринків щодо кібербезпеки і заохочення відповідних заходів, таких як використання міток безпеки, які застосовуються до продуктів і послуг, для кращого інформування ринку. Кілька стратегій поставили в якості однієї з ключових цілей політики істотний розвиток сектора кібербезпеки, включаючи розвиток людського

потенціалу в сфері кібербезпеки та розвиток сектора страхування кібербезпеки. У свою чергу, інші стратегії визначають як важливу мету політики більш високий ступінь технологічної незалежності щодо інформаційної безпеки.

Важливість діалогу за участю багатьох зацікавлених сторін. Багато стратегії поділяють думку, що діалог з неурядовими стейкхолдерами (громадськими організаціями та бізнес-структурами) є ключем до ефективного формування і реалізації політики кібербезпеки. Однак рівень деталізації щодо того, яким чином органам публічної влади налагоджувати діалог за участі багатьох зацікавлених сторін варіюється, при цьому багато стратегій містять мало або взагалі не містять подробиць з цього аспекту. У деяких стратегіях передбачається створення спеціального органу, що включає всі зацікавлені сторони для надання інформації та консультацій органам публічної влади різного рівня.

Стратегії кібербезпеки зазвичай включають або супроводжуються прийняттям планів дій, спрямованих на зміцнення ключових пріоритетних сфер, до яких, як правило, відносяться такі [413]:

1. Державна безпека: плани дій включають безліч ініціатив, починаючи від розвитку потенціалу ситуаційної обізнаності та закінчуючи раціоналізацією урядової мережевої інфраструктури і узагальненням аудитів в публічному секторі.

2. Захист критично важливої інформаційної інфраструктури: плани дій зазвичай включають заходи, пов’язані із захистом критично важливих інформаційних інфраструктур.

3. Боротьба з кіберзлочинністю: в плани дій входять різні ініціативи з розвитку потенціалу правоохоронних органів, вдосконалення нормативно-правової бази та розвитку міжнародного співробітництва на основі Будапештської конвенції про кіберзлочинність.

4. Підвищення обізнаності: плани дій включають в себе різні ініціативи, спрямовані на конкретні групи населення, такі як особи, які

приймають рішення в органах влади і критично важливих інфраструктурах.

5. Освіта: в планах дій визнається, зокрема, необхідність в розвитку кадрового потенціалу в сфері кібербезпеки. Більше того, розвиток навичок кібербезпеки визначено в якості ключового пріоритету деякими країнами.

6. Реагування: в планах дій визнається важлива роль, яку відіграють групи реагування на інциденти в сфері кібербезпеки (CSIRT), тому вони передбачають створення національної CSIRT або її розвиток там, де вона вже існує.

7. Науково-дослідні та дослідно-конструкторські роботи (НДДКР): на їх важливості стали акцентувати не так давно, але в планах дій останніх років їм приділяється серйозна увага, особливо в контексті взаємодії з приватним сектором.

Разом з тим, на наш погляд, слід до переліченого вище додати ще кілька важливих ключових сфер, яким треба відвести спеціальне місце як в політиці кібербезпеки, так і у відповідних планах дій:

– розвиток можливостей для ситуаційної обізнаності та моніторингу в режимі реального часу, в основному для публічних інфраструктур;

– визначення і моніторинг об’єктів, які, не будучи критично важливими інформаційними інфраструктурами на даний момент, можуть за певних умов завдати значної шкоди кібербезпеці;

– партнерство з Інтернет-провайдерами для усунення загрози ботнетів за участю їх клієнтів;

– проведення навчань з кібербезпеки, в тому числі, і міжнародних;

– розробка та широке впровадження систем цифрової ідентифікації;

– реалізація спеціальної політики захисту дітей в Інтернет.

Також, з огляду на сучасну спрямованість на багатосуб’єктність у забезпеченні кібербезпеки, яка передбачає співпрацю публічного, приватного і третього секторів, можна сформулювати ще ряд пропозицій для підвищення ефективності стратегій і політики кібербезпеки, а саме:

1) Спільна систематична оцінка відповідності заходів кібербезпеки,

пропонованих органами влади, іншим ініціативам у сфері кібербезпеки. Наприклад, законодавство, яке встановлює кримінальну відповідальність за хакерство, могло б взяти до уваги, що деякі дослідження сприяють підвищенню кібербезпеки, використовуючи такі ж методи, як і хакери.

2) Публічні організації як власники і оператори інформаційних систем і мереж можуть подавати приклад іншим акторам, застосовуючи передовий досвід, технології і навіть законодавчі вимоги. Технології, розроблені для одного із секторів, також можуть принести користь іншим секторам.

3) Політики можуть звернутися за порадою до технічного товариства Інтернету якомога раніше в процесі розробки політики, щоб уникнути прийняття технологічно помилкових рішень.

4) Політика в сфері кібербезпеки може стимулювати розробку відкритих стандартів, що дозволяють впроваджувати інновації для рішень у даній сфері, спираючись на шанованих в експертному співтоваристві і таких, що добре зарекомендували себе, фахівців зі стандартизації Інтернету, уникаючи при цьому односторонньої зміни стандартів Інтернету.

5) Слід заохочувати збір емпіричних даних, щоб краще оцінювати актуальність стратегій і політик, а також підтримувати підходи, засновані на оцінці ризиків. Для протидії існуючим перешкодам, з якими багато акторів стикаються при наданні додаткової інформації про кіберінциденти, слід виділяти додаткові ресурси і впроваджувати узгоджені механізми повідомлення про порушення безпеки, з якими стикаються представники всіх трьох секторів.

Крім багатосуб'єктності слід враховувати і міжнародний вимір політики в сфері кібербезпеки, який дає не тільки позитивні результати (про які багато говориться), але і негативні. Так, вимоги, що пред'являються деякими країнами до галузі ІКТ, створюють для неї технічні бар'єри у взаємодії, наприклад, у формі вимог місцевих стандартів, надлишкових схем сертифікації безпеки або втручань в глобальний ланцюжок створення вартості (якщо мова йде про комерцію); знижують функціональність,

обмежують інновації і спотворюють рівні умови гри. Щоб уникнути цього, необхідно розгортання глобальних рентабельних галузевих рішень, впровадження міжнародних стандартів, систем взаємного визнання відповідності та підвищення обізнаності менш розвинених країн з цих питань.

Ще одним важливим питанням у контексті розробки політики кібербезпеки є втручання / невтручання держави в діяльність організацій приватного сектора щодо забезпечення їх кібербезпеки.

Дійсно, сьогоднішній масштабний вплив кіберзагроз змушує уряди і органи безпеки багатьох країн зосередити увагу на кібербезпеці не тільки в публічному, а й приватному секторі. Однак навколо даного питання існує дискусія щодо того, чи можуть органи влади диктувати, яким чином приватний сектор повинен забезпечувати свою кібербезпеку, і якщо так, то наскільки це ефективно. До цієї дискусії додається суспільна заклопотаність з приводу інформаційної прозорості та її впливу на права і свободи громадян.

Інформаційно-комунікаційні системи пов’язані між собою на глобальному рівні. Безперервна робота цих систем для надання життєво важливих послуг залежить від їх невразливості для кібератак. Однак при цьому, по-перше, дуже часто як публічні, так і приватні організації не знають, яку дійсну роль Інтернет відіграє в їх інфраструктурі, по-друге, приватні підрядники все частіше надають органам влади послуги із забезпечення функціонування систем обміну критично важливою інформацією. Тому, на наш погляд, органи влади обов’язково повинні мати можливість впливати на організації приватного сектора щодо забезпечення їх кібербезпеки, що має здійснюватися на базі обміну інформацією, співпраці і спільних дій. Більш того, подібна співпраця має реалізовуватися не тільки на національному, а й на міжнародному рівні, зі створенням урядових коаліцій.

Подібні коаліції вже існують, зокрема, в рамках таких організацій як Організація економічного співробітництва і розвитку (ОЕСР), Європейське поліцейське управління (Європол) та Асоціація держав Південно-Східної Азії

(АСЕАН). Запобігання міжнародних кіберзлочинів, таких як шпигунство і злам, вимагає спільних зусиль, і міжурядові органи повинні виступати посередником при їх розслідуванні, оскільки відсутність розуміння в цьому питанні між країнами становить загрозу міжнародній боротьбі з кіберзагрозами. Що стосується приватного сектора, то органи влади можуть співпрацювати (і в багатьох країнах співпрацюють) в розробці програм, технологій і керівництв щодо дотримання передових галузевих практик кібербезпеки.

Однак, як показує практика, забезпечення інформаційної прозорості в приватному секторі виявляється складним завданням, особливо у фінансовій галузі. У ряді країн компанії зобов'язані розкривати всю інформацію про витік даних своїм клієнтам, проте не всі країни дотримуються одних й тих же законів і правил, що ще більше ускладнює інформаційну безпеку міждержавних даних споживачів. Конфіденційність інформації, свобода слова, інтелектуальна власність і права на комп'ютерну безпеку досі є невизначеними в глобальному масштабі, оскільки не існує єдиної точки зору на співвідношення цих понять. Наприклад, у США The National Journal Daily писав: «Оскільки Конгрес прагне прийняти більше законів про кібербезпеку, щоб стимулювати обмін інформацією між урядом і приватним сектором, це може відкрити скриньку Пандори щодо конфіденційності та громадянських прав і свобод» [465].

Органи влади мають співпрацювати, а не диктувати приватному сектору, тому вкрай важливо, щоб обидві сторони працювали разом, щоб допомогти захистити країну від кіберзагроз. Приватна промисловість є провідним актором і знаходиться на головній лінії вогню загроз і нападів. Разом з публічним приватний сектор також повинен співпрацювати, щоб забезпечити належну технічну підготовку осіб, що захищають від глобальних кібератак. Однак, часта проблема, з якою стикаються обидва сектора - це відсутність довіри між ними. Так, приватні компанії не вирішуються передавати інформацію та свою репутацію в руки органів влади, оскільки

витік інформації може мати згубні наслідки для приватних компаній. Що стосується громадської думки, то вона досить показово описана Кемпбеллом: «Більшість опитаних людей не вважають, що уряд повинен диктувати, як саме приватні компанії повинні зберігати свої дані, в той же час 31,5% не впевнені, що уряд робить достатньо для регулювання того, як приватні компанії захищають наші дані» [267]. Тобто громадяни все ж хотіли б, щоб органи влади певною мірою втручалися в діяльність приватних організацій щодо забезпечення тими кібербезпеки, тобто здійснювали певні інтервенції.

Органи влади можуть здійснювати інтервенції за допомогою публічної політики в певній сфері і через законодавство. Наприклад, це може бути прийняття закону про посилення кібербезпеки в публічному та приватному секторі або про обмін інформацією між органами влади та приватними організаціями. Також хорошим прикладом є прийнятий в США в 2002 році Федеральний закон про управління інформаційною безпекою (FISMA), який об’єднав інформаційну, економічну і національну безпеку шляхом забезпечення виконання оцінок ризиків, керівних принципів конфігурації і політик безпеки.

Відповідна політика може бути спрямована на впровадження загальних стандартів і протоколів безпеки незалежно від сектора. Прикладом у цьому сенсі, гідним наслідування, є Базовий план конфігурації уряду США (USGCB), що містить правила комп’ютерної безпеки, регульовані державними системами США, яким повинна відповідати будь-яка організація, яка підключається до державної системи кібербезпеки, як публічна, так і приватна.

Слід згадати ще один приклад із США. У 2014 році комітет Сенату з розвідки прийняв закон про кібербезпеку, що дозволяє обмінюватися інформацією між приватним сектором і урядом щодо загроз безпеці [325]. Однак цей закон був підданий критиці через потенційні негативні наслідки розголошення особистої інформації органами влади, внаслідок чого в закон були внесені поправки, що регулюють приватну інформацію громадян, яка

отримується приватними підприємствами.

Аслані, Уайт і Етткін відзначають, що вплив вразливостей кібербезпеки, які не усунуті заздалегідь, має серйозні операційні наслідки [236]. При цьому, за оцінками авторів, тільки 25% приватних організацій здійснюють необхідні заходи безпеки в рамках своїх стандартних операційних процесів. У той же час, недостатній захист і фінансових систем, і критичної інфраструктури, якщо вони стануть жертвами кібератак та інших шкідливих дій, може мати руйнівні наслідки для організацій (як приватних, так і публічних) і громадян. І в цьому сенсі використання політик кібербезпеки, які адмініструються органами влади, може сприяти впровадженню передових методів і посиленню безпеки для розробників програмного забезпечення, постачальників і організацій, що зберігають важливу інформацію і забезпечують функціонування критично важливих галузей і об’єктів, а також навчанню технічного персоналу методам протидії кіберзагрозам, заснованим на оцінці ризику.

Проте, питання конфіденційності, дотримання громадянських прав і свобод викликають заклопотаність у багатьох, коли органи влади вводять обов’язкові правила кібербезпеки, особливо щодо збору інформації та обміну нею між секторами, зокрема при проведенні розслідувань, не пов’язаних з кібербезпекою. Концепція обміну інформацією, про яку в даному випадку йде мова, полягає в тому, щоб дати можливість органам влади збирати інформацію про загрози у кіберсфері, і ділитися нею з організаціями приватного сектора. Ця концепція реалізована, зокрема, в США, де подібний обмін здійснюють Центри обміну і аналізу інформації (ISAC). При цьому існує певна законодавство, що регулює обмін інформацією про кібербезпеки.

У свою чергу, приватні компанії займаються виробництвом програмного забезпечення, обладнання, комп’ютерів і мережевих компонент, якими згодом користуються організації публічного сектора, в тому числі, і для забезпечення функціонування критично важливої інфраструктури, зокрема, оборонної. Відповідно, органи влади зацікавлені в дотриманні

приватними організаціями максимальних заходів захисту від кіберзагроз. У США був неприємний випадок, коли хакери з КНР вкрали надсекретні плани винищувача F-35 Joint Strike Fighter, які, за деякими даними, включали в себе відомості про найбільш інноваційні термоядерні боєголовки. Сталося це через те, що приватні підрядники оборонної промисловості не дотримувалися належних нормативних заходів контролю кібербезпеки.

Як показує практика, компанії, що використовують підхід до кібербезпеки, заснований на оцінці ризиків, який передбачає конкретну кількісну оцінку ризиків кіберзагроз, досягають більшого успіху в захисті систем і даних. Хакери шукають уразливості в високочутливих критичних системах, тому оцінка вразливостей і аналіз політик компанії будуть сприяти загальному аналізу ризиків. Поряд з цим компанії повинні проводити постійний поведінковий аналіз, вимірювати потенційні загрози, вразливості і наслідки.

У 2010 році Google разом з 20 іншими компаніями став жертвою штучно створеної кібератаки, що виходила з Китаю, під час якої зловмисники намагалися пошкодити вихідний код сайту [454]. WikiLeaks повідомляє, що цей напад був санкціонований Постійним комітетом Політбюро компартії КНР [523]. Атака не мала того успіху, на який розраховували зловмисники, але після цього випадку Google став активно співпрацювати з Агентством національної безпеки (АНБ), вони разом тестували програмні, апаратні та уразливі місця, щоб визначити можливу поведінку зловмисників і пом’якшити негативні наслідки в майбутньому. Таке партнерство між Google і АНБ показало приклад успішної взаємодії між публічним і приватним сектором. Маючи велику технічну підтримку, яку він міг отримати від таких компаній, як Facebook або Microsoft, Google вирішив співпрацювати з питань кібербезпеки з АНБ замість Департаменту внутрішньої безпеки США. Дивно, але Google довірив АНБ об’єднати ресурси для пошуку недоліків в системі безпеки, використовуючи ефективні засоби контролю кібербезпеки, а також дотримуючись протоколів

кібербезпеки, розроблених урядовими установами.

Звичайно, урядові протоколи можуть в деяких випадках стримувати інновації, а не сприяти посиленню контролю безпеки. Але, як видно з прикладу партнерства Google з АНБ, у великих гравців є певний рівень довіри з боку уряду, і вони визнають свій обов'язок захищати національну безпеку, застосовуючи заходи безпеки, визначені в політиці, постановах і протоколах, прийнятих урядом.

Таким чином, приватні суб'єкти поряд з органами влади несуть відповідальність за забезпечення національної кібербезпеки. Фундаментальна архітектура кібербезпеки на 90% належить і управляється приватними суб'єктами. Ці основні компоненти критично важливої інфраструктури включають в себе, зокрема, транспорт, фінанси, енергозабезпечення та ін., і працездатність цих компонент залежить від стійкості мереж приватного сектора. Тому потреба в створенні сильної та оперативної структури кібербезпеки очевидна, при цьому приватні компанії повинні застосовувати заходи безпеки відповідно до урядових протоколів. З іншого боку, органи влади повинні розробляти протоколи безпеки і нормативні акти, що стосуються кібербезпеки, через робочі партнерства з приватним сектором, щоб враховувати також і його інтереси, зокрема, щодо контролю інформації.

Виходячи з усього викладеного вище, на наш погляд, політика кібербезпеки в Україні повинна ґрунтуватися на таких принципах:

– впровадження стратегічного підходу до забезпечення кібербезпеки;

– комплексне вирішення проблем кібербезпеки, включаючи використання ефективних механізмів координації, адаптованих до культури і стилю управління в країні;

– своєчасність, гнучкість і адаптивність у прийнятті рішень у сфері забезпечення кібербезпеки;

– розвиток національного потенціалу команд з протидії кіберінцидентам;

– впровадження передових методів забезпечення кібербезпеки;

– покращення захисту критично важливих інформаційних інфраструктур;

– повага до фундаментальних цінностей свободи інформації, але з використанням належних запобіжних заходів, стримувань і противаг;

– підвищення кіберграмотності суспільства;

– використання системи стимулів для розвитку сфери кібербезпеки і відповідного кадрового потенціалу;

– співпраця з приватними та неурядовими організаціями, розвиток публічно-приватного партнерства;

– посилення боротьби з кіберзлочинністю;

– заохочення досліджень і розробок у сфері кібербезпеки;

– розвиток міжнародного співробітництва, зокрема, шляхом участі в розробці загальних норм поведінки в кіберпросторі.

Що стосується останнього пункту, то визначення в рамках національних стратегій точок координації з міжнародними партнерами створює можливість для активізації міжнародного співробітництва на стратегічному та оперативному рівнях. При цьому кожна країна може розглянути питання про розширення зусиль з координації, визначивши в своєму уряді «міжнародний контактний пункт», який буде доступний, наприклад, для сприяння поширенню серед відповідних національних установ запитів іноземних держав, пов’язаних з кібербезпекою, будь то для надзвичайних, інформаційних або інших цілей.

В цілому, як можна бачити з досвіду багатьох країн, розробка політики в сфері кібербезпеки виходить на новий рівень зрілості в порівнянні з попередніми політиками, характерними для першого десятиліття 21 століття, з більш кваліфікованим керівництвом, кращою координацією і більш широкою участю зацікавлених сторін. У той же час проблеми, пов’язані з розробкою політики, збільшуються, що говорить про те, що уряди також стикаються з новим рівнем складності. Наприклад, необхідно задовольняти потребу в більшій координації між агентствами за допомогою більш

високого ступеня централізації, одночасно забезпечуючи динамічні та швидкі, майже в реальному часі, процеси прийняття рішень на всіх рівнях. Ще однім складним завданням є необхідність запровадження цілісних підходів, що враховують суверенітет та економічні / соціальні проблеми, участь широкого кола органів публічної влади і розширення співпраці з приватним сектором. Також проблемою є необхідність збереження відкритості Інтернету і фундаментальних цінностей відповідно до Рекомендації 2011 року Ради по принципам формування Інтернет-політики [267].

На вирішення цих та інших проблем потрібний час, між тим, на даний момент ключовим завданням для публічного сектора в сфері кібербезпеки є підготовка до можливих серйозних кіберінцидентів і протидія їм, але таким чином, щоб не підірвати відкритість Інтернету.

3.4. Основні виклики врядування у сфері кібербезпеки

Політика у сфері кібербезпеки може ґрунтуватися на односторонніх чи багатосторонніх заходах. Проте до тих пір поки код кіберпростору, тобто інструкції, вбудовані в його апаратне та програмне забезпечення [346, с. 121], в основному ігнорує фізичні кордони, односторонні зусилля, як правило, є дорогими або неефективними. Держави завжди можуть напевно відключити себе від Інтернету. Але тоді їм доводиться нести витрати, пов’язані з економічною (і культурною) ізоляцією. Під час тижневого відключення інтернету в Єгипті у 2010 році, яке уряд навмисно здійснив, єгипетська телекомунікаційна індустрія втратила дохід, оцінюваний в 90-110 мільйонів доларів США [441]. Зведення віртуальних огорож, тобто ізоляція себе на синтаксичному, а не на фізичному рівні кіберпростору також ускладнює міжнародні обміни. Якщо запозичити метафоричний опис ситуації у М. Лібіцкі, то той, хто хоче бути на агорі, не може залишатися в замку весь час [396, с. 62].

Співпраця конче необхідна для забезпечення кібербезпеки, оскільки навіть найбільш дієздатна держава не може сподіватися самостійно передбачити та відобразити всі кібератаки. Співпраця може здійснюватися на разовій або системній основі. Останнє, на наш погляд, найкраще здатне забезпечити врядування. К. Оффе пропонує відрізняти врядування від управління ієрархічними та ринковими структурами [439]. Цей термін також застосовується до діяльності так званих багатосторонніх структур, які забезпечують механізми співпраці різних публічних і приватних акторів [407]. Відповідно до такого розумінням врядування у сфері кібербезпеки включає в себе добровільні спільні зусилля публічних і приватних акторів із забезпечення доступності, автентичності, цілісності та конфіденційності цифрових даних, що зберігаються в кіберпросторі або переданих через нього.

Існують деякі характеристики врядування у сфері кібербезпеки, які можуть як посилювати зазначене вище співробітництво, так і загрожувати йому. Серед цих характеристик найбільш важливими є наступні:

1. Практично всі можливості для атаки або захисту в кіберпросторі залежать від знання про уразливість [397]. Як правило, ці уразливості складаються з невідомих властивостей комп'ютерного коду. Але з тим же успіхом вони можуть стосуватися і людей або організацій, схильних до атак соціальної інженерії. В обох випадках саме знання, а не матеріальні можливості, дають здатність протистояти загрозам у кіберпросторі. Однак поширення та використання знань набагато важче виявити і, отже, регулювати, ніж поширення або використання матеріальних можливостей.

2. Оскільки знання є основним ресурсом у сфері кібербезпеки, в цій сфері спостерігається тенденція до зменшення асиметрії влади. Існує безліч суб'єктів, здатних здобувати знання і, відповідно, наносити серйозної шкоди в кіберпросторі. Крім того, географічне положення цих суб'єктів не має значення для більшості операцій. З цих двох причин співпраця з цими суб'єктами або проти них повинна бути всеосяжною. Отже, досягнення домовленостей утруднено. Це також більш ризиковано, враховуючи той

факт, що обмін інформацією може здійснюватися нескінченно. В цьому відношенні управління кібербезпекою структурно дуже схоже на співпрацю в галузі розвідки.

3. Наявні та діючі кодекси в кіберпросторі явно не сприяють відповідальності за інциденти. Таким чином, заохочується порушення правил і, відповідно, не заохочується їх дотримання. Можлива також і неправильна атрибуція, за якої треті сторони будуть проводити операції «під фальшивим прапором» і, таким чином, спричиняти взаємні звинувачення «всіх проти всіх». Отже, quid pro quo як основний принцип встановлення та стабілізації співробітництва [237] не працює добре в кіберпросторі.

4. Феномени, що відрізняються в фізичному світі, такі як злочинність, війна та інтелект, як правило, досить схожі в кіберпросторі. Отже, існує більший ризик неправильної класифікації поведінки й серйозного неправильного сприйняття намірів. Крім того, важко точно визначити межі співпраці та забезпечити, щоб актори не використали свої законні права в одній сфері в якості прикриття для негативних дій в інших сферах.

Зрозуміло, що ці характеристики не впливають однозначно негативно на співробітництво різних акторів у сфері кібербезпеки, але ускладнюють його, спричиняючи певні проблеми, до основних з яких можна віднести три: 1) проблема «безкоштовного використання», 2) проблема шахрайства, 3) проблема відносних вигод. Розглянемо їх докладно.

Проблема безкоштовного використання.

Деякі суб’єкти отримують вигоду від суспільних благ, не вносячи свій внесок в їх виробництво та підтримку. Вони можуть використовувати зусилля інших, оскільки суспільні блага не мають ціни для споживачів, неконкурентні і не можуть бути виключені. Неконкурентність означає, що споживання блага одним суб’єктом не призводить до зниження доступності блага для споживання іншими. Невиключність означає практичну неможливість виключення будь-якого суб’єкта зі споживання блага [457]. Але проблеми виникають, коли занадто багато людей піддаються спокусі

безкоштовного використання [440, с. 48]. У цих умовах виробництво блага може припинитися, а може і не відбутися зовсім. До речі, недостатнє виробництво суспільних благ досить часто зустрічається в міжнародних відносинах. Цього можна уникнути двома способами. Перший полягає у тому, що повинна бути або одна держава, або група держав, які готові нести додаткові витрати, докладаючи додаткові зусилля [440]. Другий полягає у тому, що державам вдається встановити спільний міжнародний режим як стримуючий чинник для безкоштовного використання певних суспільних благ [381].

Як ми зазначали раніше, кібербезпека є суспільним благом, хоча, звичайно, це не чисте суспільне благо. Хоча держава, яка інвестує в свою кібербезпеку, в першу чергу, покращує безпеку своїх власних суспільних чи приватних мереж, однак певною мірою вона також приносить користь кібербезпеці інших держав. Ми звикли вважати комп'ютерні мережі мішенню кібератак. Але вони також служать «сходинками» або «трамплінами» для атак на треті сторони. Зловмисники спрямовують свої шкідливі програми по декількох мережах юрисдикцій, щоб замести сліди. Таким чином, надійно захищені комп'ютерні мережі певною мірою сприяють забезпеченню кібербезпеки всієї глобальної кіберсистеми.

Слабо захищені комп'ютерні мережі, в свою чергу, створюють ризик не тільки для їх власників, а й для інших мереж. Вони можуть навіть піддавати ризику безпеку інших мереж тільки в тому випадку, якщо слабо захищена мережа сама по собі не містить нічого, що має достатню економічну або політичну цінність. Слабка кібербезпека, з цієї точки зору, є такою ж суспільною вадою, як і викиди вуглекислого газу або збезлісення. Практично ніхто не виключається з її наслідків. І її поширення не вповільнюється в міру того, як від неї страждає велика кількість суб'єктів. Слід додати, що слабка кібербезпека обумовлена не тільки технічними і організаційними, а й законодавчими недоліками. Хорошим прикладом є так званий «I-love-you virus» 2000 року, комп'ютерний вірус, який привів до фінансових втрат в

розмірі декількох мільярдів доларів США по всьому світу. Після того, як правоохоронні органи остаточно визначили творця вірусу, молодого студента з Філіппін, вони не змогли заарештувати і притягнути його до відповідальності, оскільки філіппінський законодавство у той час не забороняло створення і використання комп'ютерних шкідливих програм [469].

Тут слід підкреслити, що в той час як філіппінське законодавство послабило національну кібербезпеку, самі Філіппіни не стали жертвою цих недоліків. Швидше, провідні економіки Америки, Західної Європи та Східної Азії постраждали від шкоди, завданої найважливішим ІТ-системам. Тому випадок вірусу «I-love-you virus» є прикладом загальної закономірності: бідні держави мають менше стимулів інвестувати в кібербезпеку, ніж багаті держави. До тих пір, поки кожна держава самостійно забезпечує безпеку своїх мереж, і відповідно до своїх власних інтересів, досить імовірно, що кібербезпека як суспільне надбання недооцінюється на глобальному рівні. Як уникнути глобального недообеспечення кібербезпеки? Повертаючись до того, що було зазначено, можна сказати, що є, по суті, дві можливості. Одна з них полягає в створенні та забезпеченні дотримання міжнародному режиму, який ефективно карає тих, хто не відповідає певному стандарту кібербезпеки. Інша можливість полягає в тому, що група сильніших держав добровільно надає допомогу в забезпеченні кібербезпеки слабшим державам. Перша стратегія обговорювалася, перш за все, в США. Друга вже здійснюється в різних двосторонніх та багатосторонніх угодах.

Що стосується першої стратегії, то ще приблизно десять років тому, як в «Огляді політики у сфері кіберпростору» 2009 року, так і в «Міжнародній стратегії США у сфері кіберпростору» 2011 року наводяться аргументи на користь встановлення нової міжнародної норми, яка покладе на держави відповідальність за будь-які кібератаки, що здійснюються з інфраструктур, які перебувають під їх юрисдикцією [489, с. 8]. Ідея полягає в тому, щоб працювати над проблемою атрибуції. Норми «суверенної відповідальності»,

на думку прихильників даної ідеї, мають зобов'язати кожну державу не допустити, щоб її національні мережі стали притулком для кіберзлочинців та інших зловмисників. З цієї ж причини держави більше не можуть приховувати свої власні кампанії за нібито приватними хакерами.

Деякі американські чиновники та коментатори навіть наполягають на більш радикальній ідеї, виступаючи за введення санкцій або легітимізацію тактики «зворотного злому» в разі порушення норм. За словами Майкла Хейдена, колишнього директора Агентства національної безпеки (АНБ), інтернет-трафік в штатах з відхиленнями від норми може бути сповільнений або навіть перерваний [465]. Аналогічні ідеї висловлює колишній радник з кібербезпеки Білого дому Річард Кларк [278] та інші фахівці у цій сфері. Так, ще в 2008 році полковник Чарльз Вільямсон закликав до створення військової бот-мережі, яка могла б використовуватися в цілях самозахисту від атак навіть нейтральних або союзних держав [525]. Міжнародне право вже дає достатньо підстав для таких заходів «активної оборони», стверджує співробітник Міністерства оборони Дж. Метью. До тих пір, поки держава, з юрисдикції якої виходять атаки, або не бажає, або не в змозі зупинити такі атаки, жертва може законно «відповісти» на ці загрози, причому вона не зобов'язана доводити усвідомлення або співучасть держави, суверенітету якої вона збирається нашкодити. Саме за такою логікою Рада Безпеки ООН санкціонувала військові дії США проти уряду талібів в Афганістані [464]. Подібний режим в сфері кібербезпеки майже напевно відрадить держави від неуважного ставлення до захисту своєї IT-інфраструктури. Однак Склеров також визнає, що нинішня державна практика, а також більшість експертів в галузі міжнародного права поки не підтримують аналогічні підходи в кіберпросторі [там само, с. 62].

Другий підхід до вирішення проблеми безкоштовного використання полягає у тому, що одна держава або групи держав надають допомогу в забезпеченні кібербезпеки державам зі слабкими стратегіями та можливостями у сфері кібербезпеки. Ті, хто особливо зацікавлений у

високому рівні кібербезпеки, можуть запропонувати технічну або юридичну допомогу іншим. В якості альтернативи вони можуть навіть взяти на себе захист іноземних мереж, подібно до того, як США взяли на себе велику частину захисту Західної Європи під час холодної війни. Але при цьому слід мати на увазі, що той, хто захищає іноземні мережі, може й використовувати їх у власних інтересах, у тому числі для шпигунської діяльності, тому що одні й ті ж знання дають можливість як оборонного, так і наступального характеру. Ймовірно, далеко не всі держави готові скомпрометувати свою національну безпеку таким чином.

На відміну від цього підтримка кібербезпеки через технічну та правову допомогу є моделлю низького ризику з точки зору тих, хто отримує допомогу. Вона вже досить активно практикується на двосторонній та багатосторонній основі. До числа найбільш активних постачальників допомоги по забезпеченню кібербезпеки належать США, оскільки:

«Будучи світовим лідером в області інформаційної економіки, Сполучені Штати прагнуть до того, щоб і інші країни користувалися цими технічними ресурсами та досвідом. США може грати і буде відігравати активну роль у наданні знань і потенціалу для створення та забезпечення безпеки нових та існуючих цифрових систем» [489, с. 14].

Для досягнення цієї мети багато публічних організацій США співпрацюють з міжнародними партнерами. Управління з питань державної підзвітності (УПДЗ) перераховує кілька з цих ініціатив: організаційні підрозділи Міністерства торгівлі та Міністерства національної безпеки допомагають державам Латинської Америки та Карибського басейну підвищувати технічний, регулятивний та адміністративний потенціал в рамках Організації американських держав (ОАД). Міністерство юстиції США бере участь у навчальних програмах для членів АТЕС та АСЕАН, а також для держав-членів Африканського союзу та ЕКОВАС. Бюро розвідки та досліджень (БРД) Державного департаменту США надає експертні послуги в рамках ОБСЄ. Але незважаючи на ці та інші види діяльності,

американські експерти та політики регулярно закликають до розробки більш комплексної програми кіберпомочі іншим державам [400].

Поряд із США та іншими великими кібернетичними державами основними акторами з надання допомоги в забезпеченні кібербезпеки є міжнародні організації. Так, як вже зазначалось, Глобальний порядок денний з кібербезпеки (GCA) Міжнародного союзу електрозв'язку (ITU) спрямований на поліпшення публічних та приватних можливостей по всьому світу. Країни, що розвиваються, можуть взяти участь у «Робочій програмі МСЕ з кібербезпеки для надання допомоги країнам, що розвиваються» [367]. В рамках Європейського союзу Європейське агентство мережевої та інформаційної безпеки (ЄНІСА) надає допомогу публічним та приватним суб'єктам у створенні та функціонуванні груп з реагування на надзвичайні ситуації в комп'ютерній сфері (CERT).

Але розглядаючи таку допомогу недемократичним режимам слід розуміти, що вона може використовуватись для спостереження та залякування політичних дисидентів, тому має бути чіткий контроль і моніторинг за використанням цієї допомоги.

Проблема шахрайства.

Ті, хто безкоштовно використовують інформаційно-комунікаційні мережі, отримують вигоду від зусиль інших, в той час як вони самі відмовляються що-небудь робити для цих зусиль. Шахраї, навпаки, беруть на себе зобов'язання підтримувати певні зусилля або утримуватися від певних дій. Після цього, однак, вони таємно діють інакше. Відсутність дієвого зовнішнього контролю влади егоїстично мотивованих національних держав робить обман однією з найпроблемніших проблем міжнародної співпраці в у цілому та у сфері кібербезпеки зокрема. Держави виявляються в ситуації, яка, як і знаменита дилема ув'язнених, позбавляє їх стимулів до співпраці, незважаючи на спільні інтереси [470]. Міжнародні інститути могли б допомогти у вирішенні цієї проблеми. Визначивши обов'язки і надавши механізми перевірки, вони можуть підтримати застосування принципу

взаємовигідного співробітництва, що дозволило б стабілізувати співпрацю навіть між егоїстично мотивованими суб'єктами. Будучи стійкими структурами, міжнародні інститути також розширюють «тінь майбутнього» і змушують держави дбати про свою репутацію.

Що стосується кіберпростору, то складнощі атрибуції у цьому просторі полегшують обман і шахрайство. Але потужні інститути можуть змінити це становище. Наприклад, держави могли б доручити міжнародному органу контролювати всі публічні та приватні мережі, що знаходяться під їх юрисдикцією. При наявності такої структури в кіберпросторі можуть бути створені добре відомі схеми на кшталт контролю над озброєннями. Зрозуміло, вони повинні бути адаптовані до конкретної проблематики. Оскільки «справжньою зброєю» в кіберпросторі є знання, навряд чи має сенс класифікувати та забороняти певні можливості. Однак держави могли б домовитися про оголошення поза законом деяких дій, наприклад, кібератак на критично важливі інфраструктури, і покладатися на міжнародні органи для перевірки дотримання їх угоди. Така ж процедура могла б застосовуватися і в ряді інших сфер.

Однак структури в кіберпросторі – це двосічний меч. Ті ж самі структури, які вирішують проблеми шахрайства, швидше за все, створять проблеми іншого роду. Можна у якості аналогії взяти такий приклад: будь-яка установа, що має можливості та повноваження інспектувати засекречені мережі, стане основною мішенню для розміщення шпигунів спецслужбами різних держав. Тому ризики просто можуть переважати вигоди, оскільки структури в кіберпросторі є одночасно «вирішувачами проблем» і «творцями проблем». І влада різних держав розуміє це добре. Розглянемо декілька прикладів, що ілюструють це.

Як відомо, існує ряд міжнародних інституційних платформ: наприклад, міждержавна Міжнародна мережа спостереження і попередження (IWWN), Форум груп з реагування на інциденти і забезпечення безпеки (FIRST), мережа публічних і приватних CERT, а також мережа Групи по боротьбі з

високотехнологічної злочинністю. Однак на практиці інформація про високочутливі ІТ-вразливості майже виключно ділиться між близькими партнерами. Між європейськими CERT існують хороші робочі відносини. Ще краще співробітництво на двосторонньому рівні. Наприклад, німецькі спецслужби тісно співпрацюють з французькими та американськими колегами. Проте, важко уявити собі подібний рівень співпраці з Росією чи Китаєм. Причина цих обмежень в обміні даними проста: знання, корисні для захисту мереж, також корисні для атак в кіберпросторі. Характер загроз, про які спецслужби повідомляють іноземним агентствам, також свідчить про їх можливості виявлення та зворотного відстеження. Співпрацюючі агентства можуть використовувати ці знання для майбутніх атак на державу-інформатор. Тому на практиці США і Росія ніколи у суттєвому обсязі не обмінювались інформацією про інциденти в кіберпросторі, як це має бути відповідно до спільного меморандуму, підписаному в 2010 році [487].

Інший приклад – інституціолізоване співробітництво між правоохоронними органами. Кіберзлочинці навмисно використовують інфраструктуру, що знаходиться під різними юрисдикціями. Найчастіше вони можуть ефективно і швидко замести сліди. Інші докази видаляються системними адміністраторами або провайдерами [506]. Традиційна співпраця правоохоронних органів навряд чи може відповідати цим реаліям. Недоліки традиційних процедур звернення за юридичною допомогою через офіційні дипломатичні канали є однією з причин того, що тільки приблизно 5% кіберзлочинців коли-небудь арештовувались та піддавалися судовому переслідуванню [526]. Правоохоронні органи розробили неформальні структури, такі як «цілодобова» мережа підгрупи G7 по високотехнологічним злочинам, для забезпечення збереження цифрових доказів кіберзлосинів до початку офіційних процедур. Це, безумовно, гарний крок для поглиблення співпраці, однак заморожування та обмін даними все ще повинні бути санкціоновані кожним національним відомством в кожному окремому випадку.

Більш ефективним вирішенням проблеми кіберзлочинців, які випереджають правоохоронні органи, було б загальне та взаємне санкціонування так званих кроссбордерських пошуків. Цей термін відноситься до законного доступу до обладнання під іноземною юрисдикцією [467, с. 197]. Конвенція Європейської ради по боротьбі з кіберзлочинністю, яку на сьогоднішній день ратифікували 33 країни, вже дозволяє проводити перехресний огляд при деяких особливих обставинах. Вони повинні бути санкціоновані провайдерами або адміністраторами, які можуть на законних підставах надавати доступ до даних або систем в кожному конкретному випадку. Однак навіть ці обмежені положення є політично спірними. Деякі держави, такі як Росія, виправдовували своє неприєднання до Конвенції посиланнями на це конкретне положення [403]. Важко сказати, чи є цей аргумент просто відмовкою або виразом справжньої стурбованості. Адже всі положення про перехресний пошук дійсно можуть використовуватися в якості прикриття для розвідувальних операцій. Тому найбільш ефективне інституційне вирішення проблеми кіберзлочинності пов’язане з найсерйознішим ризиком для національної безпеки. Принаймні, деякі держави думають про це саме так. Неясно, чи зможуть жорсткі вимоги щодо повідомлення та багатонаціональні правоохоронні групи - два засоби правового захисту, запропоновані деякими експертами [467], зняти ці побоювання.

Навіть серед союзників інституціоналізація співпраці у сфері кібербезпеки навряд чи набуває такої ж якості, як в інших тематичних сферах. Найкращим прикладом є Організація Північно-Атлантичного Договору (НАТО), і то, як вона вирішує так звану альянсну дилему. Союзники завжди потребують інституційних гарантій від двох основних ризиків: «захоплення» та «полишення». Перше стосується ризику втягування у всілякі непотрібні конфлікти, які мають союзники з іншими державами. Друге стосується ризику залишитися на самоті під час реального конфлікту. Маючи на увазі ці ризики, НАТО стикається з різними імперативами: один

закликає до більш низьких рівнів інтеграції, інший – до поглиблення союзницьких зв'язків. І слід визнати, що інституційна структура НАТО за часів холодної війни враховувала обидва імперативи. Розташування військових сил НАТО в Західній Європі гарантувало, що сили кожної держави-члена автоматично братимуть участь у бойових діях в разі конвенційної атаки держав Варшавського договору. Таким чином, страх полишення був зведений до мінімуму. У той же час мета НАТО була обмежена захистом територій її держав-членів. Обмеження мандата НАТО забезпечувало захист від ризиків захоплення.

Яким чином може бути досягнутий подібний баланс у сфері кібербезпеки? Мабуть, можна стверджувати, що існуючий рівень взаємозалежності між комп'ютерними мережами держав-членів вже працює проти ризику полишення. Однак випадок великомасштабних розподілених атак типу «відмова в обслуговуванні» (DDoS) на естонську Інтернет-інфраструктуру в 2007 році показав, що мережі більших країн-членів скоріше не постраждали від цих атак. Тому більш дрібні держави-члени схильні шукати формального підтвердження солідарності своїх союзників. Дійсно, відразу після DDoS-атак міністр оборони Естонії публічно обговорив питання про те, чи слід застосувати п'яту статтю договору НАТО у сфері кібербезпеки [493]. Власне кажучи, НАТО і справді оголосила кібербезпеку новим пріоритетом у Лісабоні в 2010 році, але досі залишило відкритим питання про можливість застосування п'ятої статті 5 у сфері кібербезпеки. Таким чином, до сих пір не існує колективного стримування потенційних кібер-зловмисників. Можна вказати на декілька причин, по яких НАТО проявляє обережність у цьому відношенні. Одна з них – це питання визначень. Експерти в галузі міжнародного права досі визначаються з питанням, чи можна класифікувати деякі види кібератак як еквіваленти збройних нападів в звичайній війні [359], оскільки тільки на ці напади можна було б на законних підставах відповісти симетричними діями.

Інша причина вибору обережного підходу, на думку деяких експертів, – це очікування максимізації ризиків потрапляння в пастку. До тих пір, поки члени альянсу не будуть спільно контролювати всі свої національні мережі, окремі держави теоретично можуть проводити операції «під чужим прапором» проти своїх мереж. Це може дати їм можливість підкріпити обвинувачення в агресії з боку інших держав, а якби кібератаки були класифіковані як «атаки за п'ятою статтею», то використовуючи вигадані атаки можна було б сподіватися залучити весь альянс до конфліктів з третіми державами. Окремі держави могли б також сфабрикувати докази, що збігаються з їх звинуваченнями, шляхом маніпулювання даними в своїх мережах. Потім вони могли б передати ці дані своїм партнерам по альянсу casus belli. Щоб уникнути подібних ризиків, НАТО, звичайно, могли б створити загальну структуру моніторингу та перевірки. Але, як вже зазначалось вище, така структура була б кошмаром для будь-якого експерта з контррозвідки. І оскільки розумно вважати, що шпигунство відбувається навіть серед союзників, то шанси на те, що така структура коли-небудь буде створена, невеликі.

Те, що буде реалізовано в рамках НАТО відповідно до останніх намірів, в першу чергу, стосується захисту власних мереж і можливостей НАТО. З цією метою альянс створив ряд органів з управління комп'ютерними інцидентами та реагування на них. Крім того, НАТО має дослідні та навчальні центри, такі як Центр підвищення кваліфікації в області спільного кіберзахисту (CCD-COE) в Таллінні. Всі ці зусилля забезпечують реальне підвищення рівня кібербезпеки НАТО, і вони також побічно позитивно впливають на кібербезпеку кожної окремої держави-учасниці.

Кібербезпека як проблема відносних вигод.

У неоліберального інституціоналізму та неореалізму багато спільного. Обидва вони розглядають стан анархії як важливу характеристику міжнародної системи [378], відтак успіх міжнародної співпраці залишається під питанням. Більш того, обидва вони розглядають поведінку держав як

засновану на раціональних розрахунках витрат та вигод. Тому для того, щоб передбачити шанси на співпрацю, вони вказують на стимули та антистимули, які формують ці розрахунки. Для інституціоналістів існує тільки одна перешкода для співпраці: проблема обману. Неореалізм, погоджуючись з цим першим пунктом, вважає не менш важливим ще одну перешкоду: те, як вигоди розподіляються між співпрацюючими партнерами. Держави просто вважають за краще не прагнути до абсолютної вигоди від співпраці, коли в той же час вони можуть отримати відносно меншу вигоду, ніж їх партнери по співробітництву. Причина цього полягає в незахищеності, яка властива стану анархії, як його бачать неореалісти. Міжнародна система, по суті, є системою самодопомоги [509], тому держави повинні завжди піклуватися про те, як співпраця впливає на їх відносну владу по відношенню до суперників. Вони можуть навіть утриматися від співпраці, яка принесла б їм користь, якби від цього більше виграли інші. Отже, співпрацю важче встановити і підтримувати з точки зору неореалістів, ніж з точки зору інституціоналістів.

Які тоді ставки з точки зору відносної влади в разі співпраці у сфері кібербезпеки? Щоб відповісти на це питання, в першу чергу необхідно знати, як влада в кіберпросторі розподіляється між державами. Але як можна визначити ранг влади в кіберпросторі? Існують різноманітні критерії, які можуть бути використані для вимірювання кібер-потужності. Згідно Кларку та Кнейку їх можна згрупувати, принаймні, в три категорії: залежність, наступальні можливості та оборонні спроможності [278, с. 148]. Якшо розглядати залежності, то слід відповісти на запитання: які активи держави повинні захищати в кіберпросторі? Цілком очевидно, що у країн з розвиненою економікою більше причин побоюватися відсутності кібербезпеки, ніж у більш відсталих у цьому сенсі країн. Крадіжка інтелектуальної власності та комерційних секретів в результаті кібератак є величезним ризиком, тому економічно розвинені країни повинні бути більш зацікавлені в здійсненні міжнародного співробітництва в боротьбі з кіберзлочинністю, ніж менш розвинені країни. У них також має бути більше

підстав утримуватися від будь-якої ескалації міжнародних та транснаціональних конфліктів, яка може ще більше підвищити рівень кібератак в глобальних мережах.

Але залежності відносяться не тільки до економіки, але і до оборонної політики. Держави, чиї військові стратегії та сили значною мірою покладаються на ІТ-системи, стикаються з більш високим ризиком кібератак, ніж держави, чиї сили все ще характеризуються низьким рівнем мережевої взаємодії. Таким чином, збройні сили США можуть зупинитися в разі великомасштабної та витонченої кібератаки, принаймні, теоретично. Швидше за все, вони все ще зможуть вести бойові дії, але втратять «інформаційне домінування», що призведе до більшої кількості жертв. У цих умовах боротьба може стати політично нестійкою. На відміну від цього структура північнокорейської армії є дзеркально протилежною, ймовірно, вона не буде паралізована кібернетичними атаками. Високий рівень втрат також не змусить її політичне керівництво відступити та відмовитися від визначених для армії завдань.

Коротше кажучи, кіберпростір, оскільки він є повністю рукотворним середовищем, перевертає з ніг на голову асиметрію влади в одному конкретному аспекті: від нього найбільше залежать провідні економічні та військові держави. Вони повинні стежити за своїми кроками в кіберпросторі. На відміну від них, низько-технологічним країнам майже нічого втрачати, і вони можуть навіть подумати про стратегії «випаленої землі» в кіберпросторі, як про крайній варіант. Коли мова йде про наступальні можливості, застосовується протилежна логіка. Великі економічні та технологічні ресурси призводять до великих атакуючих можливостей.

Кіберпростір зменшує асиметрію потужностей, але не забезпечує рівні можливості. Звичайно, окремі особи або невеликі групи хакерів можуть породжувати хаос в переважній більшості комерційних або адміністративних мереж. Проте, атаки на високосекретні та фізично ізольовані мережі практично не доступні цим приватним хакерам, швидше за все, це тільки

сфера діяльності державних органів безпеки. Маніпуляції з іранськими установками зі збагачення урану в 2010 році, як приклад високоскладних кібератак, ймовірно, потребували кількох місяців роботи різноманітних фахівців та експертів і близько чверті мільйона доларів США, щоб купити інформацію про невідомі вразливості програмного забезпечення [322]. Ймовірно, у нападників були свої можливості для перевірки фізичних ефектів шкідливого ПЗ. Вони також могли мати доступ до інсайдів для того, щоб потрапити в комп'ютерні мережі іранських об'єктів, які прослуховуються.

Тобто технічні, фінансові та організаційні ресурси все ще мають значення в кіберпросторі. Відмінності з точки зору цих ресурсів також пояснюють деякі асиметрії влади між державами в кіберпросторі, через що більшість експертів виділяють групу країн з розвиненими можливостями атак. Так, експерти Центру нової американської безпеки до таких країн відносять США, Великобританію, Францію, Ізраїль, Росію та Китай [400]. У недавньому опитуванні серед американських експертів 33% назвали Китай найбільш здатним гравцем, а 11% - Росію. Однак більшість респондентів (47%) вважають, що США перебувають на вершині списку [329]. Інше експертне опитування серед керівників найважливіших інфраструктур по всьому світу показало схожі результати. Навіть деякі експерти з союзних США країн, таких як Німеччина та Іспанія, назвали США, а не Росію чи Китай, найбільш небезпечною кібернетичною державою [238, с. 31]. Великі щорічні витрати на кібербезпеку в розмірі 12-13 мільярдів доларів США ще більше посилюють цю картину [400].

Наступальна міць, проте, не повинна вимірюватися виключно здатністю держав проводити складні кібератаки проти сильно захищених інфраструктур. Велика кількість простіших кібератак може бути досить ефективною, наприклад, з метою економічного шпигунства проти іноземних компаній. Складні, але численні атаки на дисидентські веб-сайти також можуть бути високоефективним проявом політичних репресій. Саме з цієї

причини політичні відносини між державами та різними хакерськими групами також можуть слугувати додатковим індикатором здатності держави до атак у кіберпросторі. Деякі авторитарні держави явно виграють в цьому відношенні. Найбільш вражаючим прикладом є Китай, у якому ідея інтеграції приватних хакерських груп в проведені державою кампанії по веденню кібератак давно вже обговорюється в неофіційних стратегічних документах [245]. У Китаї багато хакерів є співробітниками державних компаній або студентами технічних вузів і, таким чином, частиною китайської державної системи [там само]. Існують також ідеологічні зв'язки між державою та приватними хакерами, оскільки багато приватних хакерських груп ідентифікують себе з китайським націоналізмом. В єдиному доступному систематичному дослідженні на цю тему Гендерсон оцінює, що близько 380000 осіб тісно пов'язані з націоналістичними хакерськими групами в Китаї [352].

Росія – це інша авторитарна країна, яку підозрюють (на наш погляд, цілком обґрунтовано) у створенні довгострокових альянсів з приватними хакерськими угрупованнями. На думку деяких експертів, російські силові структури та націоналістичне хакерське співтовариство пов'язані через молодіжні організації, такі як «Наші» або «Євразійський рух молоді» [270]. Кіберзлочинність також може служити базою для рекрутингу в силові структури. А у DDoS-атаках на російські опозиційні сайти підозрюються як аматорські хакерські групи, так і професійні кіберзлочинці.

Багато інших авторитарних режимів скопіювали такий підхід. Президент Сирії Асад, наприклад, високо оцінив так звану «Сирійську електронну армію» як реальну армію у віртуальній реальності [там само]. Інші хакерські групи називають себе пакистанськими, іранськими або ізраїльськими націоналістами [357; 358]. За винятком Ізраїлю, мало які демократичні уряди, ймовірно, могли б розраховувати на допомогу приватних хакерських груп. Зовсім навпаки: більшість західних хакерів дуже

критично ставляться до ролі державних органів в кіберпросторі і навряд чи підпорядкували б себе їм в період кризи.

Нарешті, що стосується оборонних можливостей, то тут знову важливі як ресурси, так і взаємини між державою та суспільством. Але ще більш важливими є політичні обмеження. Ці обмеження в першу чергу відносяться до демократичних держав. У Китаї всі критичні вузли мереж прямо або побічно контролюються урядом. На відміну від цього, органи безпеки США юридично обмежені тільки захистом урядових мереж. Агентство національної безпеки (АНБ) і Міністерство національної безпеки (МНБ) не можуть протистояти атакам на приватні мережі. ФБР також може розслідувати випадки кіберзлочинів тільки після нанесення збитку. І потрібні були роки, щоб почати пілотний проект, що дозволяє АНБ і МНБ співпрацювати з великими оборонними компаніями США. Спочатку ідея полягала в тому, що в обмін на інформацію про нові вразливості і загрози від компаній потрібно було б інформувати служби безпеки про вторгнення в мережі і дозволяти урядовим групам проводити криміналістичну експертизу цих інцидентів [347]. Однак після того, як активісти руху за громадянські права і частина самої адміністрації виступили з масовими запереченнями, проект довелося скоротити, і на даний час відповідальність за фактичні заходи захисту, як і раніше лежить виключно на компаніях. Це є хорошим прикладом політичних та законодавчих обмежень кібербезпеки під керівництвом держави в разі демократичних політичних систем.

Зрештою, які наслідки цього складного пазла силових потенціалів щодо міжнародного співробітництва? Давайте просто візьмемо приклади з Конвенції проти кіберзлочинності. Чому авторитарні держави повинні виступати проти більш узгоджених зусиль по боротьбі з кіберзлочинністю? Чому такі держави, як Росія, відмовляються приєднатися до Конвенції? Хіба російські громадяни і бізнес не стають жертвами кіберзлочинців? Насправді, це так. Але інші країни, ймовірно, більше страждають від кіберзлочинності, ніж Росія. Отже, приєднання Росії до Конвенції принесло б більше користі

іншим країнам, ніж самій Росії. Тут слід повторити, що приватні хакери, відіграють певну роль в портфелі російських атак. Вони ще більш важливі в китайському стратегічному мисленні, в той час як у багатьох західних країнах безпекові структури та приватні хакерські угрупування в кращому випадку терплять один одного. Тому і у Росії, і у Китаю є додаткові причини очікувати від Конвенції менших вигод, ніж у західних країн. Наслідки з точки зору неореалізму очевидні: до тих пір, поки не будуть прийняті заходи по компенсації відносних вигод, Росія та Китай утримуватимуться від співпраці в боротьбі з кіберзлочинністю.

Слід зазначити, що Конвенція спрямована тільки проти приватних суб'єктів в кіберпросторі, а не проти діяльності держави. Існують навіть конкретні положення Конвенції, які можуть бути витлумаченими як лазівка для проведених під керівництвом держави розвідувальних операцій. Так, члени Конвенції можуть відмовитися від співпраці в окремих випадках, якщо вони посилаються на міркування національної безпеки [283]. Зрозуміло, вони можуть також використовувати це положення в якості прикриття діяльності союзних приватних хакерів. Але з того, що зазначалось вище, можна припустити, що кібератаки під керівництвом держави в середньому будуть менше і важче виявлятися, ніж атаки приватних хакерських груп. І держави не зможуть щодня переконливо посилатися на міркування національної безпеки. Таким чином, стратегії, засновані на численних атаках під керівництвом приватних осіб, а не на кількох складних операціях, що здійснюються під керівництвом держави, будуть відносно більш обмеженими відповідно до Конвенції. Вони також будуть більшою мірою обмежені міжнародною нормою «відповідальності держави» в цьому питанні. Оскільки Китай та Росія активно використовують кіберзброю, вони не можуть не утриматися від обох ініціатив, і тільки компенсаційні міжнародні угоди можуть змінити ці розрахунки.

З усіх можливих компенсацій деякі види заходів зміцнення довіри (СТВМ), що забезпечують, принаймні, обмежену гарантію від військових

кібератак, можуть мати найкращі шанси бути реалізованими. Держави можуть домовитися про декларування незастосування таких заходів першими, мораторій на атаки на критично важливі об'єкти інфраструктури та про проведення регулярних переговорів між воєначальниками високого рівня. Росія та Китай, можливо, могли б розцінювати ці кроки як відносний виграш, обумовлений нібито наявними у США передовими можливостями для нанесення ударів. Крім того, США мають кращу репутацію в плані виконання міжнародних зобов'язань по контролю над озброєннями, ніж колишній Радянський Союз та інші авторитарні країни. Однак, крім СТВМ, простір для компромісів досить обмежений. Авторитарні країни, безумовно, вітали б деякі розпливчасті угоди щодо обмеження контенту, які вони могли б використовувати в якості законного прикриття для внутрішньої Інтернет-цензури та діяльності зі спостереження у кіберпросторі. Держави-члени Шанхайської організації співпраці (ШОС), в тому числі Росія та Китай, вже виступили із заявою, що засуджує так звану інформаційну війну. Під цим вони мають на увазі передачу контенту, який нібито порушує внутрішній світ в суспільствах [337]. Проте, здається, що немає ніяких шансів, що західні держави погодяться з цими умовами. Принаймні, в разі США це було б навіть неконституційно. Таким чином, міжнародна угода, яка може вирішити проблему відносних вигод, все ще залишається під великим питанням.

Висновки до третього розділу

Розгляд практичних аспектів забезпечення кібербезпеки у публічному секторі дав можливість зробити такі висновки:

1. Встановлено, що інтеграція цифрового світу в повсякденне життя громадян привела до збільшення їх попиту як користувачів на прозорість публічного управління, доступ до інформації та її доступність, а також на можливість отримання зворотного зв'язку з органами влади та іншими публічними організаціями. Органи влади багатьох країн за останні десять

років стали активними учасниками так званого «цифрового руху», який згодом назвали «уряд 2.0» або просто «Gov 2.0», у якому важливе місце посідають соціальні мережі. При цьому одним з ключових питань політики кібербезпеки, що стоять перед публічними чиновниками при розгляді рішень про те, як краще за все впровадити соціальні мережі в діяльність публічних організацій, є питання забезпечення належного балансу між управлінням ризиками і створенням дійсно відкритого уряду. Це не дивно, оскільки існує природне протиріччя між характеристиками відкритого уряду, – відкритими даними, відкритим доступом, прозорістю і підзвітністю, – і проблемами забезпечення безпеки.

2. З'ясовано, що особливо в соціальних мережах найбільш реальною загрозою безпеки може бути ненавмисне розкриття потенційно компрометуючої інформації або непублічних даних недбалими публічними службовцями. У той же час, більша частина привабливості соціальних мереж полягає в їх здатності «пов'язувати» велику кількість людей в режимі реального часу. Тому в режимі реального часу Gov 2.0 надає великі можливості, в тому числі можливість інформувати учасників про різні деталі по мірі того, як відбуваються події, і надавати відкриті канали, які можуть негайно з'єднати різних акторів. Однак взаємодія в реальному часі також може не давати достатньо часу і концентрації зусиль для надання правильних відповідей, і збільшує ймовірність того, що публічні службовці можуть надати інформацію, яка ще не була перевірена, відповідно, може завдати шкоди безпеці. Крім того, експонентне щоденне зростання соціальних мереж, сервісів і додатків надає численні нові потенційні точки входу в комп'ютерні мережі. Це одна з найбільш основних і очевидних загроз, яку не можна ігнорувати.

3. Визначено, що правові, технічні та процедурні заходи й організаційні структури щодо забезпечення кібербезпеки повинні бути зроблені / створені на національному рівні, а також узгоджені на міжнародному рівні в такий спосіб: національні закони повинні прийматися

там, де їх ще немає, а існуючі закони, а також регіональні та міжнародні угоди повинні ґрунтуватися на загальному розумінні того, що являють собою загрози кібербезпеки; технічні рішення повинні бути визначені та розроблені з урахуванням загальноприйнятих стандартів, спрямованих на забезпечення базових показників безпеки апаратного та програмного забезпечення, які можуть бути прийняті виробниками, постачальниками і кінцевими користувачами; необхідно на національному рівні створити відповідні організаційні структури, такі як центри та групи координації та реагування (наприклад, групи реагування на комп'ютерні інциденти), щоб швидко реагувати на кібератаки і координувати дії зі своїми колегами на міжнародному рівні.

4. Аналізуючи діяльність міжнародних організацій у сфері кібербезпеки, було визначено декілька важливих напрямків дій, які повинні бути реалізовані в Україні для підвищення національної кібербезпеки в цілому і публічного сектора зокрема, а саме: 1) гармонізація національного законодавства в сфері кібербезпеки із законодавством ЄС; 2) впровадження стандартів і рекомендацій, розроблених МСЕ, які стосуються технічних аспектів забезпечення кібербезпеки; 3) створення на національному та регіональних рівнях спеціальних організаційних структур і команд протидії кіберзагрозам різного характеру; 4) реалізація масових освітніх програм, спрямованих на формування безпечної поведінки в кіберпросторі; 5) розширення міжнародного співробітництва в сфері кібербезпеки, участь в реалізації різних ініціатив у цій сфері. Також було визначено низку загальних аспектів, які повинні бути присутніми в політиці та стратегії кібербезпеки в Україні. До таких аспектів слід віднести: посилення координації органів влади на політичному та оперативному рівнях; зміцнення публічно-приватного співробітництва; покращення міжнародного співробітництва; повага до фундаментальних цінностей; урахування питань суверенітету при розробці політики в сфері кібербезпеки; гнучкий підхід до формування та реалізації політики; важливість економічних аспектів кібербезпеки;

важливість діалогу за участю багатьох зацікавлених сторін.

5. З огляду на сучасну спрямованість на багатосуб'єктність у забезпеченні кібербезпеки, яка передбачає співпрацю публічного, приватного і третього секторів, було сформульовано ряд пропозицій для підвищення ефективності стратегій і політики кібербезпеки, а саме: 1) спільна систематична оцінка відповідності заходів кібербезпеки, пропонованих органами влади, іншим ініціативам у сфері кібербезпеки. Наприклад, законодавство, яке встановлює кримінальну відповідальність за хакерство, могло б взяти до уваги, що деякі дослідження сприяють підвищенню кібербезпеки, використовуючи такі ж методи, як і хакери; 2) публічні організації як власники і оператори інформаційних систем і мереж можуть подавати приклад іншим акторам, застосовуючи передовий досвід, технології і навіть законодавчі вимоги. Технології, розроблені для одного із секторів, також можуть принести користь іншим секторам; 3) політики можуть звернутися за порадою до технічного товариства Інтернету якомога раніше в процесі розробки політики, щоб уникнути прийняття технологічно помилкових рішень; 4) політика в сфері кібербезпеки може стимулювати розробку відкритих стандартів, що дозволяють впроваджувати інновації для рішень у даній сфері, спираючись на шанованих в експертному співтоваристві і таких, що добре зарекомендували себе, фахівців зі стандартизації Інтернету, уникаючи при цьому односторонньої зміни стандартів Інтернету; 5) слід заохочувати збір емпіричних даних, щоб краще оцінювати актуальність стратегій і політик, а також підтримувати підходи, засновані на оцінці ризиків. Для протидії існуючим перешкодам, з якими багато акторів стикаються при наданні додаткової інформації про кіберінциденти, слід виділяти додаткові ресурси і впроваджувати узгоджені механізми повідомлення про порушення безпеки, з якими стикаються представники всіх трьох секторів.

6. Доведено, що політика кібербезпеки в Україні повинна ґрунтуватися на таких принципах: впровадження стратегічного підходу до

забезпечення кібербезпеки; комплексне вирішення проблем кібербезпеки, включаючи використання ефективних механізмів координації, адаптованих до культури і стилю управління в країні; своєчасність, гнучкість і адаптивність у прийнятті рішень у сфері забезпечення кібербезпеки; розвиток національного потенціалу команд з протидії кіберінцидентам; впровадження передових методів забезпечення кібербезпеки; покращення захисту критично важливих інформаційних інфраструктур; повага до фундаментальних цінностей свободи інформації, але з використанням належних запобіжних заходів, стримувань і противаг; підвищення кіберграмотності суспільства; використання системи стимулів для розвитку сфери кібербезпеки і відповідного кадрового потенціалу; співпраця з приватними та неурядовими організаціями, розвиток публічно-приватного партнерства; посилення боротьби з кіберзлочинністю; заохочення досліджень і розробок у сфері кібербезпеки; розвиток міжнародного співробітництва, зокрема, шляхом участі в розробці загальних норм поведінки в кіберпросторі.

РОЗДІЛ 4
ЗАПОБІГАННЯ ТА ПРОТИДІЯ КІБЕРЗАГРОЗАМ В ПУБЛІЧНОМУ СЕКТОРІ УКРАЇНИ: СОЦІОЛОГІЧНИЙ АНАЛІЗ

4.1. «Цифровізація» в Україні: сучасний стан та проблеми

З метою з'ясування інформації щодо стану кібербезпеки в Україні в сучасних умовах та пошуку шляхів підвищення рівня захисту кіберпростору в Україні у період з 24 жовтня по 3 листопада 2020 р. автором за сприяння кафедри політології та філософії Харківського регіонального інституту державного управління було проведено всеукраїнське експертне соціологічне опитування.

До складу експертної групи входили: керівники державних та комунальних підприємств, представники великого і середнього бізнесу, банківських структур, керівники громадських організацій, депутати різних рівнів, працівники органів виконавчої влади та місцевого самоврядування, політичні аналітики, журналісти.

Виходячи з мети, було сформульовано такі основні завдання дослідження:

– оцінка нинішнього стану кібербезпеки (під якою в дослідженні розумілася захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [179, Ст.1]) в Україні в цілому, та на рівні окремих організацій і установ;

– визначення основних кіберзагроз для Україні в цілому, та для сфери публічного управління, зокрема,

– визначення рівня цифровізації публічного управління в Україні;

– з‘ясування рівня «цифрової грамотності» працівників різних сфер;

– визначення основних чинників, що негативно впливають на рівень кібербезпеки України в цілому, та сфери публічного управління, зокрема;

– встановлення основних шляхів підвищення рівня кібербезпеки в Україні, в цілому, та в сфері публічного управління, зокрема.

Загальна кількість респондентів на цьому етапі дослідження склала 1007 осіб. Відповідно до результатів опитування експерти розподілилися (у % до тих, які відповіли):

за статтю:

чоловіків – 30; жінок – 70;

за віком:

від 18 до 35 років – 27; від 36 до 45 років – 38;

понад 46 років – 35;

за освітою:

мають вчений ступінь – 2; закінчили аспірантуру (без ступеня) – 2;

вища – 94; незакінчена вища – 1;

середня спеціальна – 1;

за профілем освіти (можна було вказати декілька варіантів, тому сума складає більше 100%):

гуманітарний – 8; технічний – 19; економічний – 74;

юридичний – 11; природничо-науковий – 1; сільськогосподарський – 1;

військовий - 1 публічне управління – 13; інший – 1.

за місцем проживання:

обласний центр – 68; селище/село – 3;

місто з населенням більше 50 тис. – 20; інше – 3.

місто з населенням менше 50 тис. – 4;

селище міського типу – 2;

за характером роботи:

вище керівництво організацій – 3; заступник керівника організації – 3;

керівники середнього рівня (начальник управління) – 17; керівники нижнього рівня (начальник відділу, сектору) – 17; спеціалісти – 57; інше – 3.

<u>за кількістю працівників в організації:</u>

до 10 осіб– 3; 10-20 осіб – 2; 20-30 осіб – 1; 30-40 осіб – 1; більше 40 осіб – 90; інше – 3.

81% опитаних працюють в органах публічного управління.

<u>За стажем роботи в них вони розподілилися:</u>

до 3 років – 8; від 6 до 10 років – 16; від 3 до 5 років – 7; від 11 до 15 років – 19; від 16 до 20 років – 18; понад 20 років – 25; інше – 7%

Усі цифри у розділі наводяться у % до тих опитаних, які відповіли на запитання.

Оцінюючи ступінь розвитку цифровізації в Україні (а під нею у дослідженні розумілося насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір [2]), відносна більшість експертів визначили його як середній (рис. 4.1).

Найнижче серед усіх категорій опитаних рівень «цифровізації» в Україні оцінили опитані, які працюють в приватному секторі економіки. Серед них 43% визначили його як низький (у середньому по масиву 27%) і лише 32% як середній (відповідно 42%).

Говорячи про відповідний рівень «цифровізації» у своєму місті /районі, експерти висловили схожі із попередніми оцінки (рис. 4.2.).

Однак, у цьому разі привертає увагу відсутність істотної різниці в оцінках між мешканцями обласного центру і «провінції» (рис. 4.3).

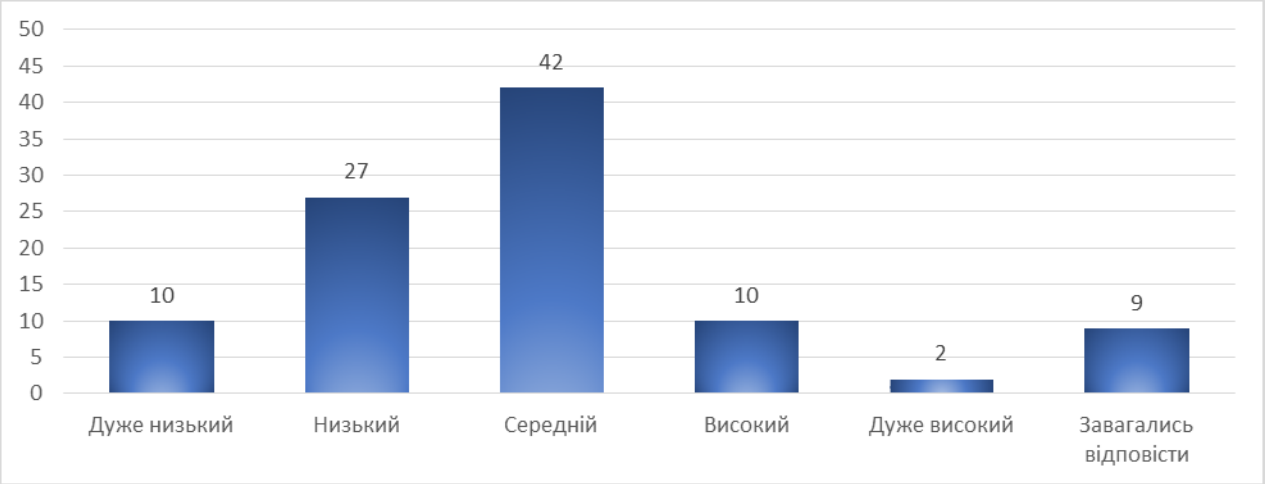

Рис.4.1. Загальна оцінка рівня цифровізації в Україні

Рис.4.2. Оцінка рівня цифровізації в місті/районі, де мешкають респонденти

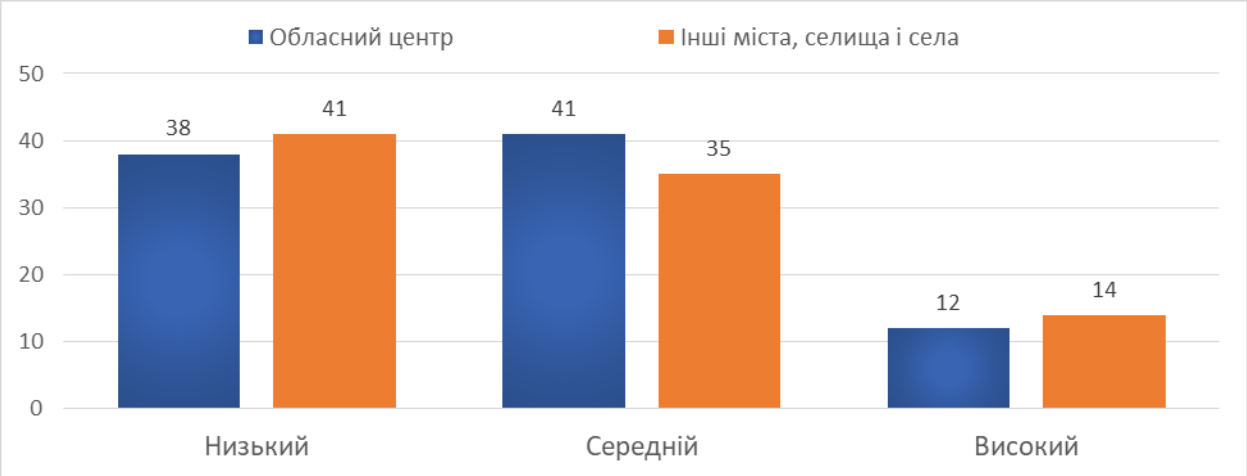

Рис.4.3. Оцінка рівня «цифровізації» в населених пунктах, де проживають респонденти (у % до тих, які відповіли у кожній групі)

Таким чином, можна стверджувати, що в межах всієї країни рівень «цифровізації» є приблизно однаковим.

Схожими і є думки респондентів щодо рівня розвитку електронного урядування в Україні (рис. 4.4.). Відносна більшість опитаних визнає його середнім. При цьому оцінки експертів, що працюють в органах публічного управління, є більш високими у порівнянні з іншими опитаними (рис. 4.5).

Середнім відносна більшість опитаних визнає і рівень розвитку електронного урядування у їхніх містах та районах (рис. 4.6).

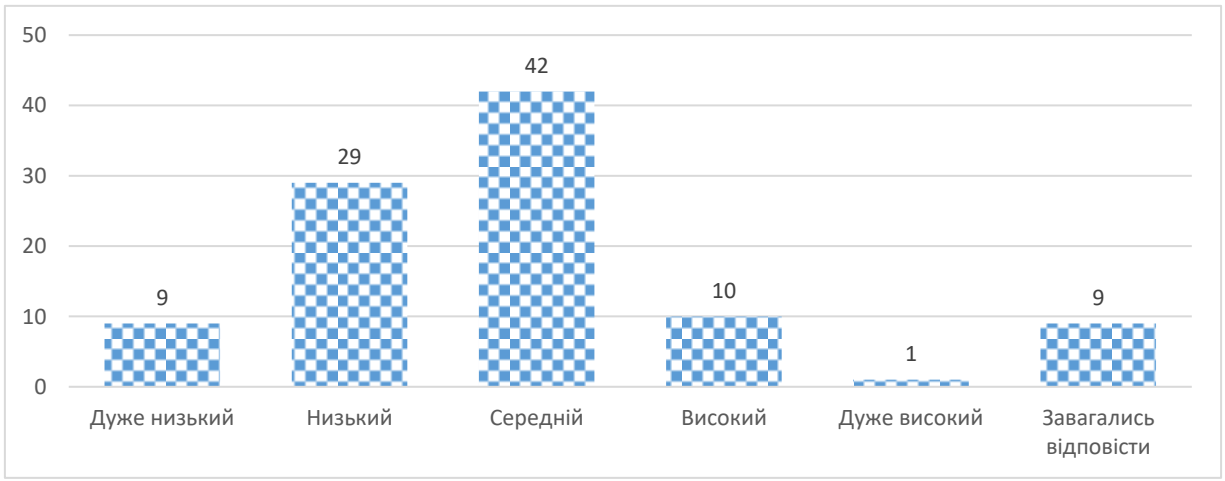

Рис.4.4. Оцінка рівня розвитку електронного урядування в Україні

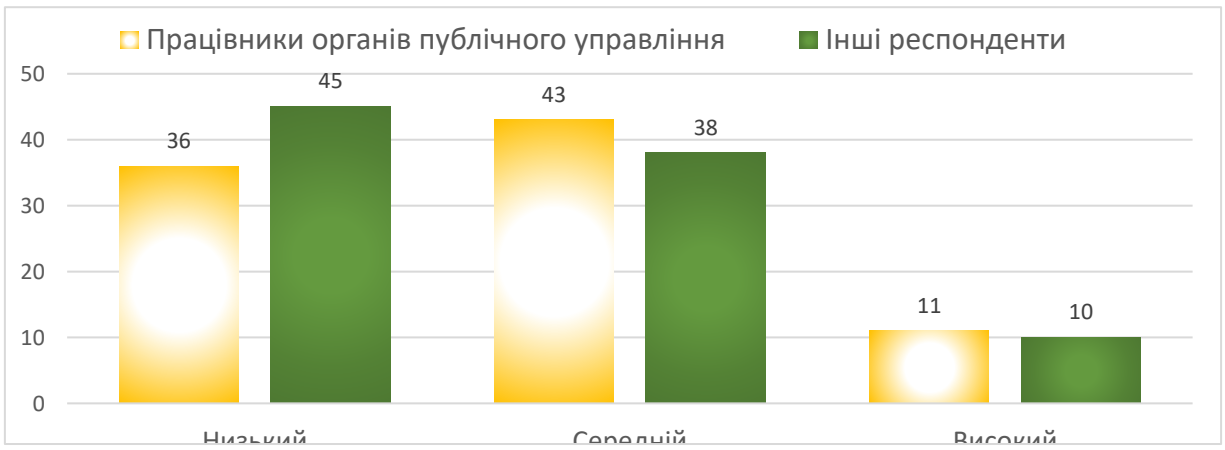

Рис.4.5. Порівняльні оцінки рівня розвитку «електронного урядування» в Україні працівниками органів публічного управління та іншими експертами (у % до опитаних у кожній групі)

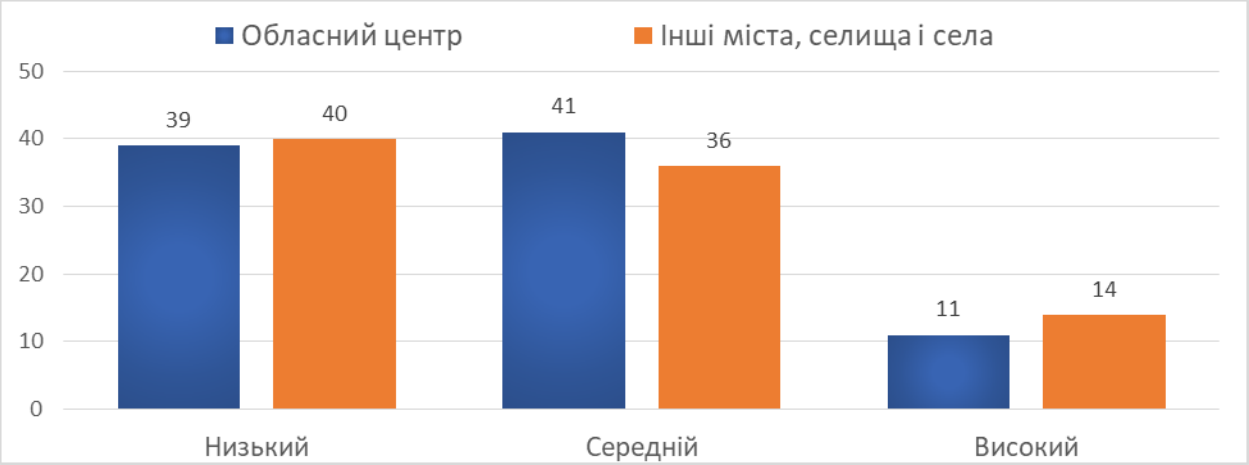

Рис.4.6. Оцінка рівня електронного урядування в населених пунктах, де проживають респонденти (у % до тих, які відповіли у кожній групі)

Говорячи про окремі складові «цифровізації» та розвитку електронного урядування, привертають увагу як позитивні, так і негативні моменти.

Серед позитивного: переважна більшість опитаних (99%), і зокрема, працівників органів публічного управління (99%), мають на своєму робочому місці персональний комп'ютер. Однак рівень продуктивності комп'ютерів в «публічному секторі» значно поступається «приватному сектору». Так, якщо в публічному секторі 36% оцінили свій комп'ютер як продуктивний, то в приватному – 50%. Порівняльний аналіз наведено на рис. 4.7.

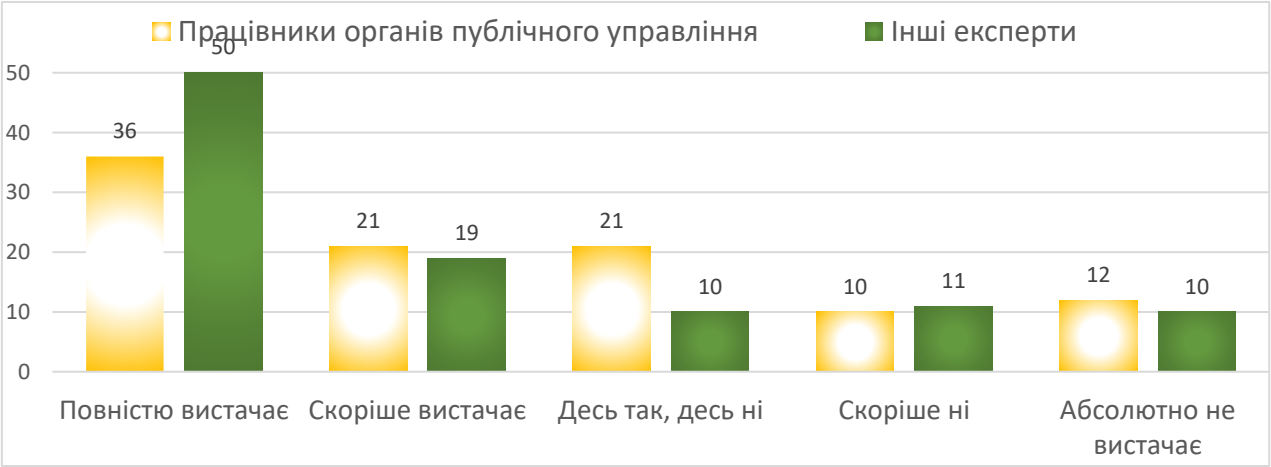

Рис.4.7. Оцінка рівня продуктивності персонального комп'ютера, на якому працюють експерти (у % до тих, які відповіли у кожній групі)

Таким чином, можна констатувати перший негативний момент – рівень продуктивності комп‘ютерів, що використовуються в роботі, в публічному секторі є нижчим, ніж у приватному.

Наступна проблема – це рівень забезпечення робочих місць організаційною технікою. В органах виконавчої влади та органах місцевого самоврядування він є значно гіршим порівняно з іншими організаціями та установами. Так, в органах публічного управління лише третина опитаних (33%) зазначила, що у них є вся необхідна організаційна техніка. Серед інших експертів – таких більше половини (52%). Порівняльний розподіл відповідей експертів наведено на рис. 4.8.

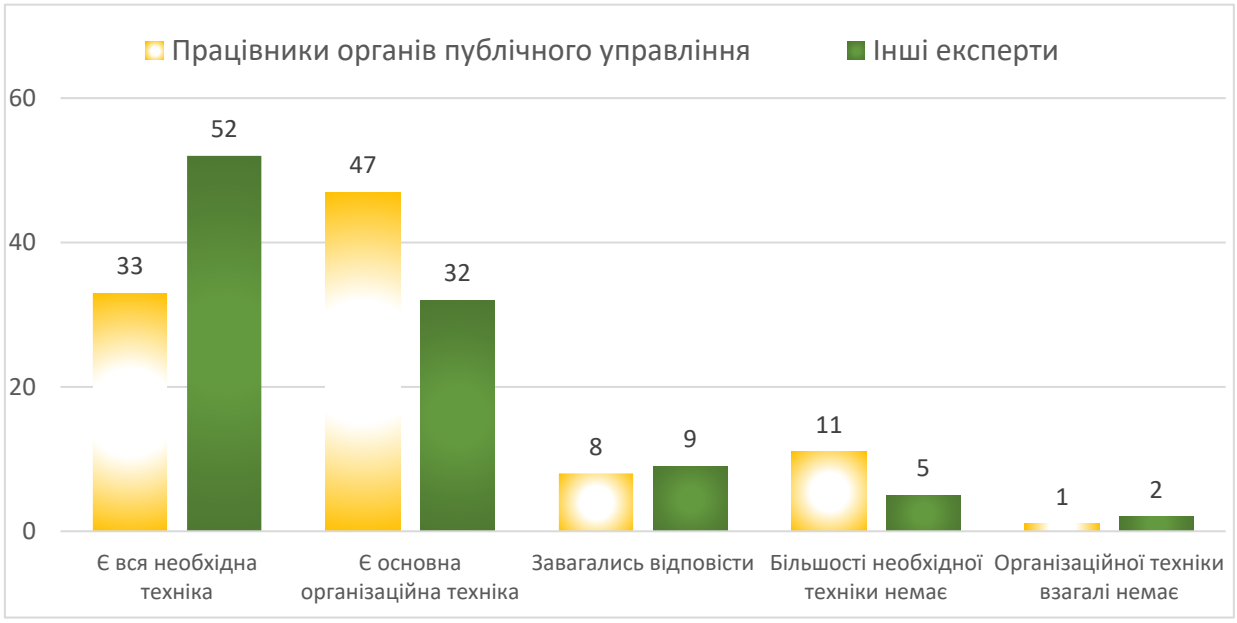

Рис.4.8. Порівняльна оцінка рівня забезпечення опитаних організаційною технікою, необхідною для виконання посадових обов‘язків (у % до тих, які відповіли у кожній групі)

До речі, відмінності спостерігаються і у відповідях респондентів, які мешкають і працюють в різних населених пунктах. Ті, хто працює в обласних центрів – краще забезпечені організаційною технікою ніж ті, хто працює в провінції (рис.4.9).

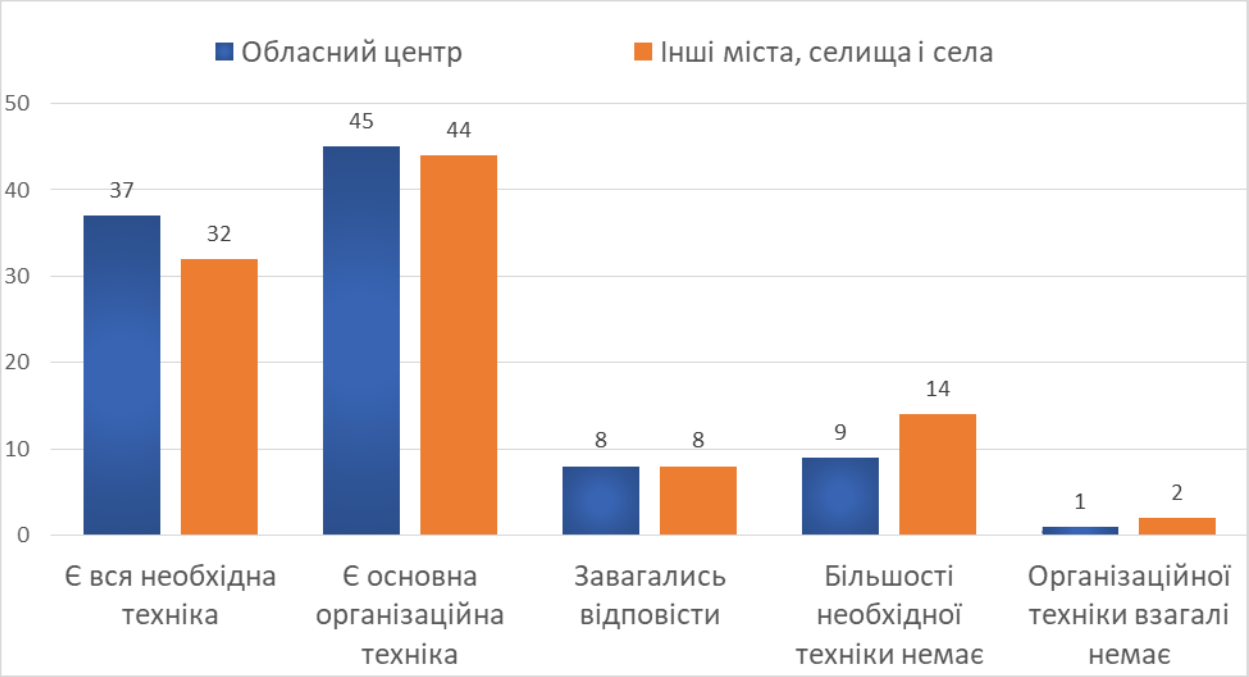

Рис.4.9. Оцінка рівня забезпечення організаційною технікою робочих місць в населених пунктах, де працюють респонденти (у % до тих, які відповіли у кожній групі)

Ще більш показовим є розрив в рівні продуктивності організаційної техніки між «публічним» та «приватним» сектором (рис.4.10).

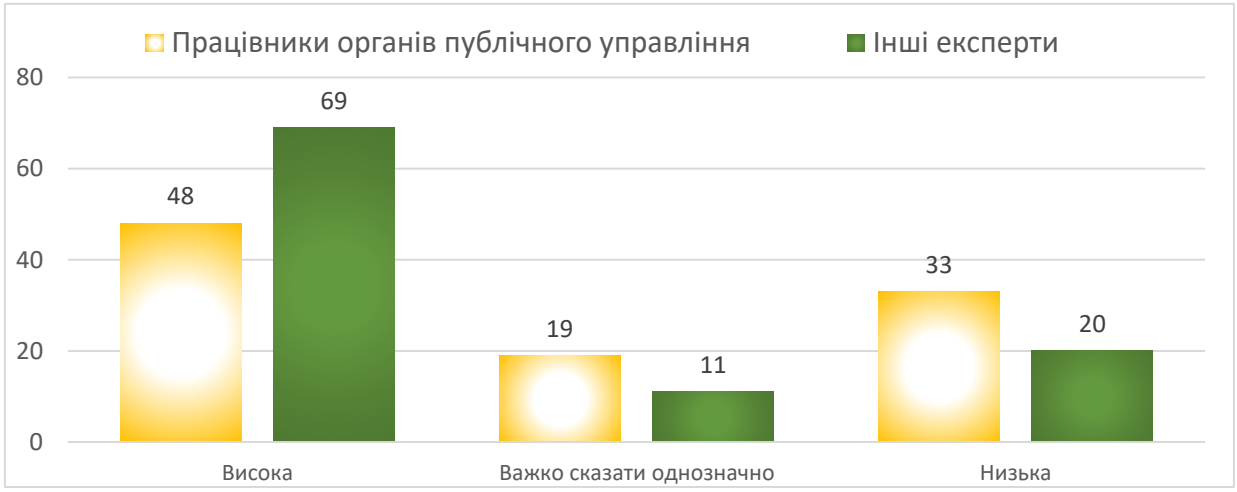

Рис.4.10. Оцінка рівня продуктивності організаційної техніки, якою обладнані робочі місця опитаних (у % до тих, які відповіли у кожній групі)

Як видно з наведеного вище, рівень продуктивності комп‘ютерної та організаційної техніки, якою користуються працівники органів публічного управління, є порівняно невисоким. А це, як наслідок, негативно впливає на якість їх праці.

Між тим, рівень вимог до працівників органів публічного управління останнім часом значно виріс. Як показало проведене дослідження, сучасні працівники органів публічного управління для ефективного виконання своїх функціональних обов‘язків повинні володіти: технологіями електронного документообігу (90%); електронним листуванням (74%); технологіями он-лайн комунікації (65%); інтернет-месенджерами (53%).

Між тим, порівняння необхідного та наявного, тобто такого, що безпосередньо використовують працівники органів публічного управління в своїй роботі, визначає високий рівень їх потреб в удосконаленні вмінь щодо використання технологій електронного документообігу та он-лайн комунікацій. Порівняльний аналіз відповідей наведено на рис. 4.11.

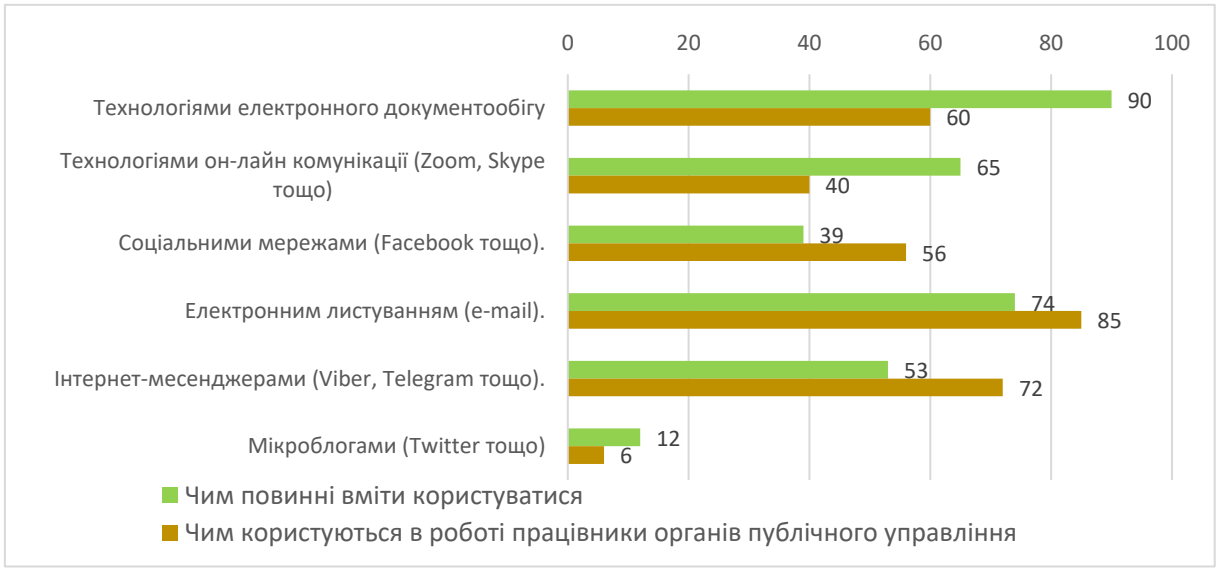

Рис. 4.11. Порівняльний аналіз відповідей всіх експертів щодо того, чим повинні вміти користуватися працівники органів публічного управління (у % до всіх, які відповіли) та них самих щодо того, чим вони користуються в своїй роботі (у % до тих, хто відповіли у даній категорії респондентів)

Позитивним моментом і наслідком «цифровізації» та інформатизації суспільства стало майже повсюдне поширення інтернету (рис. 4.12). І у публічному, і у приватному секторі 92% опитаних мають можливість виходу до всесвітньої мережі на своєму робочому місці.

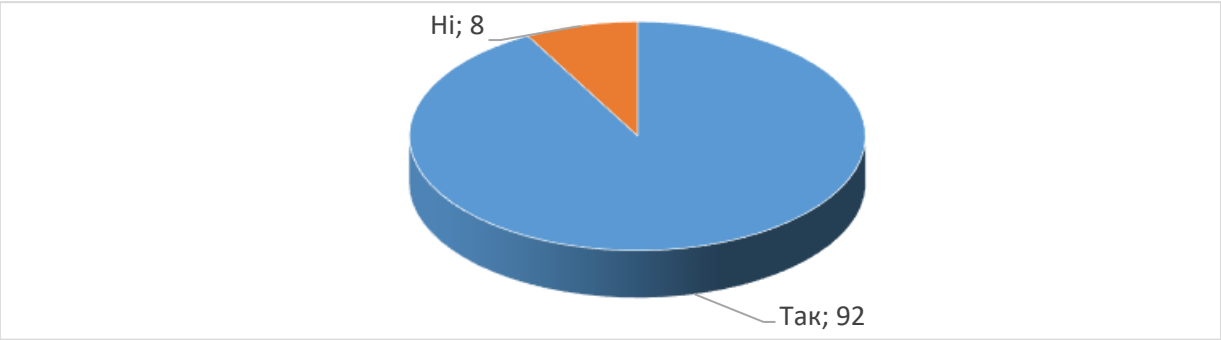

Рис. 4.12. Розподіл відповідей опитаних на запитання «Чи маєте Ви доступ до інтернету на робочому місці?»

У той же час швидкість інтернету не скрізь є однаковою. Як доводять результати дослідження, в «публічному секторі» вона є порівняно низькою (рис. 4.13).

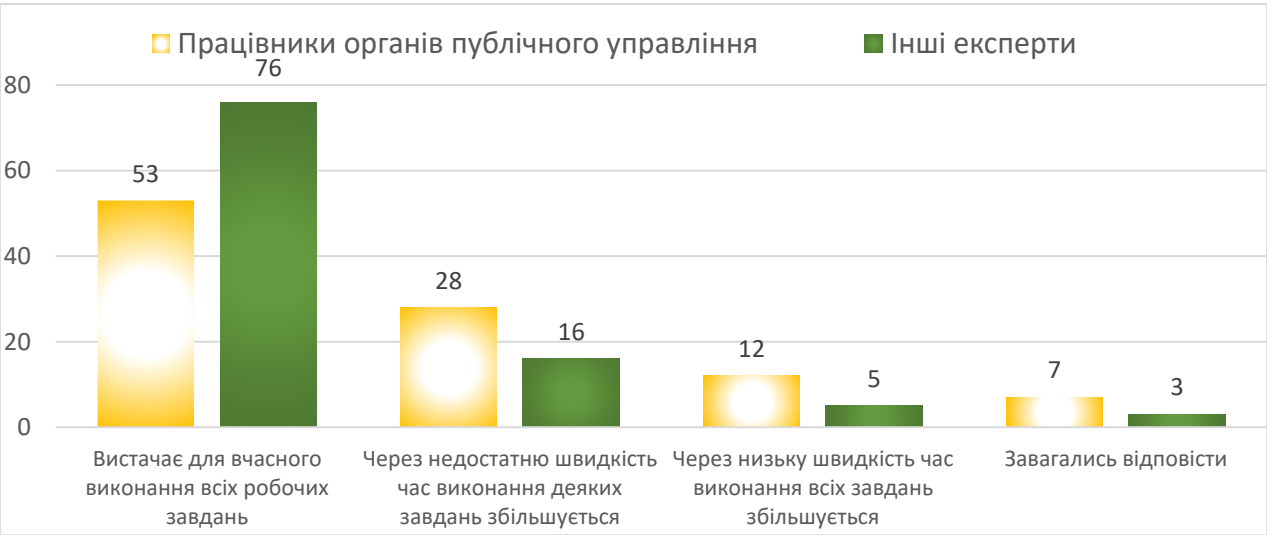

Рис. 4.13. Оцінка рівня швидкості інтернету на робочому місці у працівників органів публічного управління та інших експертів (у % до тих, які відповіли у кожній групі)

При цьому у працівників, які займають керівні посади в своїх організаціях, швидкість інтернету є трохи вищою, ніж у рядових працівників (рис.4.14).

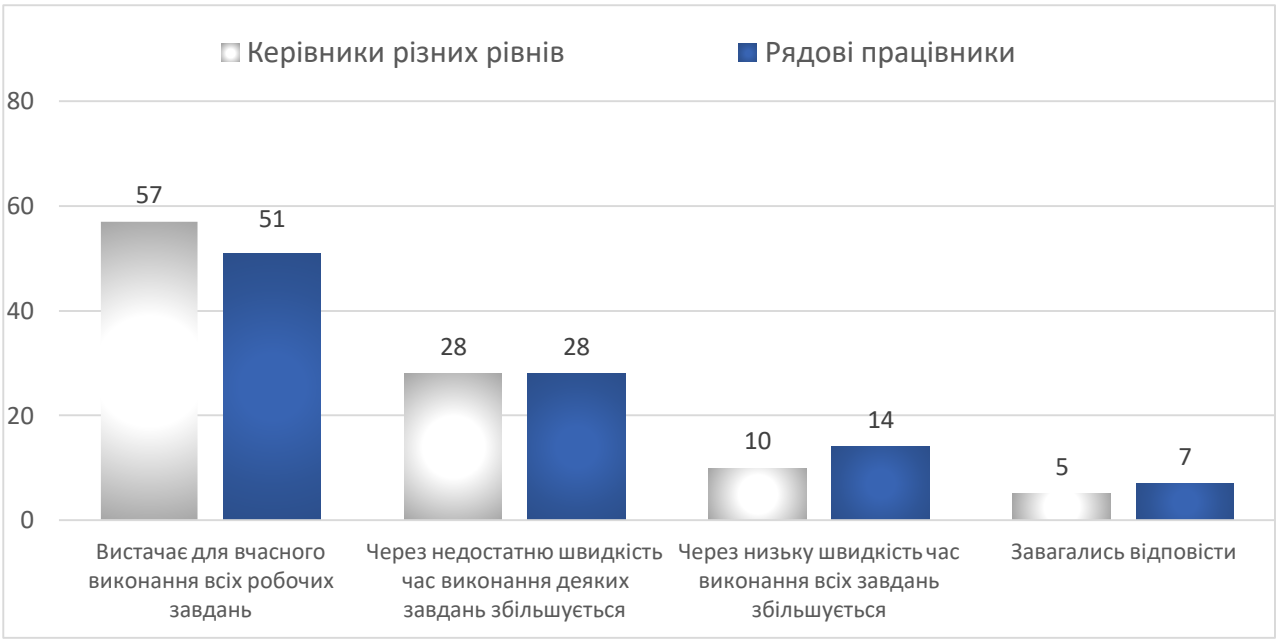

Рис.4.14. Порівняльна оцінка рівня швидкості інтернету на робочому місці у працівників органів публічного управління, що займають і не займають керівні посади (у % до тих, які відповіли у кожній групі)

Таким чином, за результатами проведеного дослідження, можна спостерігати цілу низку «цифрових нерівностей», пов‘язаних з різним рівнем забезпечення опитаних комп‘ютерною та організаційною технікою, швидкістю інтернету та ін. Найбільш вразливою у цьому аспекті є категорія працівників органів публічного управління, які не займають керівні посади і працюють невеличких містах, селищах і селах. При цьому спільною для всіх працівників органів публічного управління є потреба в опануванні технологій електронного документообігу та он-лайн комунікацій, а також в підвищенні рівня особистої захищеності в кіберпросторі (під яким в опитуванні розумілося середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних

відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних). Останню тезу підтверджують відповіді опитаних на запитання «Чи відчуваєте Ви себе безпечно в сучасному кіберпросторі?» (рис. 4.15).

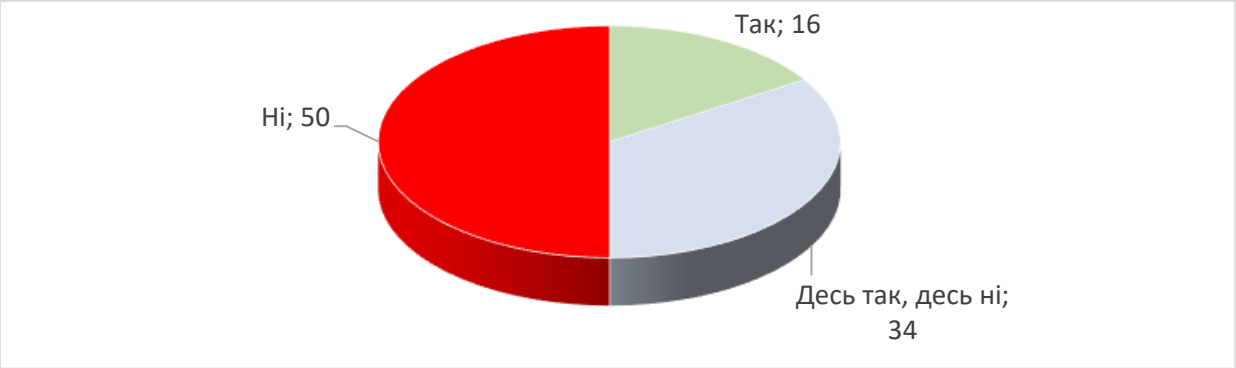

Рис. 4.15. Оцінка рівня особистої захищеності експертів в сучасному кіберпросторі

Цікаво, що найбільш захищеними себе почувають експерти віком до 35 років (21% серед них відзначили цей факт). Як наслідок, у всіх опитаних є достатньо високими потреби у знаннях і вміннях з кіберпитань (рис.4.16).

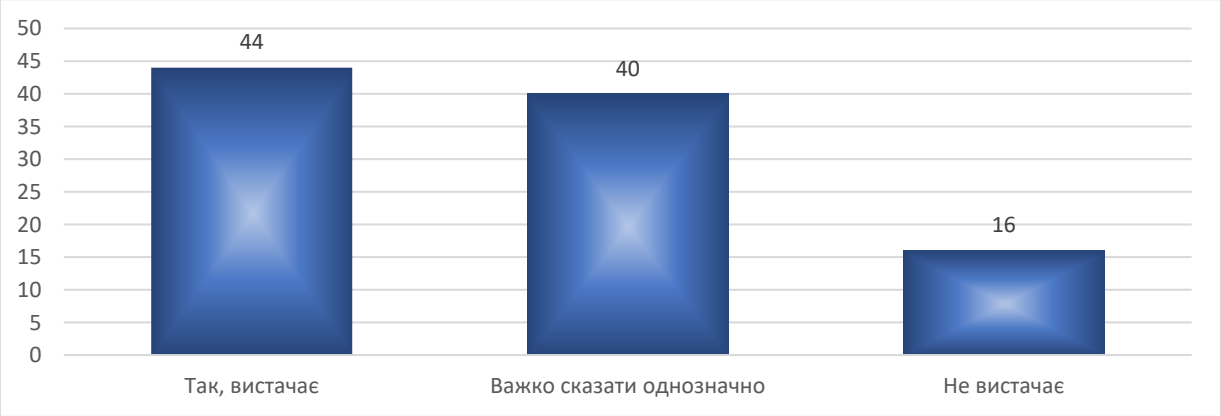

Рис. 4.16. Розподіл відповідей на запитання «Чи вистачає Вам знань, вмінь і навичок для використання сучасних інформаційних технологій і продуктів у своїй повсякденній професійній діяльності»

Більшими при цьому є потреби у таких знаннях, вміннях і навичках у працівників органів публічного управління (рис. 4.17).

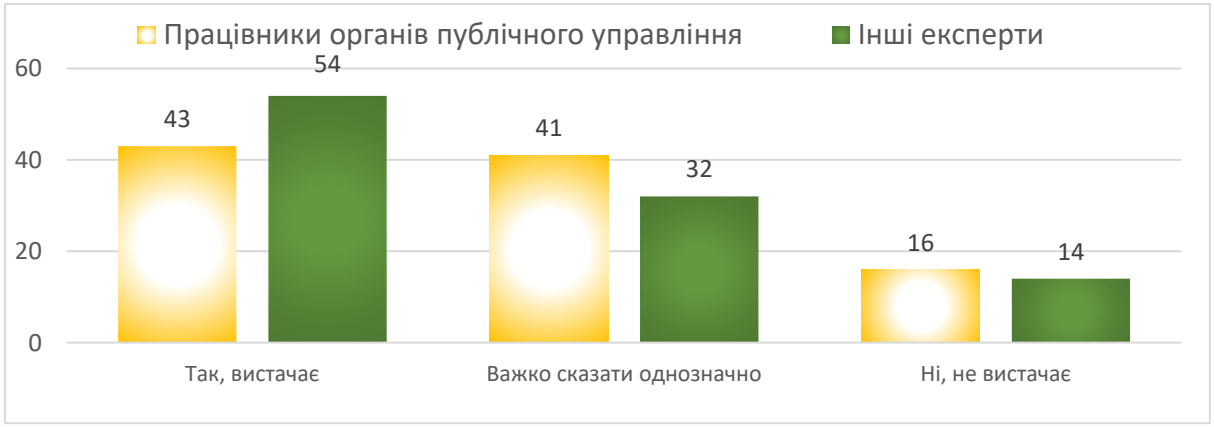

Рис. 4.17. Порівняльний розподіл відповідей працівників органів публічного управління та інших експертів на запитання «Чи вистачає Вам знань, вмінь і навичок для використання сучасних інформаційних технологій і продуктів у своїй повсякденній професійній діяльності» (у % до тих, які відповіли у кожній групі)

Серед вікових категорій опитаних порівняно високий рівень потреб відзначається у опитаних віком понад 35 років (рис. 4.18).

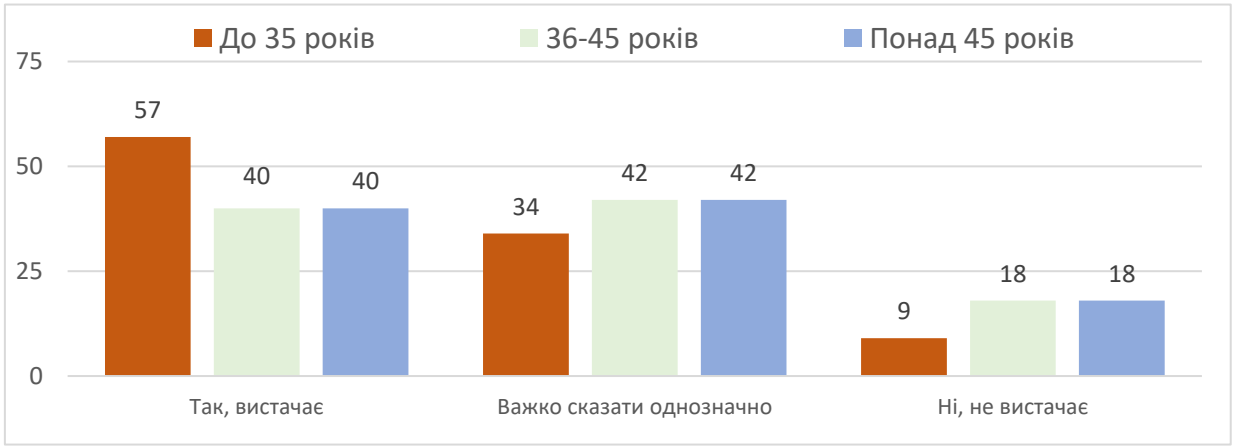

Рис. 4.18. Розподіл відповідей на запитання «Чи вистачає Вам знань, вмінь і навичок для використання сучасних інформаційних технологій і продуктів у своїй повсякденній професійній діяльності» серед представників різних вікових груп експертів (у % до тих, які відповіли у кожній групі)

Як наслідок, не дивно, що значна кількість опитаних хотіли б підвисити свій рівень обізнаності з кіберпитань (рис. 4.19). Найбільше серед усіх категорій опитаних у цьому зацікавлені експерти віком понад 45 років (88% у цій групі).

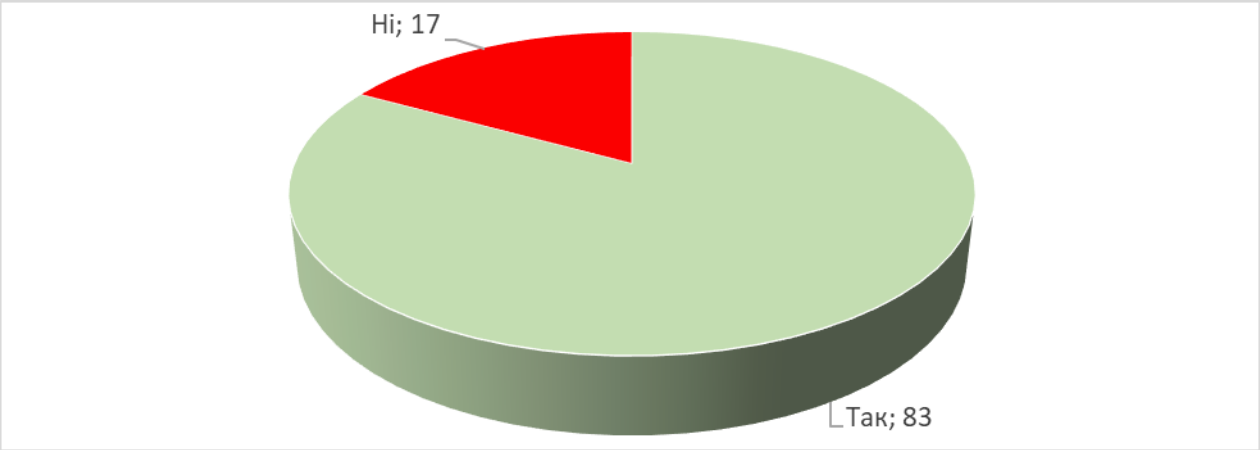

Рис. 4.19. Розподіл відповідей опитаних на запитання «Чи хотіли б Ви підвищити рівень своїх знань, вмінь і навичок щодо використання інформаційних технологій і продуктів у своїй повсякденній професійній діяльності»

Серед знань, вмінь і навичок, найбільш затребуваними у опитаних виявилися у сфері технологій електронного документообігу (81%). Серед працівників органів публічного управління, порівняно високими виявилися потреби у оволодінні технологіями он-лайн комунікацій (37%). Що в цілому відповідає наведеним вище результатам і об‘єктивно виявленим потребам.

При цьому опитані також дуже низько оцінюють рівень своїх знань, вмінь та навичок щодо захисту інформації своєї організації від кіберзагроз (рис. 4.20). Так, лише 21% опитаних визнали його високим. У той же час більше третини опитаних (37%) вважають його низьким або констатують повну відсутність таких знань. При цьому у працівників органів публічного управління рівень знань з питань протистояння організаційним кіберзагрозам є більш низьким порівняно з іншими респондентами (рис. 4.21).

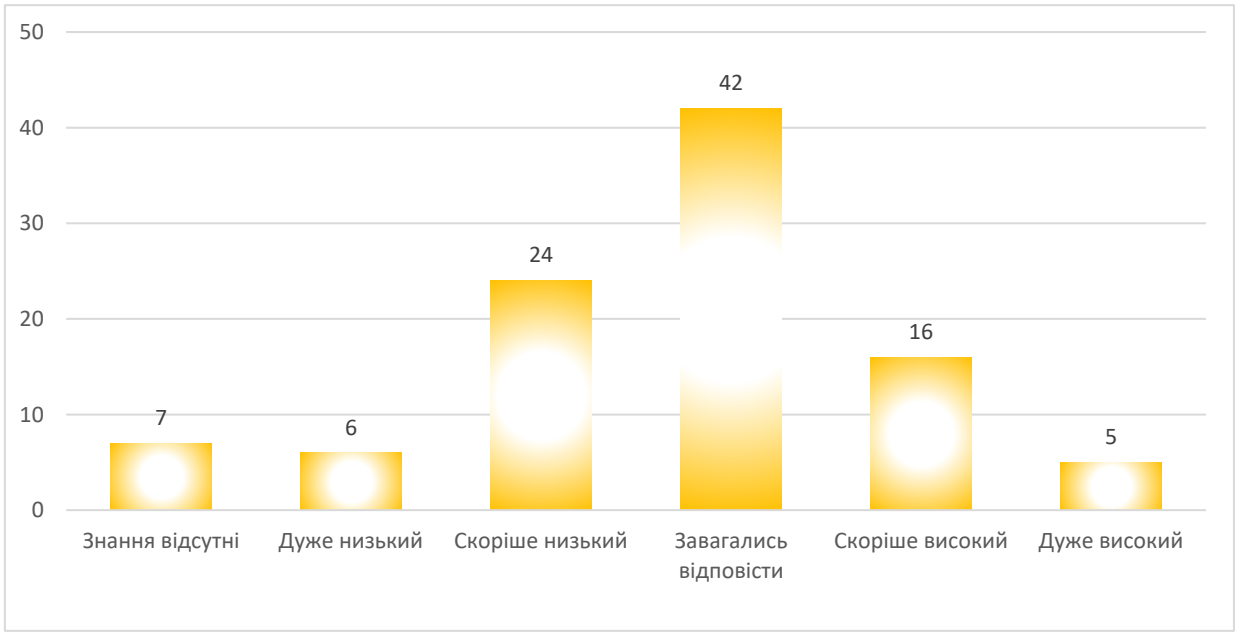

Рис. 4.20. Розподіл відповідей опитаних на запитання «Яким є рівень Ваших знань, вмінь та навичок щодо захисту інформації Вашої організації від кіберзагроз»

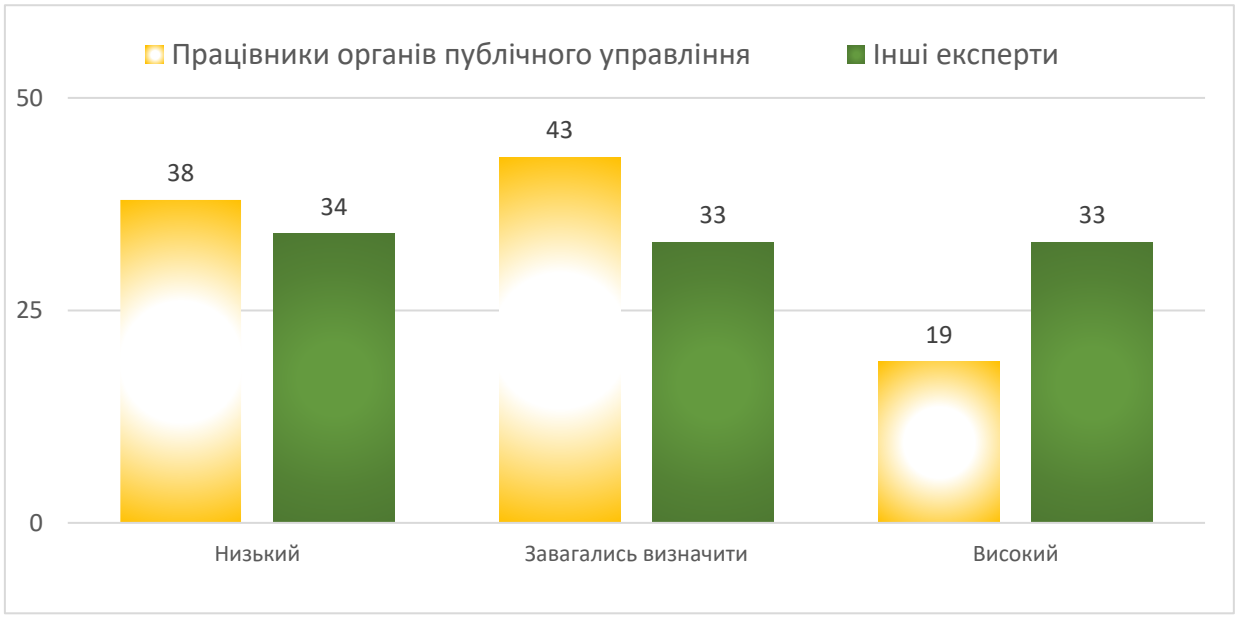

Рис. 4.21. Порівняльна оцінка рівня знань, вмінь та навичок щодо захисту інформації Вашої організації від кіберзагроз серед працівників органів публічного управління та інших експертів (у % до тих, які відповіли у кожній групі)

Привертає увагу і низький рівень обізнаності з питань протидії організаційним кіберзагрозам у опитаних віком понад 35 років (рис. 4.22). Негативно опитані оцінюють і рівень знань своїх колег з цього питання (рис. 4.23). Лише 16% визнали його високим.

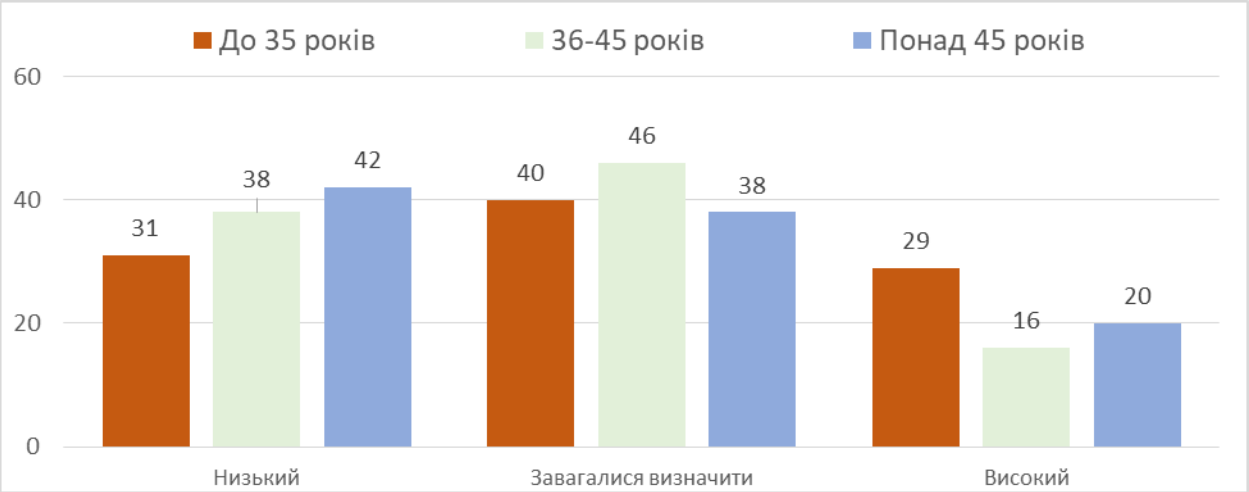

Рис. 4.22. Порівняльний розподіл відповідей представників різних вікових груп експертів на запитання «Яким є рівень Ваших знань, вмінь та навичок щодо захисту інформації Вашої організації від кіберзагроз» (у % до тих, які відповіли у кожній групі)

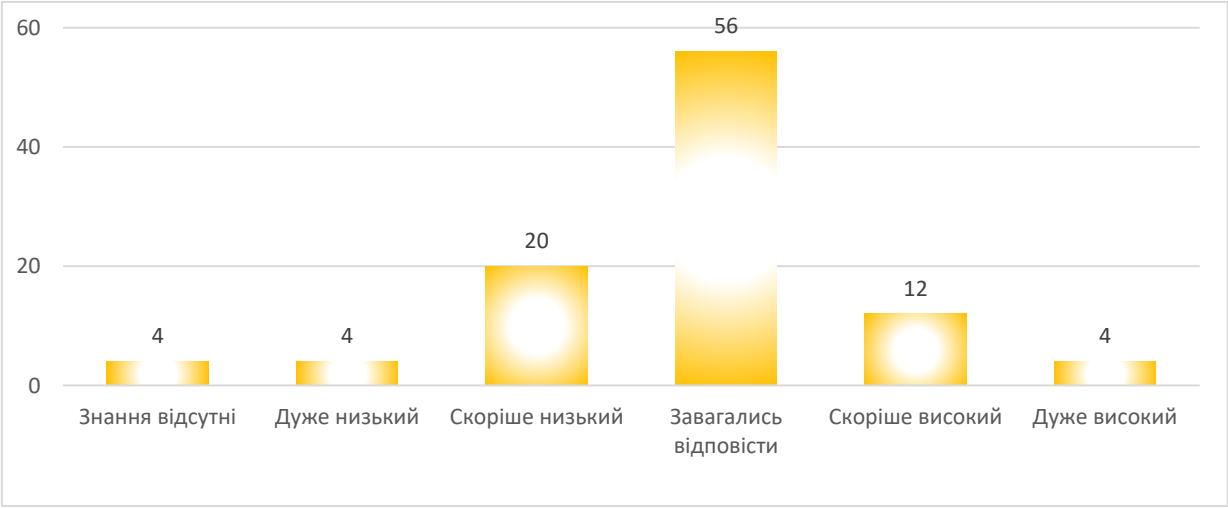

Рис. 4.23. Розподіл відповідей опитаних на запитання «Яким є рівень знань, вмінь та навичок Ваших колег щодо захисту інформації Вашої організації від кіберзагроз»

4.2. Особиста кібербезпека та захист персональних даних: шляхи підвищення рівня кіберзахисту

Більша частина опитаних негативно оцінюють рівень своїх знань щодо захисту особистої інформації від кіберзагроз (рис. 4.24).

Рис. 4.24. Розподіл відповідей опитаних на запитання «Яким є рівень Ваших знань, вмінь та навичок щодо захисту Вашої особистої інформації від кіберзагроз»

При цьому рівень знань значною мірою залежить від віку опитаних (рис. 4.25).

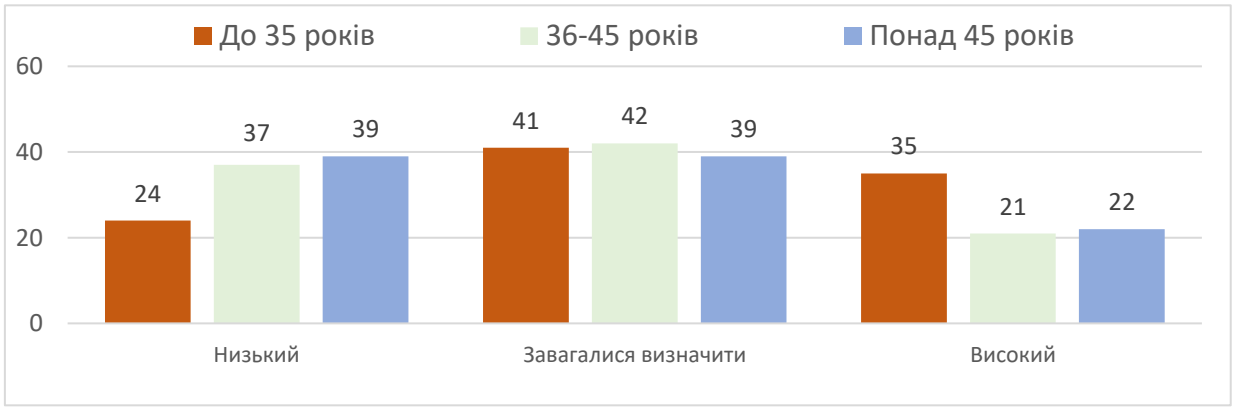

Рис. 4.25. Порівняльний розподіл відповідей представників різних вікових груп експертів на запитання «Яким є рівень Ваших знань, вмінь та навичок щодо захисту Вашої особистої інформації від кіберзагроз» (у % до тих, які відповіли у кожній групі)

Привертає також увагу, що рівень знань, вмінь і навичок працівників публічного сектору виявився нижчим, ніж в інших експертів. Так, лише 22% працівників органів виконавчої влади та місцевого самоврядування визначили його як високий. У той час, як серед інших експертів цей показник виявився удвічі більшим (рис. 4.26).

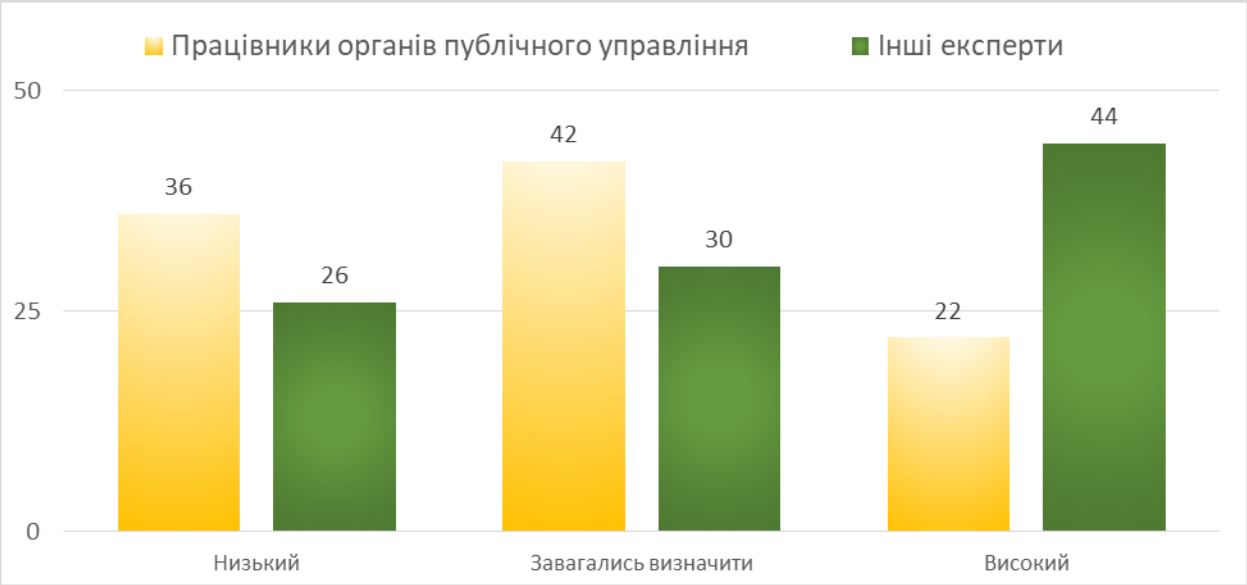

Рис. 4.26. Порівняльна оцінка рівня знань, вмінь та навичок щодо захисту особистої інформації від кіберзагроз серед працівників органів публічного управління та інших експертів (у % до тих, які відповіли у кожній групі)

60% опитаних заявили, що їм невідомо про кібератаки (під якими в дослідженні розумілися спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму

функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту стосовно їх персональної інформації (рис. 4.27).

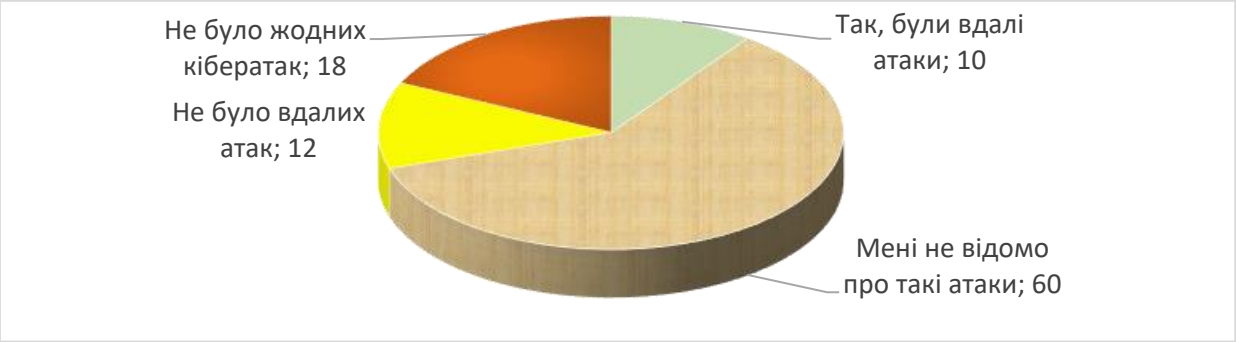

Рис. 4.27. Розподіл відповідей опитаних на запитання «Чи піддавалася Ваша персональна інформація кібератакам»

Між тим, переважна більшість опитаних відчувають неабиякі ризики і висловили бажання підвищити свій рівень знань, вмінь та навичок щодо захисту інформації від кіберзагроз (рис. 4.28). Найбільше серед усіх категорій опитаних дану потребу відчувають керівники органів публічного управління (72%). Найбільшу потребу при цьому опитані висловили у підвищенні кваліфікації щодо захисту персональних даних та електронного документообігу.

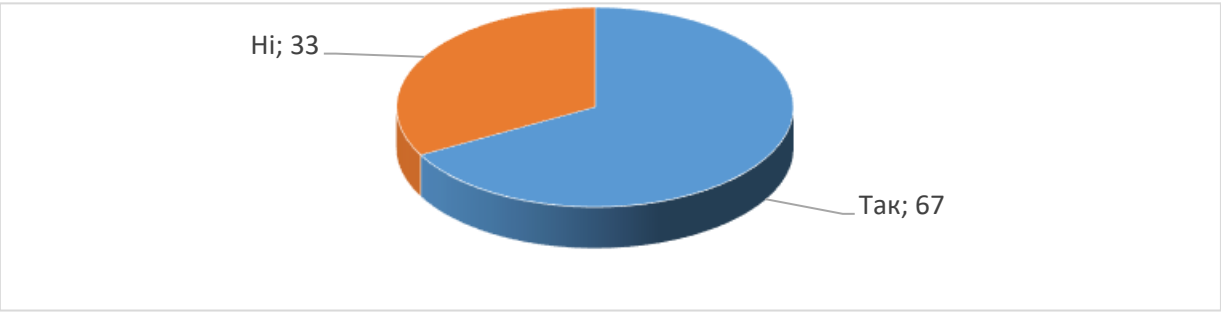

Рис. 4.28. Розподіл відповідей опитаних на запитання «Чи бажали б Ви підвищити свій рівень знань, вмінь та навичок щодо захисту інформації від кіберзагроз?»

Необхідність підвищення рівня знань у питаннях кібербезпеки доводить і самооцінка опитаними своєї обізнаності у ключових поняттях сучасної епохи «цифровізації». Жодне з них не змогли пояснити більшість опитаних (рис. 4.29).

Неабияке занепокоєння при цьому викликає низька самооцінка працівників органів публічного управління. Лише 43% з них змогли б пояснити таке поняття, як «електронне врядування», 21% – «цифрове врядування», 17% «віртуальні співтовариства», 15% – «електронна демократія». При цьому в межах цієї категорії опитаних кидаються в очі різкі розбіжності в рівні знань між керівниками та рядовими працівниками. Останні, як показано на рис. 4.30, є набагато менш підготовленими та обізнаними з питань розвитку сучасного кіберпростору.

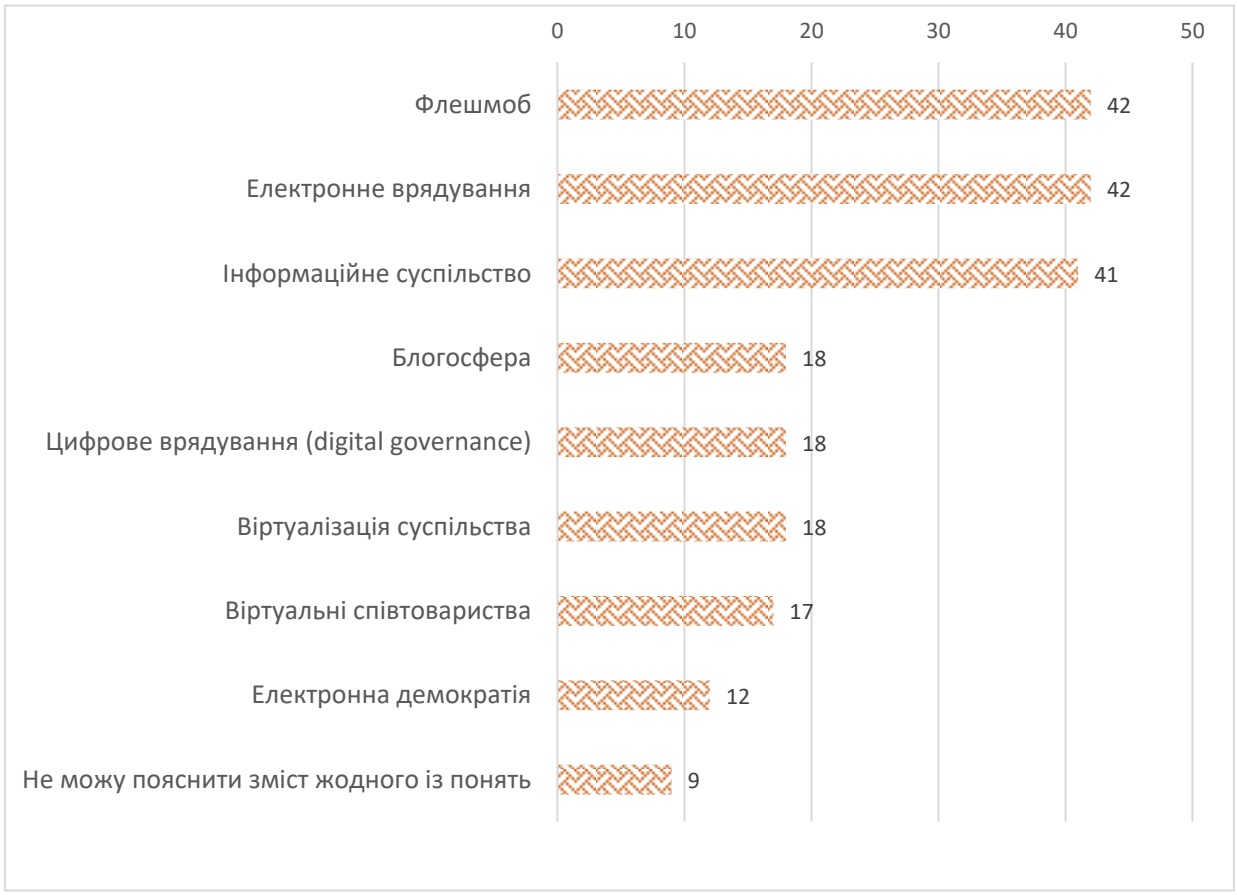

Рис. 4. 29. Розподіл відповідей опитаних на запитання «Які з наступних понять Ви могли б пояснити іншим?»

Рис. 4.30. Розподіл відповідей працівників органів публічного управління, які займають керівні посади, та рядових працівників на питання «Які з наступних понять Ви могли б пояснити іншим» (у %, які відповіли у кожній групі).

Не дивлячись на низький рівень знань з питань кібербезпеки, більшість опитаних заявила про те, що у питаннях захисту персональної інформації довіряє лише собі (рис. 4.31). Цікаво, що інтернет-провайдерів та мобільних операторів як суб‘єктів довіри серед опитаних не виділяє майже ніхто.

При цьому чим молодше опитані – тим більше у них покладання в питаннях кібербезпеки виключно на себе (рис. 4.32).

Також звернемо увагу на відповіді працівників сфери публічного управління. Вони порівняно більше у даному питання довіряють державі і порівняно менше організаціям, в яких вони працюють (рис. 4.33).

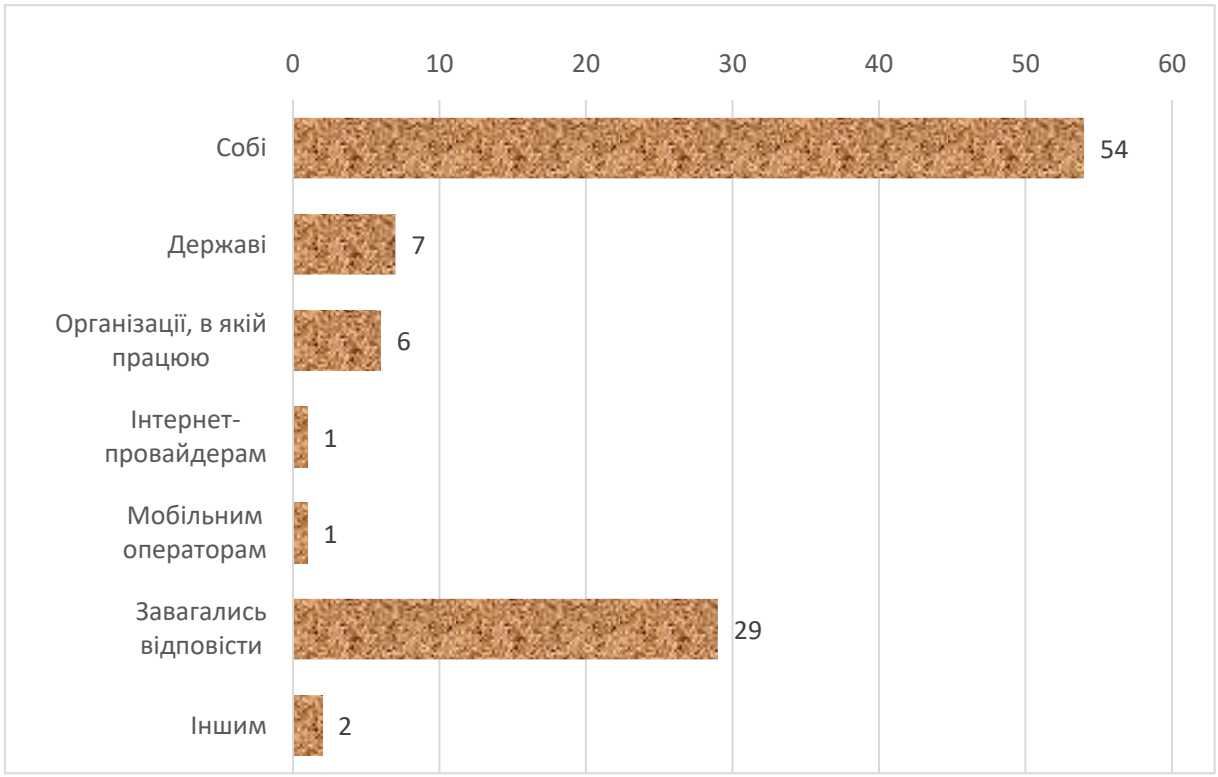

Рис. 4.31. Розподіл відповідей опитаних на запитання «Кому Ви найбільше довіряєте в питаннях захисту персональної інформації?»

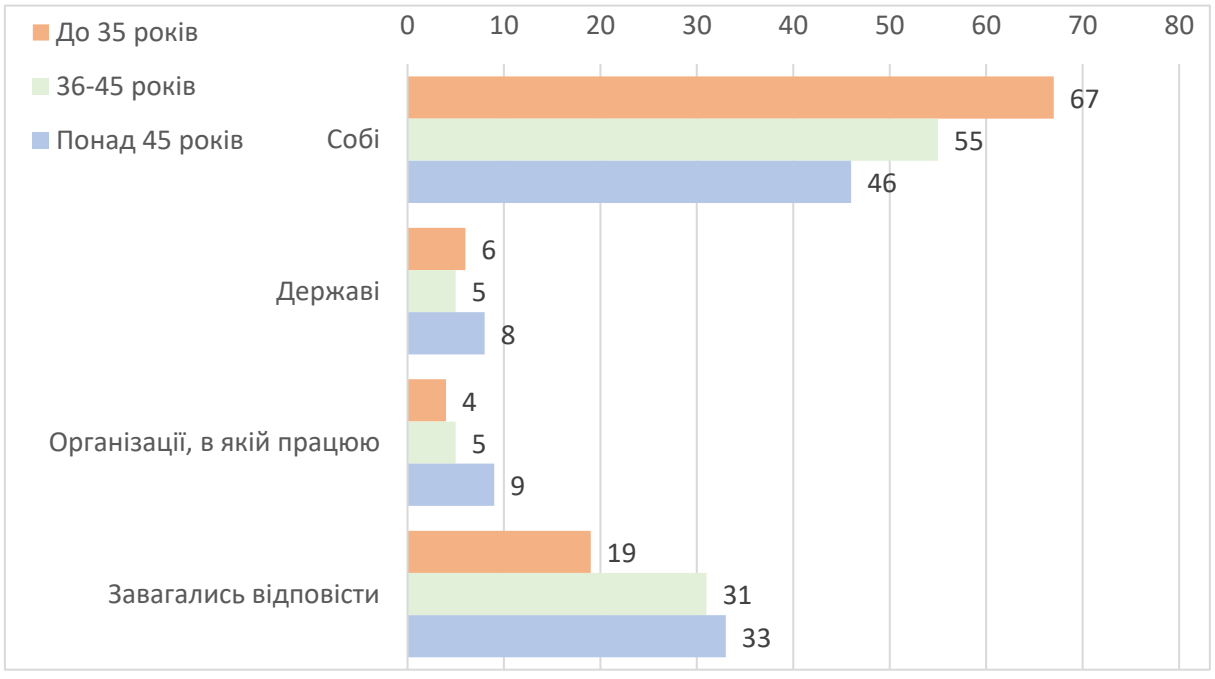

Рис. 4.32. Порівняльний розподіл відповідей різних вікових груп опитаних на запитання «Кому Ви найбільше довіряєте в питаннях захисту персональної інформації?» (% до опитаних в кожній групі)

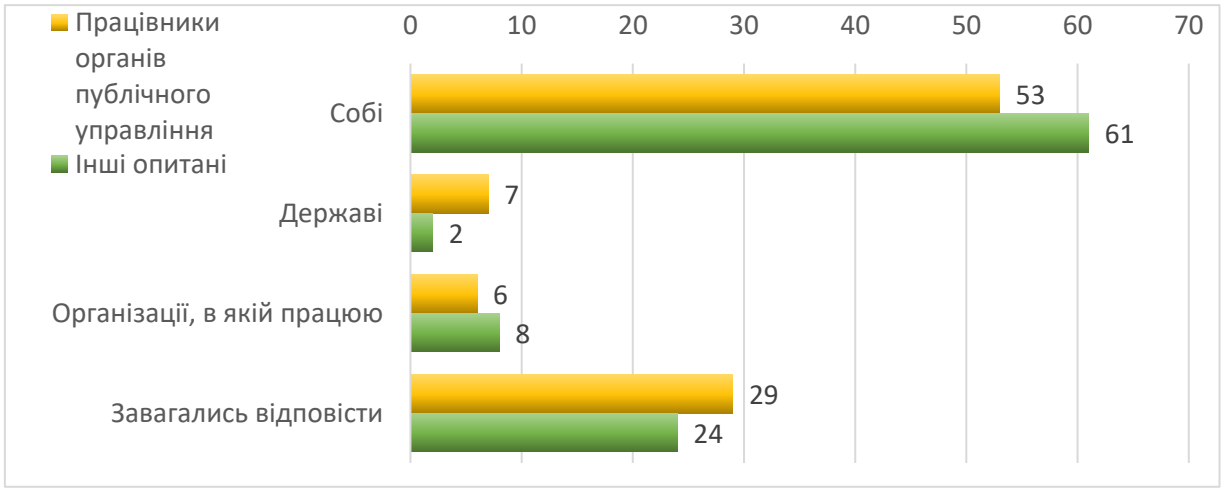

Рис. 4.33. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання «Кому Ви найбільше довіряєте в питаннях захисту персональної інформації?» (% до опитаних в кожній групі)

Відзначимо, що виходячи з наведених оцінок довіри, не дивними виглядають і показники недовіри до суб‘єктів захисту персональної інформації. На першому місці майже в усіх категоріях опитаних знаходяться мобільні оператори (рис. 4.34). Між тим, одним з лідерів «недовіри» є держава.

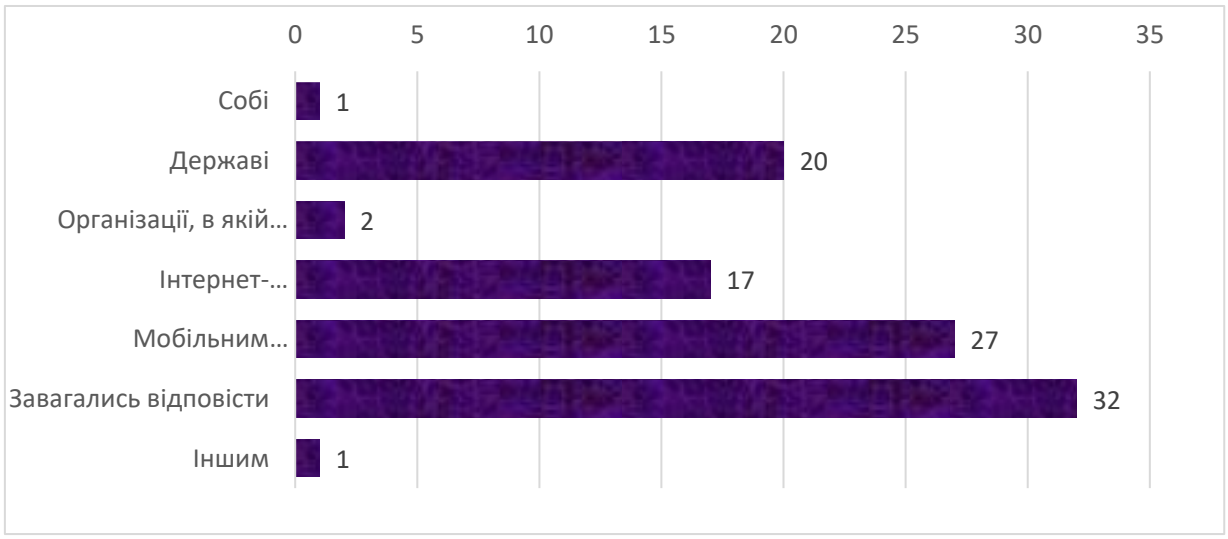

Рис. 4.34. Розподіл відповідей опитаних на запитання «Кому Ви найбільше не довіряєте в питаннях захисту персональної інформації?»

І в даному разі цікаво порівняти думки представників «публічного сектору» та інших опитаних. Лідером «недовіри» у інших виступає саме держава (рис. 4.35).

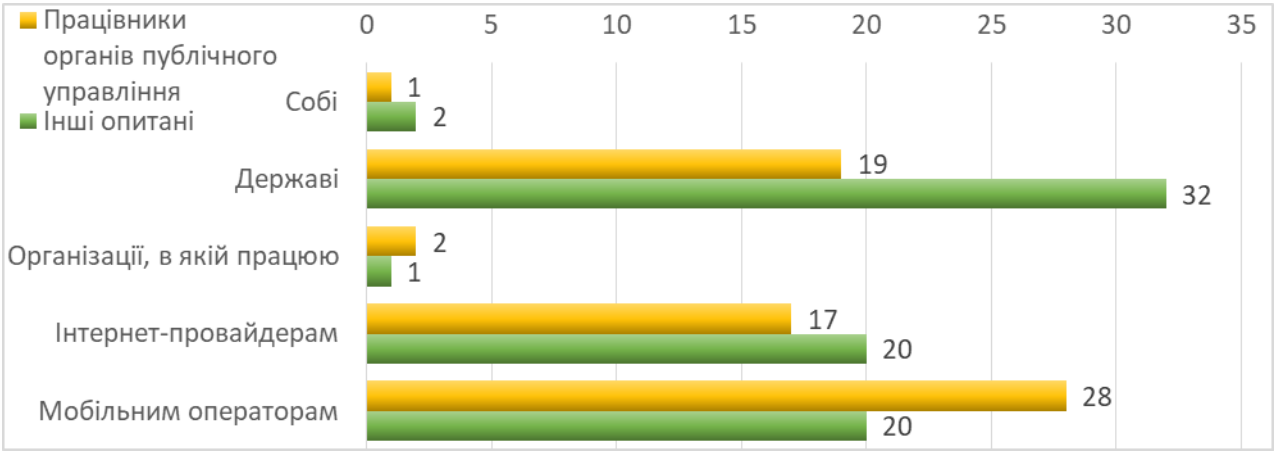

Рис. 4.35. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання «Кому Ви найбільше не довіряєте в питаннях захисту персональної інформації?» (% до опитаних в кожній групі)

Відзначимо, що більше половини опитаних, при цьому, вважає, що саме держава несе відповідальність за захист персональних даних (рис. 4.36).

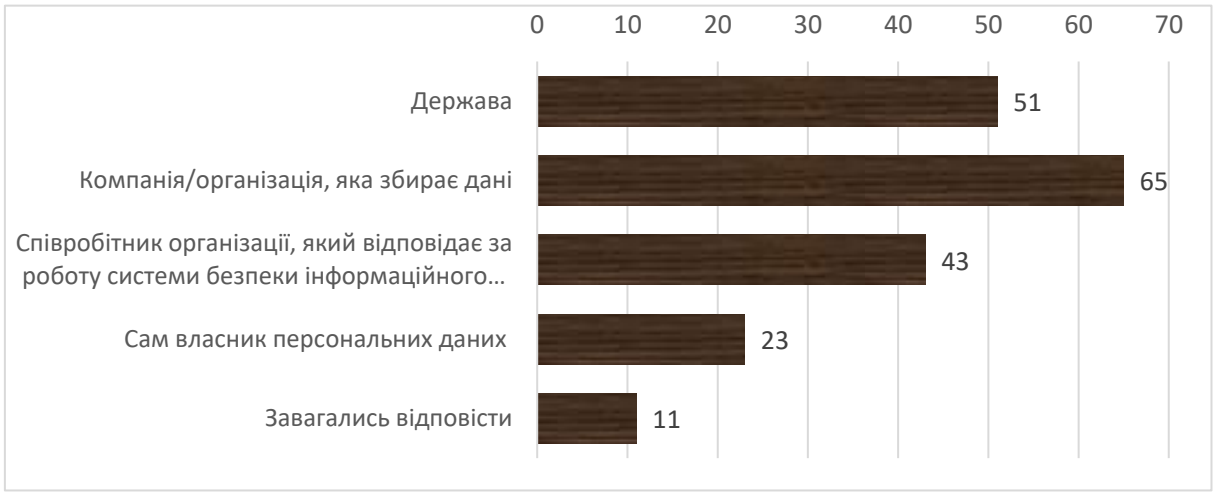

Рис. 4.36. Розподіл відповідей опитаних на запитання «Хто має нести відповідальність за захист персональних даних?»

Хоча, безперечно, головним суб‘єктом відповідальності є організація (компанія), яка збирає дані. При цьому більшою відповідальністю державу наділяють особи віком понад 45 років (56%).

Говорячи про ситуації, за результатами яких опитані будуть утримуватися від продовження співпраці з певною організацією/компанією, що має доступ до персональних даних, головним чинником стала передача конфіденційної персональної інформації третій стороні без отримання особистої згоди (на це вказали 65% опитаних). Загальний розподіл відповідей наведено на рис. 4.37. Найбільш вимогливими до організацій, що користуються персональною інформацією, є опитані з гуманітарною освітою (75% з них в жодному разі не будуть співпрацювати з компанією, що одного разу передала персональну інформацію третій стороні).

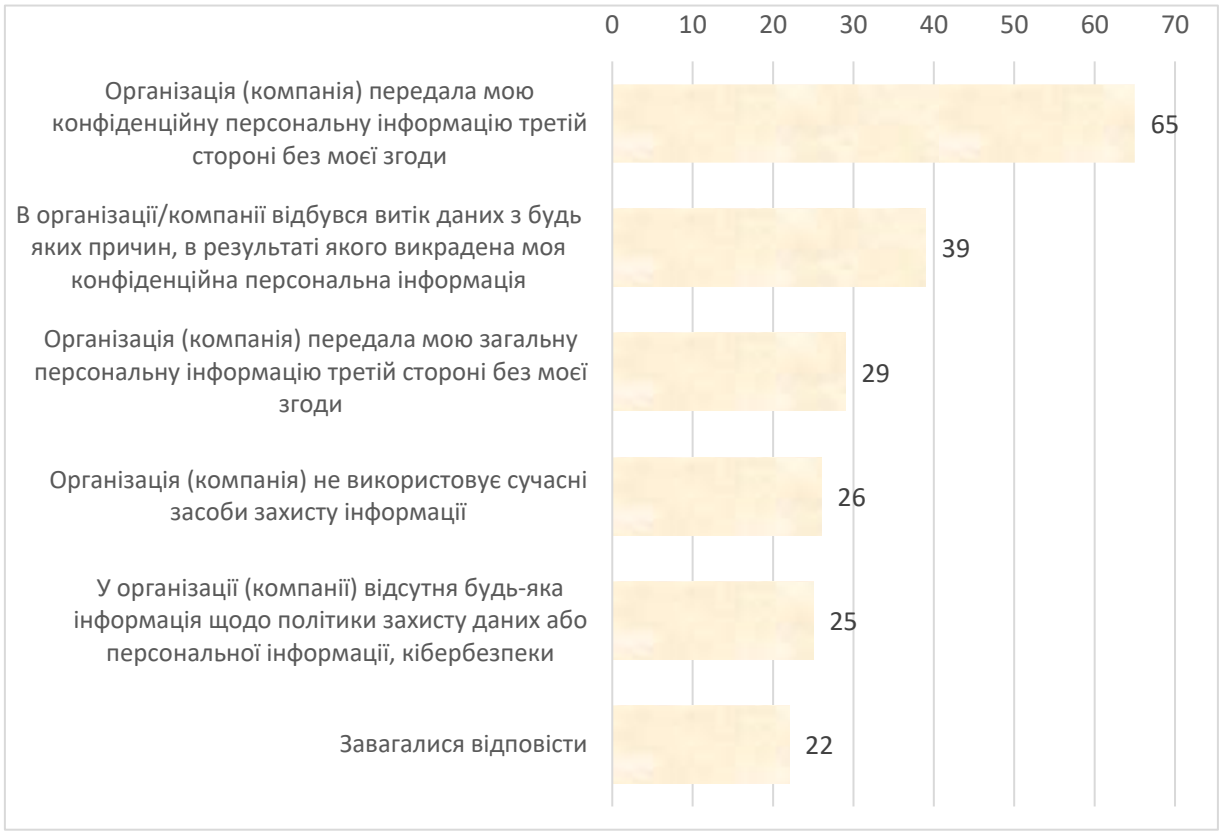

Рис. 4.37. Розподіл відповідей опитаних на запитання «В яких випадках Ви утримаєтесь від продовження дій з певною організацією/компанією?» (указано п‘ять основних причин)

Як видно з рис. 4.37 найбільше опитані стурбовані можливим витоком саме персональної інформації. Говорячи про інформацію, яку опитані не готові розголошувати в кіберпросторі, вони звертають увагу на: паролі входу до різних систем, сайтів, соціальних мереж (85%), паспортні дані, індивідуальний податковий номер (85%), аналогічні дані друзів і родичів (79%), номер кредитної картки (83%), адресу проживання (73%). Загальний розподіл відповідей респондентів наведено на рис. 4.38.

Рис. 4.38. Розподіл відповідей опитаних на запитання «Яку інформацію Ви особисто не готові розголошувати в кіберпросторі?»

Як видно з рис. 4.39, працівники органів публічного управління більш стурбовані імовірним витоком своїх паспортних даних, адреси проживання, номера кредитної картки, а інші опитані – даних про розмір своїх доходів. Оцінюючи технології, які представляють найбільшу загрозу для захисту конфіденційних персональних даних, опитані звернули увагу, насамперед, на мобільні пристрої і цифрові платіжні системи (рис. 4.40).

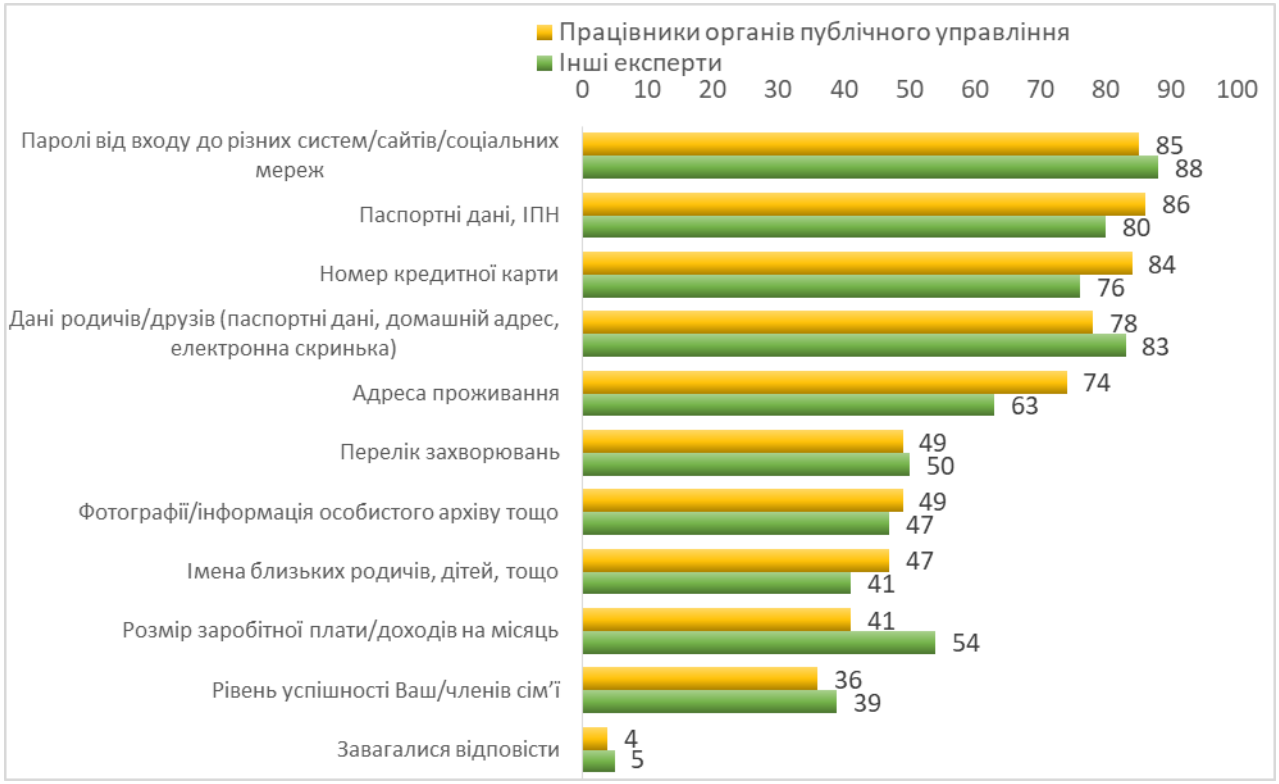

Рис. 4.39. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання «Яку інформацію Ви не готові розголошувати в кіберпросторі?» (у % до опитаних в кожній групі)

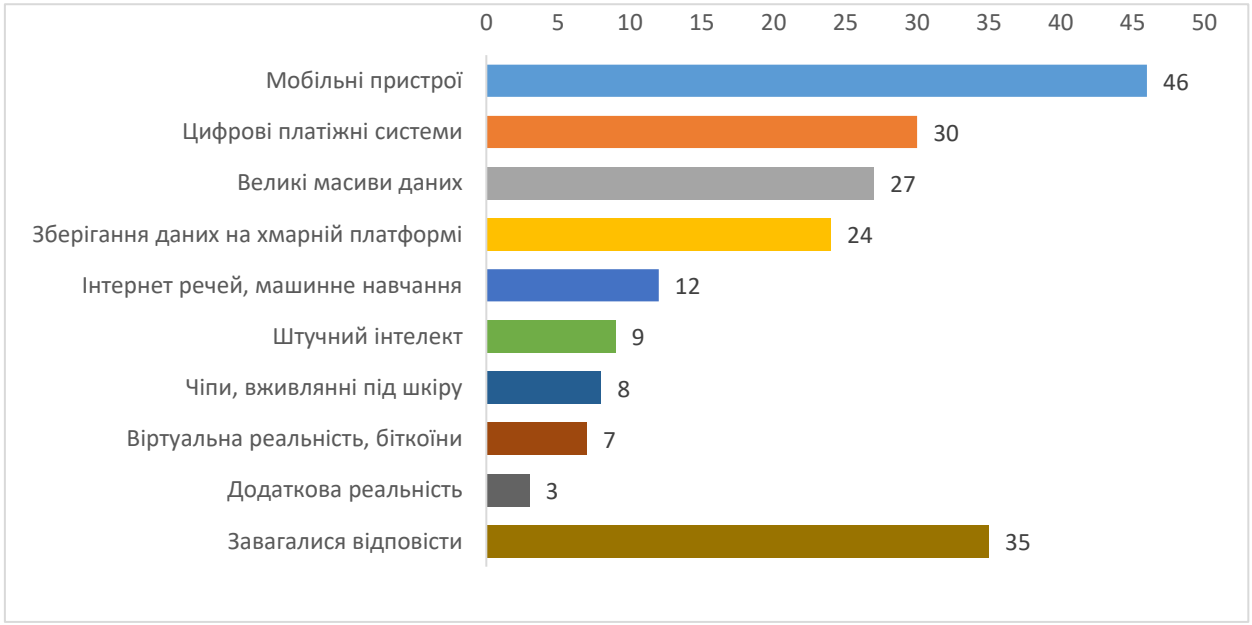

Рис. 4.40. Розподіл відповідей опитаних на запитання «Які технології представляють найбільшу загрозу для захисту конфіденційних персональних даних?»

Відзначимо, що найбільше мобільних пристроїв побоюються опитані, які не працюють в «публічному секторі» (56%). Також вони порівняно більше не довіряють зберіганню даних на «хмарних платформах» (32%).

У цілому, опитані не є занадто категоричними у питанні взаємодії з організаціями, які допустили виток персональних даних. Лише 22% заявили про те, що в жодному разі не можна повернути довіру до організації/компанії після здійснення на неї кібератаки або витоку персональних даних.

Основним чинником, які можуть повернути довіру до організації після витоку персональних даних, на думку опитаних, може стати посилення політики захисту інформації, чітке та зрозуміле інформування про це клієнтів (рис. 4.41).

Рис. 4.41. Розподіл відповідей опитаних на запитання «Як можна повернути довіру до організації/компанії після здійснення на неї кібератаки або витоку персональних даних?» (указано п‘ять основних чинників, у % до тих опитаних, які відповіли)

На фоні високого рівня стурбованості витоком персональних даних, опитані в цілому не висловили різко негативного ставлення до хакерів. Менше третини опитаних визначили як злочинців (рис. 4.42).

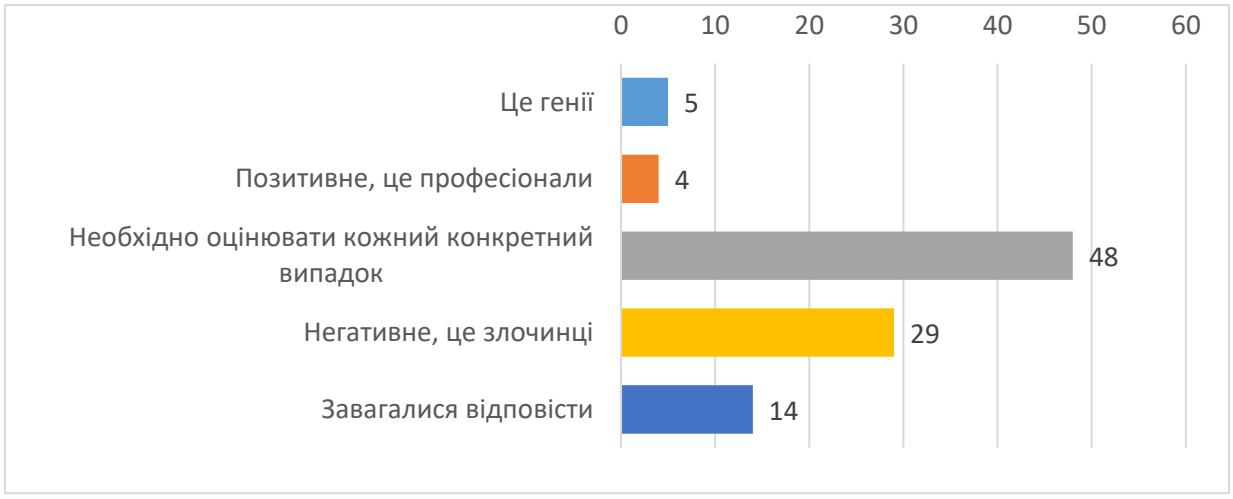

Рис. 4.42. Оцінка ставлення опитаних до хакерів

Цікаво, що найбільш негативне ставлення до хакерів у осіб віком понад 45 років, найбільш нейтральне – у осіб віком до 35 років (рис. 4.43).

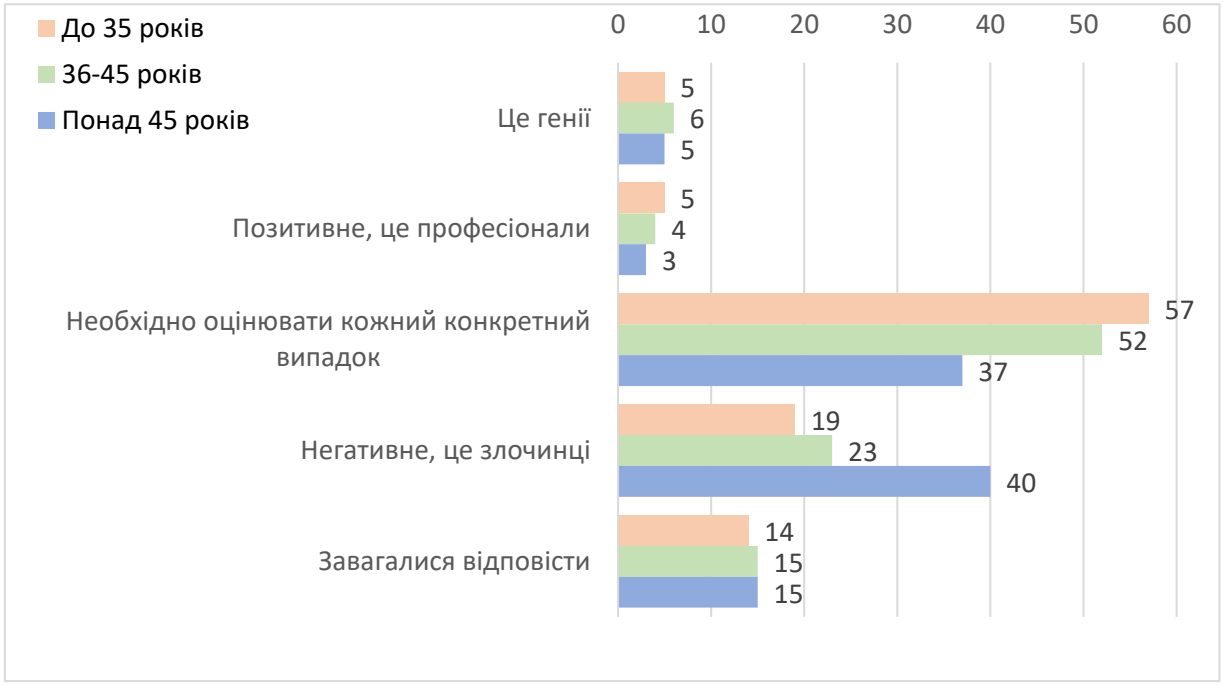

Рис. 4.43. Оцінка ставлення різних вікових груп опитаних до хакерів

При цьому опитані не змогли визначитися зі своїм ставленням до «благородного хакерства», або до такого, що обумовлений соціально значущими потребами або інтересами (рис. 4.44). 27% підтримали таку можливість, 36% – виступили категорично проти.

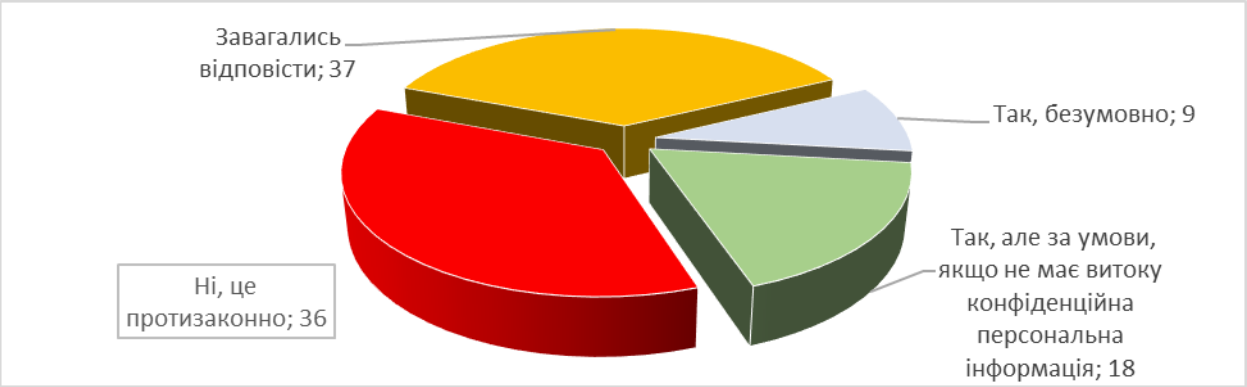

Рис. 4.44. Розподіл відповідей на запитання «Чи можливим є здійснення кібератаки для отримання інформації, яку має право знати громадськість»

Цікаво, що більш схвально до таких «кібератак» ставляться опитані, які не працюють в публічному секторі (рис. 4.45).

Рис. 4.45. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання «Чи можливим є здійснення кібератаки для отримання інформації, яку має право знати громадськість» (у % до тих, які відповіли в кожній групі)

4.3. Рівень захисту кіберпростору в публічній сфері: національний та організаційний вимір

Переважна більшість опитаних не вважає кіберпростір в Україні захищеним. При цьому рівень захисту кіберпростору своїх організацій порівняно з загальнодержавним опитані вважають набагато вищим (рис. 4.46).

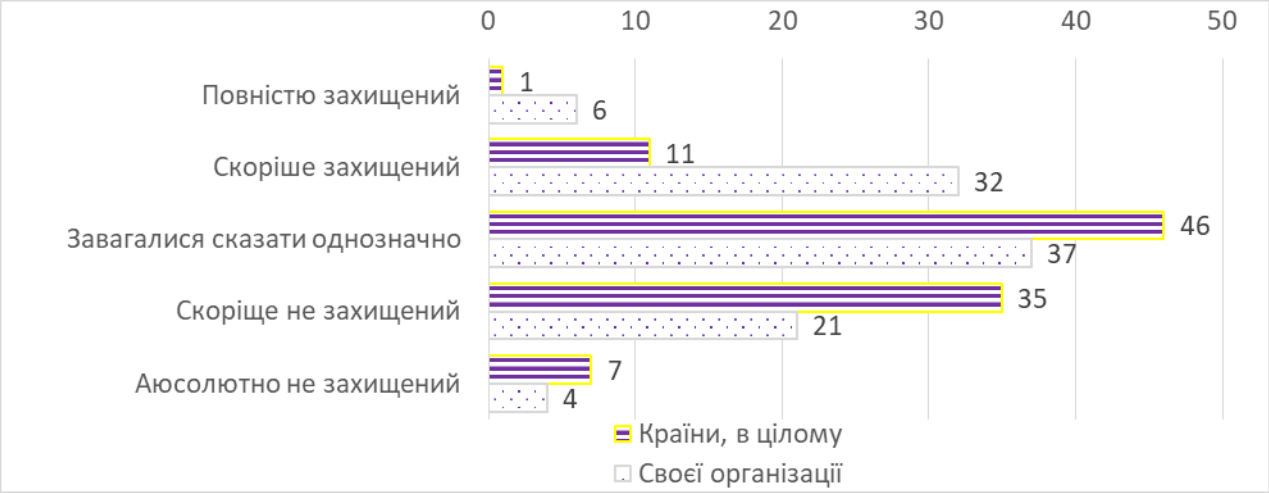

Рис. 4.46. Оцінка захисту кіберпростору країни та організацій, в яких працюють опитані

Дуже цікавим виглядає порівняння рівня захисту «публічних» і «непублічних» організацій. В останніх, згідно з результатами проведеного дослідження», система захисту від кібератак налагоджена набагато краще (рис. 4.47). Так, лише 35% працівників органів публічного управління назвали кіберпростір своїх організацій захищеним у порівнянні з 56% працівниками інших організацій. Також звертає увагу, що трохи більш «захищеними» свої організації вважають мешканці обласних центрів порівняно з мешканцями інших адміністративно-територіальних одиниць (40% проти 35%).

Відповідно, і рівень загроз для країни в цілому, експерти вважать вище, ніж для організацій, в яких вони працюють (рис. 4.48). І в даному разі, не

дивно, що «публічний сектор» виявився, за оцінками опитаних, більш незахищеним (рис. 4.49). Лише 15% опитаних працівників органів публічного управління оцінили рівень кіберзагроз своїм організаціям як низький.

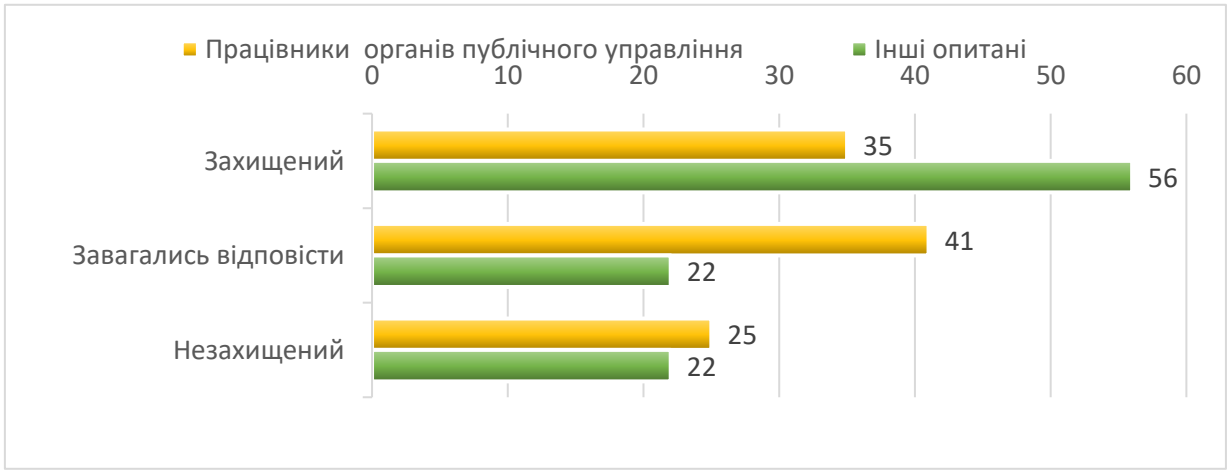

Рис. 4.47. Розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо рівня захисту від кіберзагроз організацій, в яких вони працюють (у % до опитаних к кожній групі)

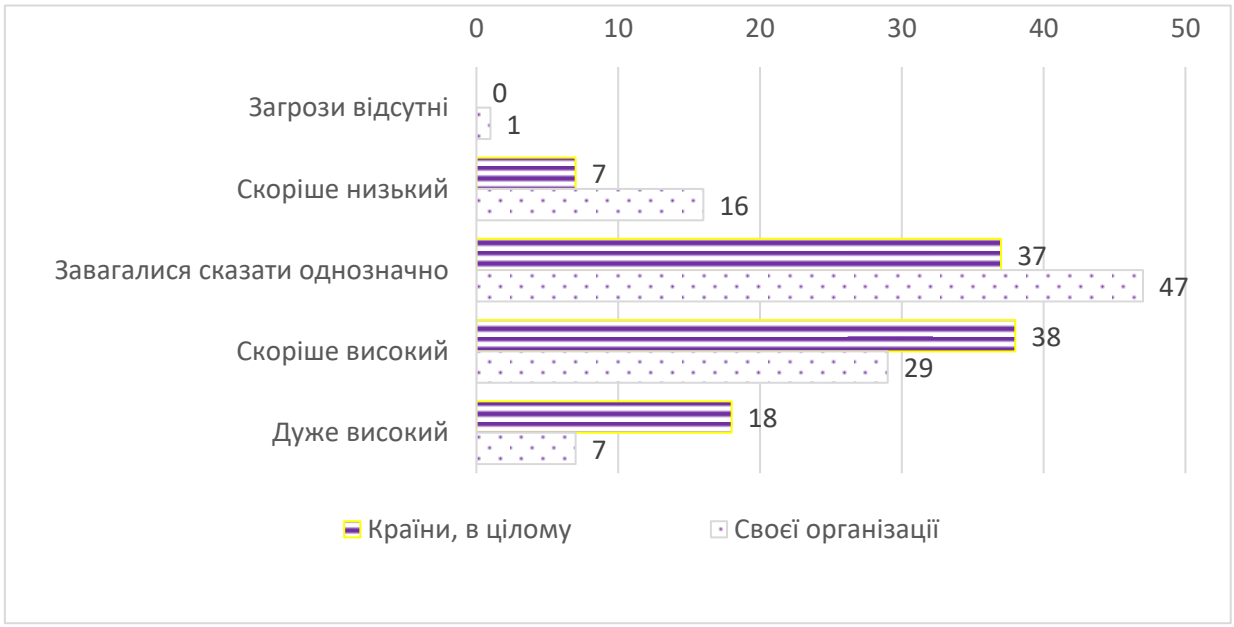

Рис. 4.48. Оцінка рівня кіберзагроз країни, в цілому, та організацій, в яких працюють опитані

Рис. 4.49. Розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо рівня загроз кіберпростору організацій, в яких вони працюють (у % до опитаних к кожній групі)

Виходячи з наведеного, не дивно, що за результатами опитування більшість респондентів визнали рівень кібербезпеки в України низьким (рис. 4.50). До речі, найгірше його оцінили опитані, які займають керівні посади в своїх організаціях (58% з них заявили про низький рівень кібербезпеки країни).

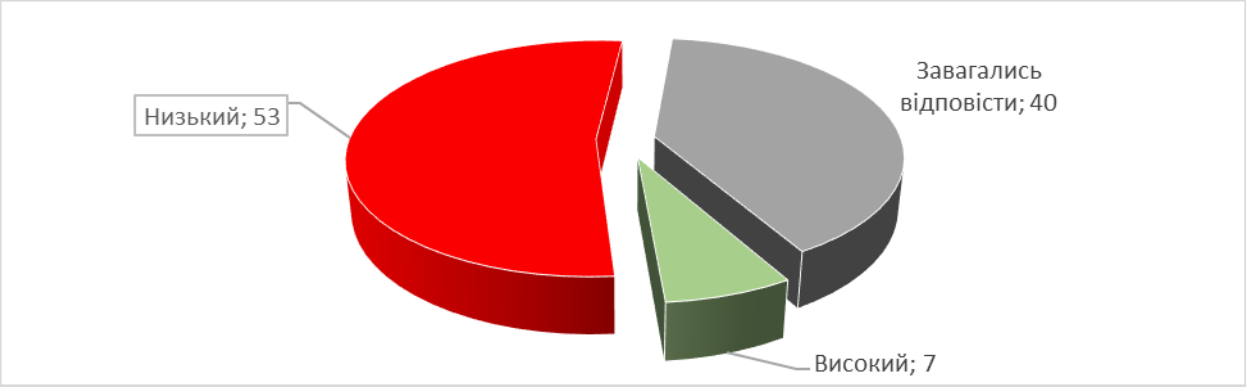

Рис. 4.50.Оцінка рівня кібербезпеки в Україні

Серед головних кіберзагроз, які сьогодні є основними/найбільш актуальними для України експерти виділили такі, як: крадіжку інформації

(67%); фінансове шахрайство (63%); хакерські атаки (59%); вірусні програми (52%). Найбільше на крадіжці інформації (73% у цій групі) та фінансовому шахрайстві (72%) акцентують особи, які не працюють в «публічному секторі».

На думку опитаних, найбільш успішними з точки зору протистояння кібератакам в Україні є IT-компанії (64%) і банківський сектор (47%). Лише шоста частина опитаних (17%) віднесли до успішних державний сектор. Майже ніхто (3%) не бачить позитивного досвіду протистояння кібератакам у органів місцевого самоврядування (рис. 4.51).

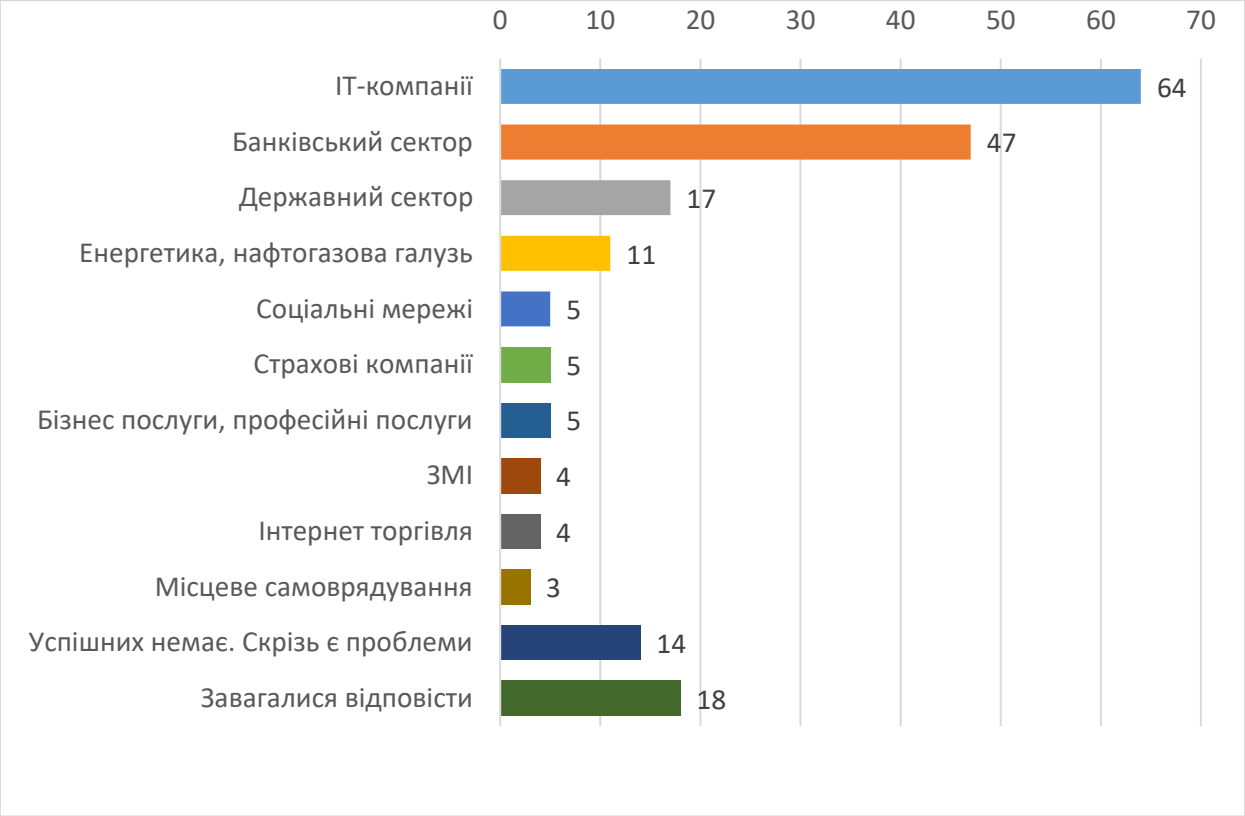

Рис. 4.51. Розподіл відповідей опитаних на запитання «Які галузі найбільш успішні з точки зору протистояння кібератакам та витоку даних в Україні?» (указані варіанти відповідей, які відзначили 3 і більше % опитаних)

При цьому державний сектор, за оцінками респондентів, є найменш захищеним від кібератак та ризиків витоку баз даних (рис. 4.52). Поряд з ним

за рівнем кіберзагроз знаходяться лише соціальні мережі. Цікаво, що про незахищеність державного сектору більше говорять ті опитані, які не працюють в публічній сфері (52%).

Рис. 4.52. Розподіл відповідей опитаних на запитання «Які галузі найбільш незахищені з точки зору протистояння кібератакам та витоку даних в Україні?» (указані варіанти відповідей, які відзначили 4 і більше % опитаних)

Таким чином, можна констатувати, що публічний сектор в цілому є найменш підготовленим до кібератак і немає успішного досвіду протистояння ним. Утім така ситуація має свої причини. Як показало дослідження, фінансування організацій, в яких працюють опитані знаходиться на вкрай низькому рівні (рис. 4.53).

Як свідчать результати опитування, лише 8% респондентів вважають, що їх організація виділяє абсолютно достатню кількість ресурсів для того,

щоб інформація організації була повністю захищена.

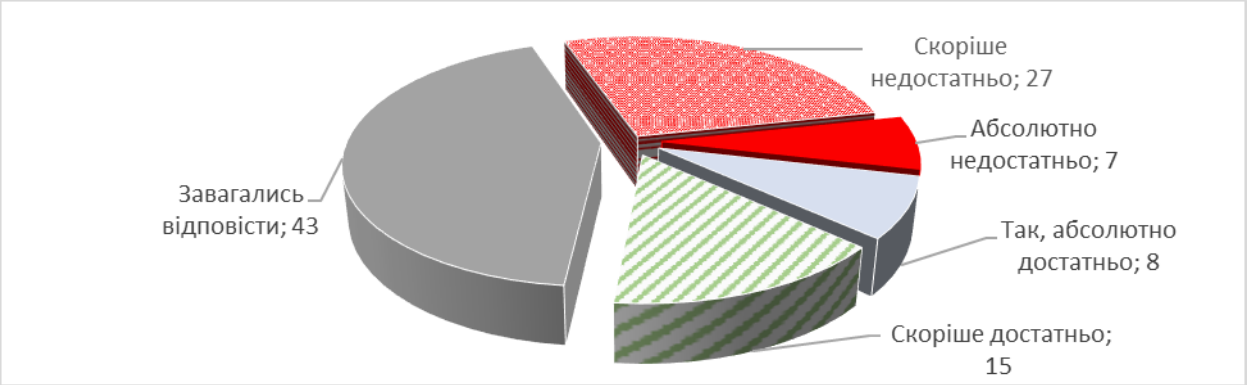

Рис. 4.53. Розподіл відповідей опитаних на запитання «Чи достатньо фінансових ресурсів виділяє Ваша організація для забезпечення кібербезпеки?»

При цьому у 4 рази більше опитаних (34%) зазначають, що таких ресурсів виділяється недостатньо. Показовим є порівняння відповідей опитаних, які працюють в публічному секторі та інших (рис. 4.54).

Рис. 4.54. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо достатності фінансових ресурсів, які виділяє їх організація для забезпечення своєї кібербезпеки (у % до опитаних к кожній групі)

Як видно з рис. 4.54, рівень фінансування кібербезпеки у «публічному

секторі» є удвічі гіршим, у порівнянні з іншими сферами.

Серед причин такої ситуації опитані працівники органів публічного управління називають, насамперед, залежність їх бюджету від «головної організації» (рис. 4.55).

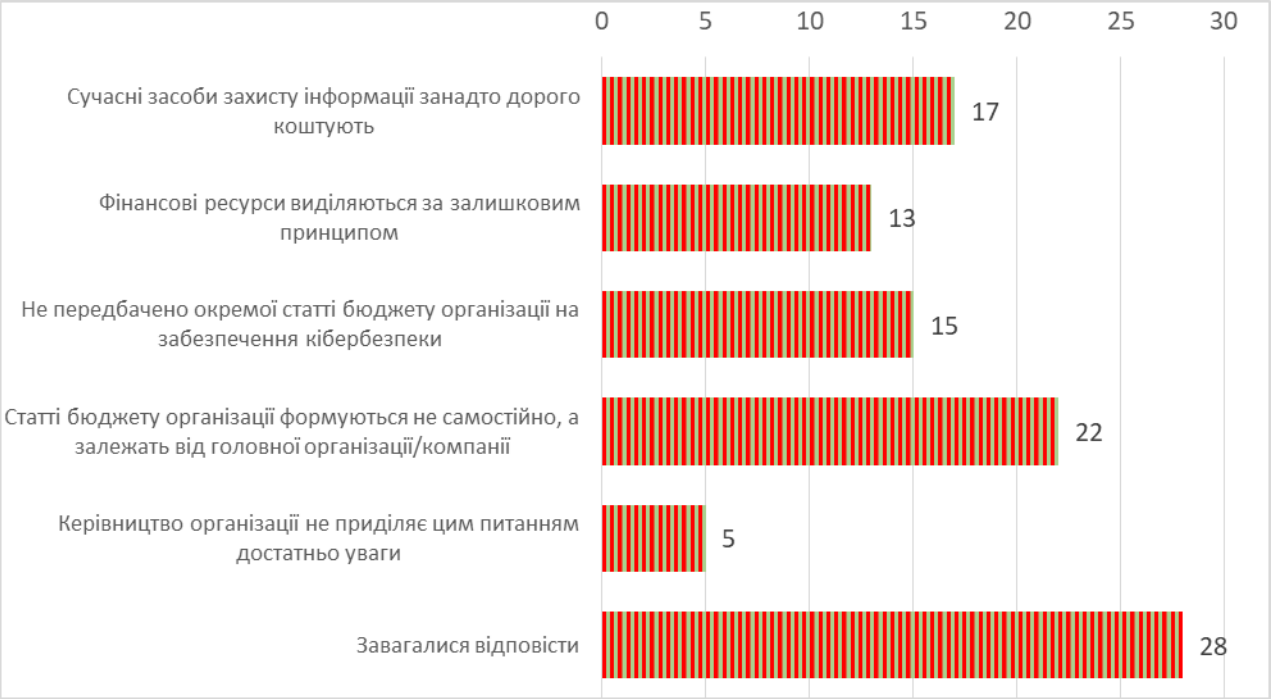

Рис. 4.55. Розподіл відповідей працівників органів публічного управління на запитання «Чому у Вашій організації виділяється недостатньо фінансових ресурсів для забезпечення кібербезпеки?» (у % до тих, які відповіли у даній групі)

Позитивним моментом є той факт, що лише 5% опитаних працівників «публічного сектору» вважає, що керівництво не приділяє цим питанням достатньої уваги. Загалом, узагальнюючи результати відповідей респондентів, можна зазначити перевагу об‘єктивних чинників недофінансування над суб‘єктивними. Між тим, негативним моментом є те, що бюджети органів публічного управління щодо забезпечення кібербезпеки за останні роки не збільшилися (рис. 4.56.). Як видно з рисунку 4.56, така ситуація є порівняно гіршою з непублічною сферою, де майже чверть

опитаних вказали на зростання витрат за цією статтею.

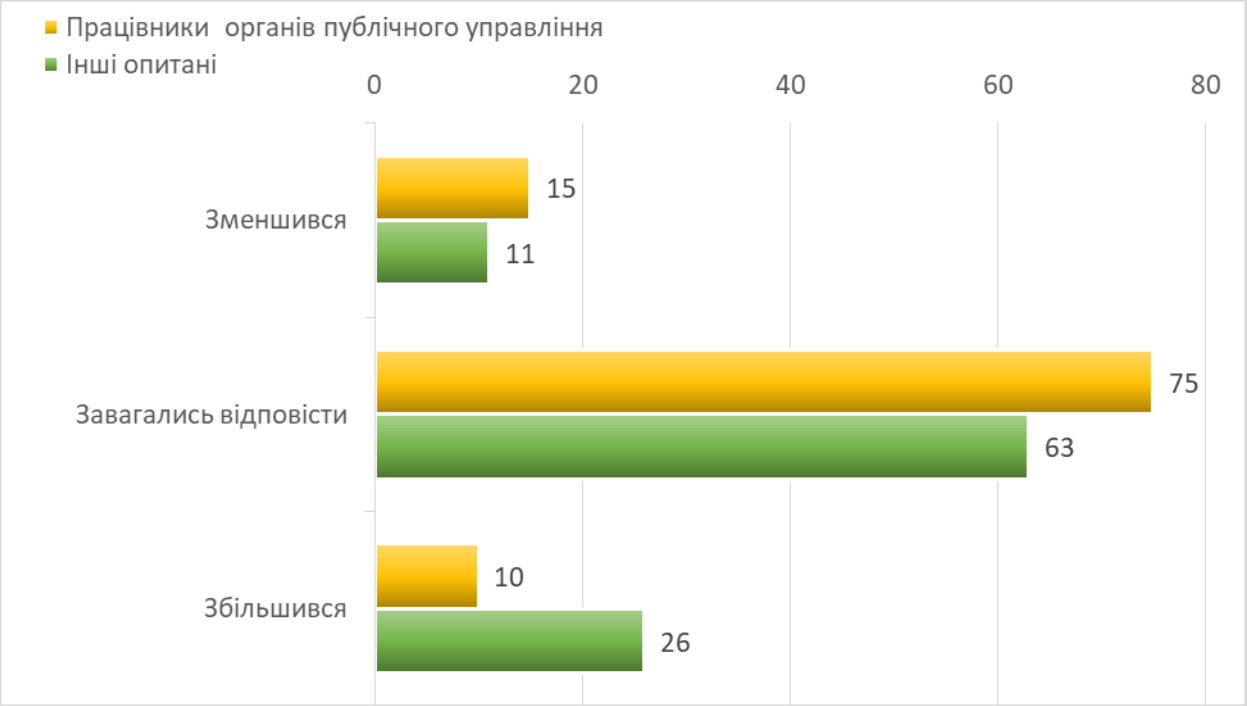

Рис. 4.56. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо того чи збільшився бюджет їх організації для забезпечення кібербезпеки за останні роки (у % до опитаних к кожній групі)

Ще одним недоліком у роботі органів публічного управління у сфері кібербезпеки є фактична відсутність профілактичної діяльності щодо кіберзахисту своїх підприємств. Як видно з рис. 4.57, лише 12% працівників органів публічного управління вказали, що в їх організаціях проводяться регулярні тести щодо проникнення до баз даних інформаційних ресурсів. У недержавних установах цей показник більше ніж удвічі вище (27%). При цьому більше половини опитаних в «публічному секторі» (61%)взагалі не володіють інформацією з цього питання.

Також звернемо увагу на різницю у відповідях опитаних, які працюють у різних за кількістю працівників організаціях. У «маленьких» (з кількістю до 40 співробітників) на проведення тестування вказали 22% опитаних. У

«великих» (з кількістю більше 40 співробітників) на реалізацію таких заходів вказали лише 14% опитаних.

Рис. 4.57. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо того чи проводить їх організація регулярні тести щодо проникнення до баз даних її інформаційних ресурсів (у % до опитаних к кожній групі)

При цьому, недостатньо поінформованими респонденти про кіберінциденти на місці своєї роботи. Більшості опитаних (70%) на момент проведення дослідження було не відомо про кібератаки на організації, в яких вони працюють (рис. 4.58).

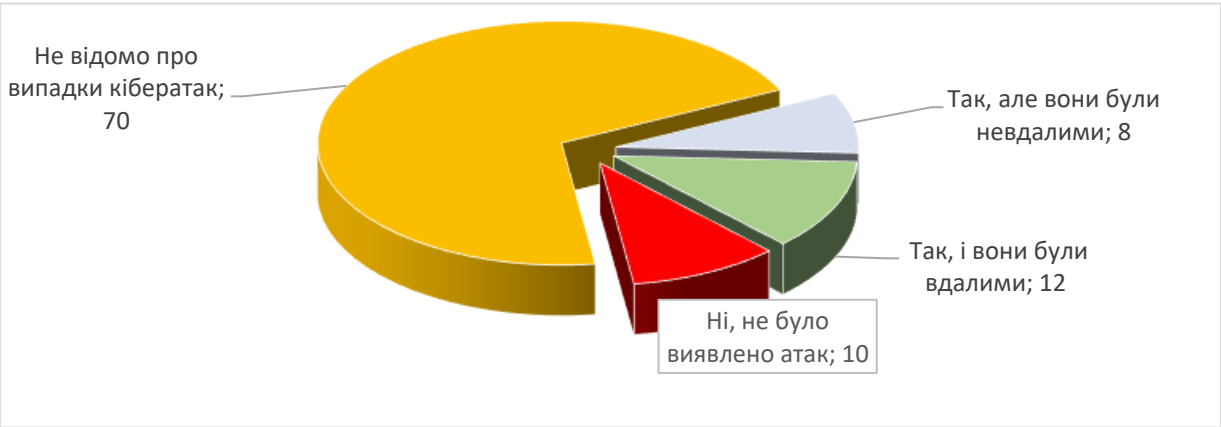

Рис. 4.58. Розподіл відповідей на запитання «Чи можливим є здійснення кібератаки для отримання інформації, яку має право знати громадськість»

Однак, з рис. 4.58, привертає увагу той факт, що 20% організацій все ж таки піддавалися таким атакам. Судячи з результатів опитування, більше загроз відчуває на собі «непублічний сектор» (рис. 4.59).

Рис. 4.59. Розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо того, чи були кібератаки на організацію, в якій вони працюють (у % до опитаних к кожній групі)

За результатами опитування, можна визначити, що найбільшу цінність для здійснення кібератак в публічному секторі представляють персональні дані працівників, а також дані, пов‘язані з державною таємницею, то в непублічному – дані фінансового характеру, а також матеріали, пов‘язані з комерційною таємницею (рис. 4.60).

При цьому відносна більшість опитаних, що працюють і в публічній і в непублічній сферах, погодилися з тим, що основні ризики, пов‘язані з витоком інформації з їх організації, йдуть від особистої недбалості працівників організації (рис. 4.61). Хоча в цьому випадку на недбалості співробітників більше наголошують працівники «непублічного сектора».

Цікаво, що про особисту недбалість працівників також більше стверджують особи, які займають керівні посади (47% проти 32% у рядових працівників).

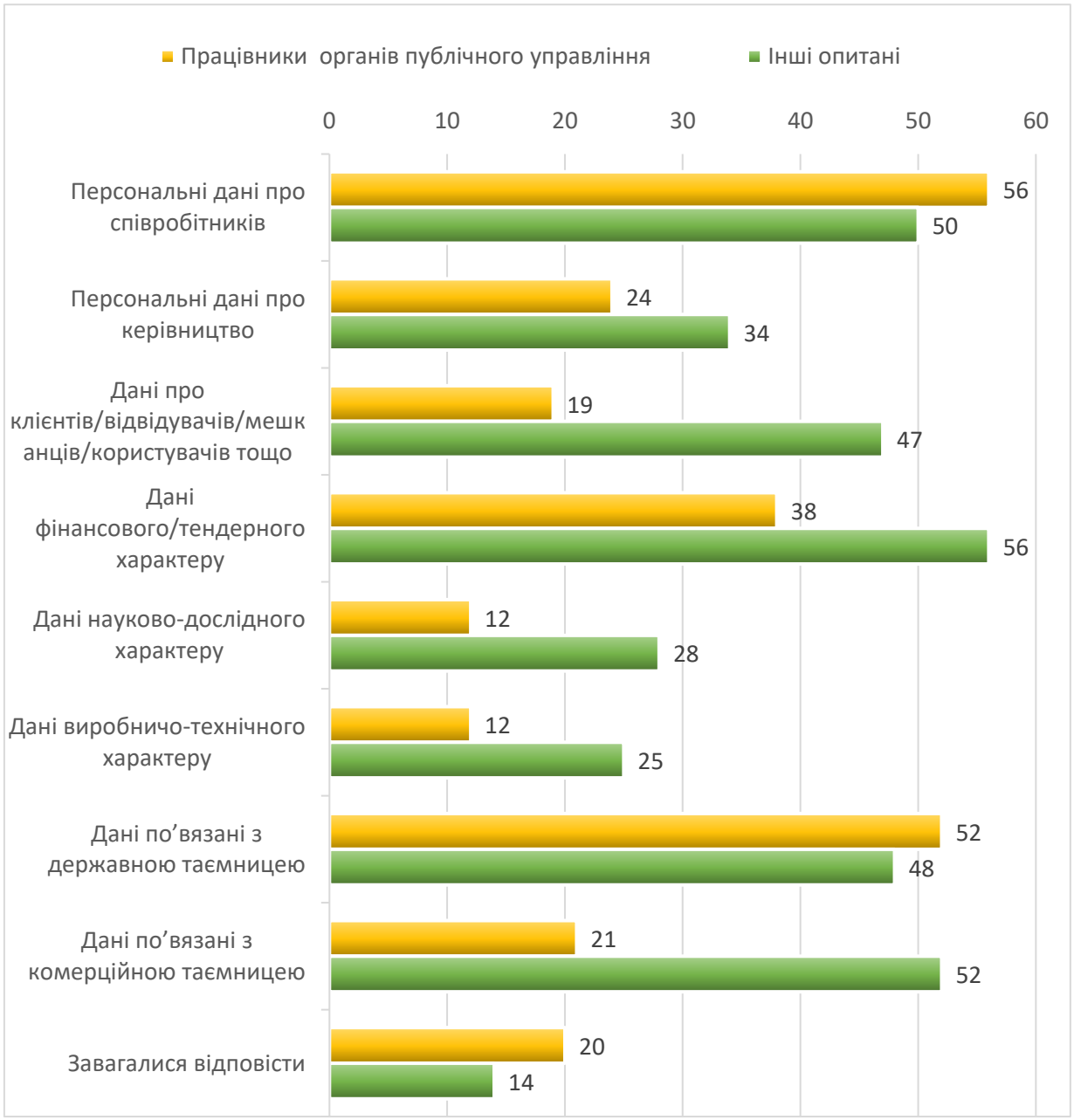

Рис. 4.60. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо видів інформації в їх організації, які мають найбільшу цінність для здійснення кібератак (у % до опитаних к кожній групі)

Цікавим є і розподіл відповідей опитаних на запитання щодо чинників, які сприяють успішності проведення кібератак в публічному секторі (рис. 4.62).

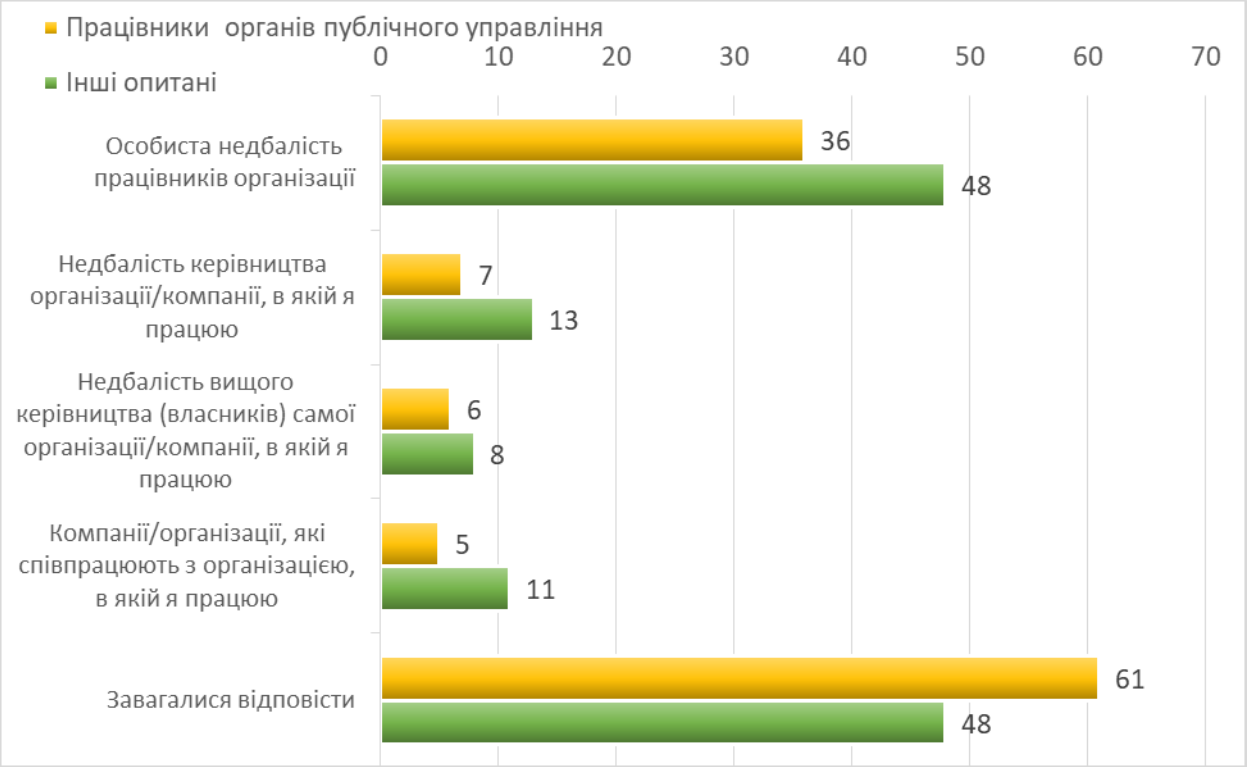

Рис. 4.61. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо основних можливих шляхів витоку інформації в їх організаціях (у % до опитаних к кожній групі)

Більшість опитаних визначили, що це недосвідченість персоналу в питаннях кібербезпеки (54%). Також значущими факторами є недостатня кількість інструментів для виявлення кібератак (61%), недостатня захищеність інформаційних даних, мереж (58%) і відсутність кваліфікованих фахівців з інформаційної безпеки (50%). При цьому привертають увагу певні відмінності у відповідях на це питання працівників органів публічного управління та інших респондентів (рис. 4.63). Перші більше акцентують на відсутності в публічному секторі належних інструментів для виявлення та запобігання кібератак (об‘єктивні чинники), другі – на відсутності підготовлених фахівців та недосвідченості персоналу у сфері кібербезпеки (суб‘єктивні чинники).

Рис. 4.62. Розподіл відповідей опитаних на запитання «Які чинники сприяють успішності проведення кібератак в публічному секторі?» (у % до тих, які відповіли у даній групі)

Рис. 4.63. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо чинників, які сприяють успішності (у % до опитаних к кожній групі)

Різними в державних та недержавних установах є і рівень володіння інформацію про реакції на такі атаки, а також способи реагування на кіберзагрози. У недержавних організаціях намагаються самостійно вирішувати проблеми, у «публічному секторі» працівникам взагалі невідомо як їх організації протистояють кіберзагрозам (рис. 4.64). При цьому це стосується як керівників органів публічного управління (68% з них завагалися відповісти на дане питання) так і рядових працівників (80%).

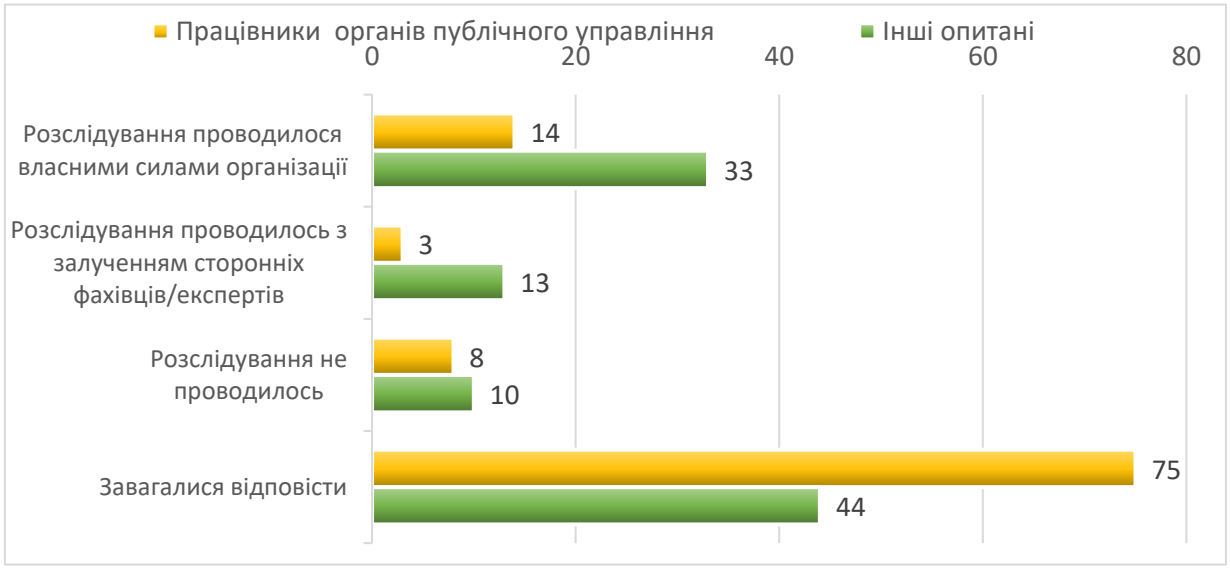

Рис. 4.64. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо того, чи було проведене розслідування кібератаки на організацію, в якій вони працюють (у % до опитаних к кожній групі)

Відмінними є розуміння в різних організаціях і політики щодо інцидентів в сфері кібербезпеки. Так, 71% працівників органів публічного управління невідомо про таку політику в своїх організаціях взагалі. На цьому фоні близько половини опитаних працівників «непублічної сфери» зазначили, що такі інциденти в їх організаціях фіксуються, класифікуються і приймаються заходи щодо реагування на них (рис. 4.65).

Рис. 4.65. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання стосовно політики їх організації щодо інцидентів в сфері кібербезпеки (у % до опитаних к кожній групі)

Виходячи з наведеного, не дивною представляється і оцінка опитаними заходів, що проводить їх організація щодо захисту своїх інформаційних ресурсів (рис. 4.66).

Рис. 4.66. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо оцінки заходів, спрямованих на захист інформаційних ресурсів, які проводить їх організація (у % до опитаних к кожній групі)

Як бачимо з рис. 4.66, лише 10% опитаних працівників органів публічного управління визнали, що таких заходів достатньо. Що практично в три рази менше, ніж у «непублічному секторі». Привертає в черговий раз увагу і рівень низький рівень обізнаності опитаних працівників органів публічного управління щодо кіберполітики своїх організацій (більше половини не змогли оцінити заходи щодо кіберзахисту на своєму місці роботи).

Говорячи про шляхи підвищення рівня кібербезпеки своїх організацій, відносна більшість опитаних (47%) погодилася з тим, що це має бути регулярне проведення контролю щодо установки оновлення свого програмного забезпечення. Також важливим опитані визнали регулярне проведення навчання працівників (38%) і створення власного підрозділу щодо захисту інформаційних ресурсів (33%).

Однак, і в цьому підходу підходи працівників «публічного сектору» і «непублічної сфери» істотно відрізняються (рис. 4.67). Працівники недержавних організацій порівняно більше акцентують на необхідності створення власного підрозділу щодо захисту інформаційних ресурсів, а також на перевірці ефективності заходів, які застосовувалися раніше для усунення виявлених недоліків.

Також думки опитаних розділилися у відповіді на запитання «Яку частину бюджету сучасна організація має витрачати для забезпечення ефективного захисту свого інформаційного простору?». Відносна більшість опитаних вважає, що на це йти до 30% наявних коштів (рис. 4.68). Між тим, серед працівників органів публічного управління є порівняно більшим усвідомлення збільшення фінансування заходів у сфері кібербезпеки (рис. 4.69)

При цьому головними напрямами, на які необхідно спрямовувати кошти, респонденти назвали: сучасне ліцензоване програмне забезпечення, техніку і устаткування, навчання всіх працівників, а також оплату праці фахівців у сфері кібербезпеки.

Рис. 4.67. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання щодо заходів, які повинна вживати їх організація для захисту своїх інформаційних ресурсів (у % до опитаних к кожній групі)

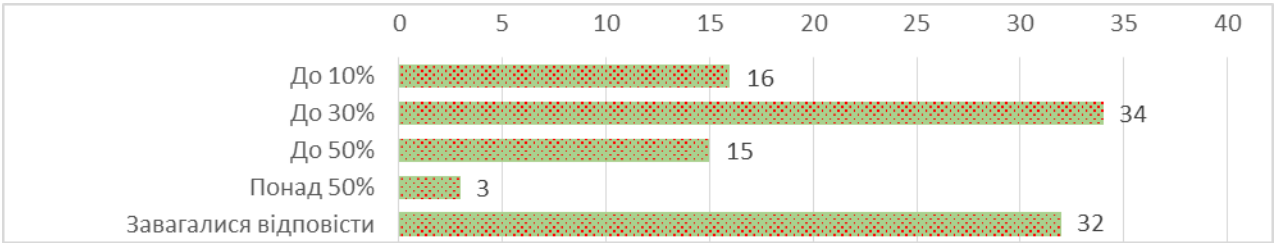

Рис. 4.68. Розподіл відповідей опитаних на запитання «Яку частину бюджету сучасна організація має витрачати для забезпечення ефективного захисту свого інформаційного простору?»

Рис. 4.69. Порівняльний розподіл відповідей працівників органів публічного управління та інших опитаних на запитання «Яку частину бюджету сучасна організація має витрачати для забезпечення ефективного захисту свого інформаційного простору?» (у % до опитаних к кожній групі)

Говорячи про пріоритетні напрями щодо інвестування (фінансування) для підвищення рівня кібербезпеки в країні в цілому, опитані звернули увагу, насамперед, на кібераналітику (69%) і хмарні технології (50%). У публічному секторі важливими було визнано інвестування в хмарні технології і машинне навчання (по 52% відповідно). На рівні окремих організацій – в кібераналітику (66%) і хмарні технології (63%).

Висновки до четвертого розділу

Дослідження особливостей запобігання та протидії кіберзагрозам у публічному секторі України дало можливість зробити такі висновки:

1. Рівень цифровізації та інформатизації, а відповідно і розвитку електронного урядування є невисоким. Двома основними причинами цього є такі:

– незадовільне матеріально-технічне забезпечення органів публічного управління, зокрема, застарілість комп‘ютерної та організаційної техніки тощо;

– відсутність швидкісного інтернету, особливо в невеличких містах, селищах і селах.

2. Головними кіберзагрозами для сучасної України є: крадіжка інформації, фінансове шахрайство і хакерські атаки. При цьому держава в цілому і органи публічного управління, зокрема, не є готовими сьогодні до адекватного реагування на ці загрози. Рівень кіберзахисту у «публічному секторі» значно поступається приватному. Державний сектор взагалі виявився найбільш незахищеним з точки зору протистояння кібератакам та витоку даних в Україні. Це зумовлено як недостатньою захищеністю інформаційних мереж, недосконалістю існуючого обладнання і програмного забезпечення, так і відсутністю кваліфікованих фахівців в сфері кіберзахисту. Виходячи з цього, держава не виступає суб‘єктом, якому громадяни довіряють в питаннях кіберзахисту та захисту персональної інформації, зокрема. У даному разі більшість опитаних покладається на себе. При цьому найбільш захищеними від кібератак та витоку даних є ІТ-компанії та банківський сектор.

3. Публічний сектор має сьогодні неабиякі проблеми з фінансуванням сфери кібербезпеки і в цьому питанні значно поступається приватному. Це зумовлено як недосконалістю державної політики у цій сфері (недостатня увага до цих проблем, низький рівень фінансування, відсутність ефективного моніторингу, тестувань, спеціальних підрозділів тощо), так і високою вартістю відповідного обладнання і програм.

4. Дослідження довело низький рівень кваліфікації працівників органів публічного управління щодо кіберпитань в цілому та використання технологій організаційного і особистого кіберзахисту зокрема. При цьому саме особиста недбалість та непідготовленість працівників визнається одним з найголовніших чинників успішних кібератак в публічному секторі.

Спільною для всіх осіб, які працюють в органах публічного управління, є також потреба в опануванні технологій електронного документообігу та он-лайн комунікацій, що пов‘язано із специфікою їх роботи.

5. Шляхами підвищення рівня кібербезпеки в публічному секторі є збільшення бюджетного фінансування відповідної сфери, стратегічне інвестування в кібераналітику і хмарні технології, створення в організаціях спеціальних підрозділів з кіберзахисту, установка сучасного програмного забезпечення та його постійне оновлення, регулярне підвищення кваліфікації всіх працівників з питань захисту організаційної та персональної інформації.

РОЗДІЛ 5
УДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПУБЛІЧНОМУ СЕКТОРІ В СУЧАСНИХ УМОВАХ

5.1. Впровадження моделі інституційної кібербезпеки

Дослідження, проведене у попередніх розділах, дає можливість сформулювати певні узагальнюючі положення, що стосуються проблематики забезпечення кібербезпеки у сучасних умовах. Викладемо їх нижче.

Інформаційні технології набули широкого поширення у нашому житті, включаючи мобільні телефони та комп'ютери, та складніші системи, такі як інфраструктура інформаційних технологій (IT), електромережі, системи управління повітряним рухом, промислове виробництво та банківський сектор. Здається, вони і надалі матимуть тенденцію до зростання. Безпека цих компонентів інформаційних технологій буде важливішою завдяки збільшенню кібератак з кожним днем. Чим більше критичні інфраструктури залежать від інформаційної системи, тим більше кіберризиків ми маємо очікувати.

Попередні кібератаки показали, що існуючі вразливості в мережах та інформаційних системах несуть серйозний ризик пошкодження критичних інфраструктур. В останні роки, на додаток до традиційних кібератак, у багатьох інцидентах, які мають конкретну ціль для атаки, використовуються нові методи атаки, такі як вдосконалені атаки, пов'язані зі стійкими загрозами, з використанням так званих «нульових днів», шкідливих програм руткітів тощо. Тому з кібератаками потрібно поводитись комплексно через відсутність атрибуції та географічних меж, низькі витрати та низький ризик для зловмисника та великий масштаб застосовності. Отже, технічних заходів недостатньо поодинці, щоб впоратись із таким видом складних кіберзагроз.

Внаслідок різкого зростання складності шкідливих програм та комп'ютерних вірусів установи можуть бути вразливими до кібератак через

виникаючі кіберризики. Тому відтепер виникаючі кіберризики слід детально вивчати в новому розумінні обізнаності щодо кібербезпеки. У традиційному сприйнятті безпеки у кіберпросторі часто використовуються звичні терміни, такі як безпека ІКТ, InfoSec, забезпечення інформації, кібербезпека тощо. Однак розвинені багатовимірні та складні кібератаки вимагають і неявно дають деякі інші визначення та поняття, такі як національна кібербезпека, індивідуальна та корпоративна інформаційна безпека, обізнаність про кібербезпеку тощо. Крім того, через швидкі зміни у кіберсередовищі, розширення хмарних обчислень та залишкового використання мобільних пристроїв, особливо в установах, поняття та терміни, пов’язані з кібербезпекою, повинні бути перероблені з більш широкою точкою зору. Все це вимагає запровадження нових моделей кібербезпеки, одна з яких розглядатиметься нижче. Ця нова модель дозволяє нам розуміти кіберризики краще, ніж традиційні підходи, і в основному містить виклики, компоненти та основні принципи кібербезпеки на інституційному рівні, відповідно до чого ми її назвали моделлю інституційної кібербезпеки. Можна також сказати, що інституційна кібербезпека – це здатність, яка складається з компонентів інформаційної безпеки (InfoSec), співпраці з різними партнерами з кібербезпеки та обізнаності щодо кібербезпеки з точки зору кіберризиків.

Як зазначалось раніше, кіберсередовище, що визначається як «умовне середовище, в якому відбувається спілкування через комп’ютерні мережі», або «глобальний домен в інформаційному середовищі, що складається із взаємозалежної мережі інфраструктур інформаційних систем, включаючи Інтернет, телекомунікаційні мережі, комп’ютерні системи та вбудовані процесори та контролери» [443], швидко зростає.

У кіберсередовищі існують певні кіберризики. Кіберризик, який за своєю суттю існує у всіх ІТ-активах, є різновидом ризику, який виникає у різних акторів, від приватних осіб до міжнародних організацій, які мають критично важливі ІТ-активи. Кіберризик відрізняється від «звичайного» не

лише одним конкретним ризиком, а й технологією, переносниками, засобами тощо. Більше того, кіберризики мають дві характеристики: мають великий потенційний вплив та низьку ймовірність (рис. 5.1) [241].

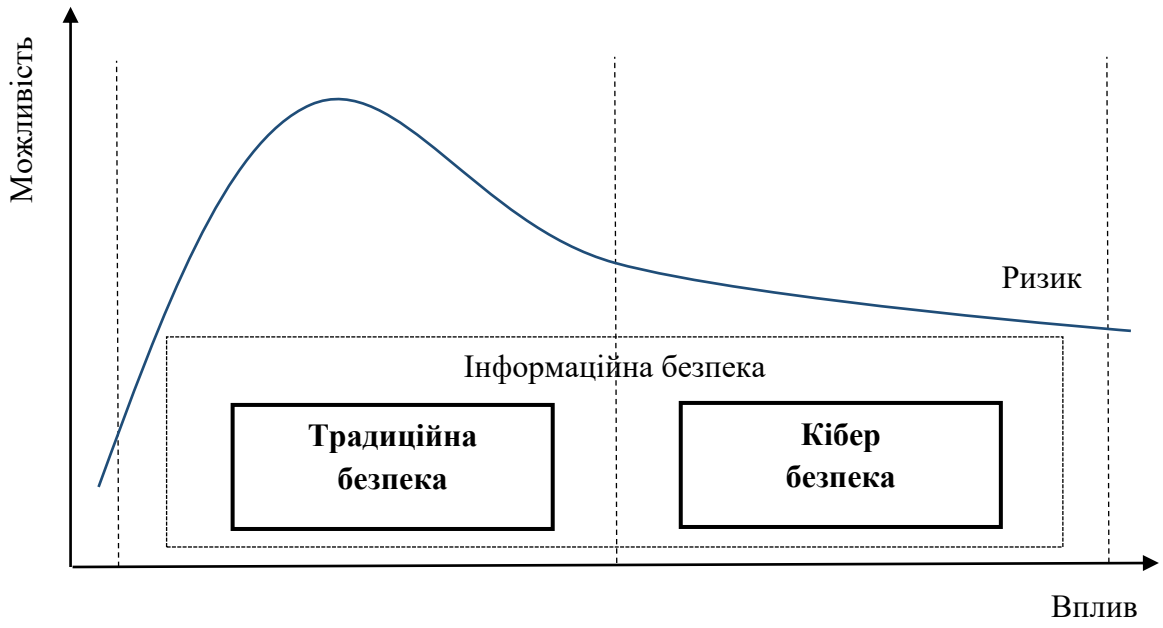

Рис. 5.1. Можливість і вплив кіберризику

Крім кіберризиків існує ще один важливий термін – кіберзагроза. Кіберзагрозу можна визначити як потенційну ситуацію, яка охоплює спотворення інформації, зміну інформації несанкціонованими людьми, розголошення чи викрадення інформації або перешкоджання її доступності. Джерелом кіберзагрози може бути інфікований комп'ютер або бот-мережа, що може складатися з мільйонів комп'ютерів. Отже, навіть один комп’ютер у кіберсередовищі, як з інформацією, яку він містить, так і з’єднанням з іншими системами, може бути джерелом для кіберзлочинців для досягнення критичних систем і порушення їх нормального функціонування.

Як показала практика останніх двадцяти років, можна визначити такий основний перелік кібератак:

– атаки соціальної інженерії в Інтернеті;
– мережеві сніфери та спуфінги пакетів;

– знаходження та використання вразливостей у програмному забезпеченні без вихідного коду;

– кіберзагрози та кібербулінг;

– автоматизовані зонди та скани;

– інструменти вторгнення графічного інтерфейсу;

– DDOS-атаки;

– промислове шпигунство;

– атаки на виконувані коди (проти браузерів);

– викрадення сесій;

– поширені атаки на інфраструктуру DNS та використання NNTP для розповсюдження атаки «Stealth» та інших вдосконалених методів сканування;

– трояни віддаленого доступу на базі Windows (Back Orifice);

– поширення шкідливого коду електронною поштою;

– широкомасштабне розповсюдження троянів;

– атака на конкретних користувачів;

– широкомасштабне використання хробаків;

– складні атаки ботнет-команд

– експлойти мобільних пристроїв на Android;

– Advance Persistent Threat (APT);

– хмарні атаки;

– вбудовані шкідливі програми;

– шкідливі компоненти на базі апаратного забезпечення;

– шкідливі програми Old School (MiniDuke).

Отже, кібератаки можуть варіюватися від фіктивного комп’ютерного вірусу (хробака Морріса) до APT, і вони розвиваються постійно та експоненційно. Ці кібератаки можна класифікувати як: кіберзлочинність, хактивізм, кібертероризм, кібершпигунство та кібервійна [264]. А ключовими аспектами у протистоянні ним є інформаційна безпека, інформаційне забезпечення та, звісно, кібербезпека.

Інформаційна безпека визначається як захист інформації або інформаційної системи від несанкціонованого доступу, модифікації або знищення [382]. Також відповідно до міжнародного стандарту ISO / IEC 27002: 2005, інформаційна безпека – це збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути задіяні й інші властивості, такі як достовірність, підзвітність, невідмова та надійність [там само].

Інформаційне забезпечення як поняття і практика є ширшим за інформаційну безпеку. Інформаційне забезпечення – це практика забезпечення інформації та управління ризиками, пов'язаними з використанням, обробкою, зберіганням та передачею інформації або даних, а також системами та процесами, що використовуються для цих цілей [461]. Інформаційне забезпечення включає захист цілісності, доступності, автентичності, безвідмовності та конфіденційності даних користувачів. Для виконання цих завдань воно використовує фізичний, технічний та адміністративний контроль. Незважаючи на те, що воно орієнтоване переважно на інформацію в цифровій формі, повний спектр інформаційного забезпечення охоплює не тільки цифрову, але й аналогову або фізичну форму інформації.

У свою чергу, з точки зору Міжнародного союзу електрозв'язку (МСЕ), кібербезпека – це сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, навчання, кращих практик, гарантій та технологій, які можуть бути використані для захисту кіберсередовища та організації й активів користувача. Активи організації й користувача включають підключені обчислювальні пристрої, персонал, інфраструктуру, додатки, послуги, телекомунікаційні системи і сукупність переданої та/або збереженої інформації в кіберсередовищі [315].

Концепція будь-якої безпеки містить компоненти, які є активами, ризиками, загрозами, вразливими місцями та контрзаходами. Як правило,

безпека у загальному випадку – це процес вибору та впровадження засобів контролю (також званих контрзаходами), які допомагають зменшити ризик, що виникає через вразливі місця [507]. Але процес захисту інформації та елементів, що пов’язані з інформацією, розвивається у міру того, як за нею стоїть технологія. Мотивацією цієї еволюції є головним чином зміна активів та ризиків, які породжує збільшення залежності від Інтернету, набір активів зростає з кожним днем, як було зазначено вище. На жаль, різноманітність кіберризиків зростає швидше. Через дуже взаємопов’язаний характер цих активів кожна вразливість впливає на інші, що робить еволюцію експоненціальною.

З іншого боку, за цією технологічною еволюцією невід’ємно стоять зміни з боку безпеки. Тому розуміння еволюції інформаційної безпеки та кібербезпеки вимагає аналізу питання про те, як / чому виникли ключові концепції у даній сфері. Поняттями, які в цьому випадку слід враховувати, є безпека ІКТ, інформаційна безпека та кібербезпека (рис. 5.2).

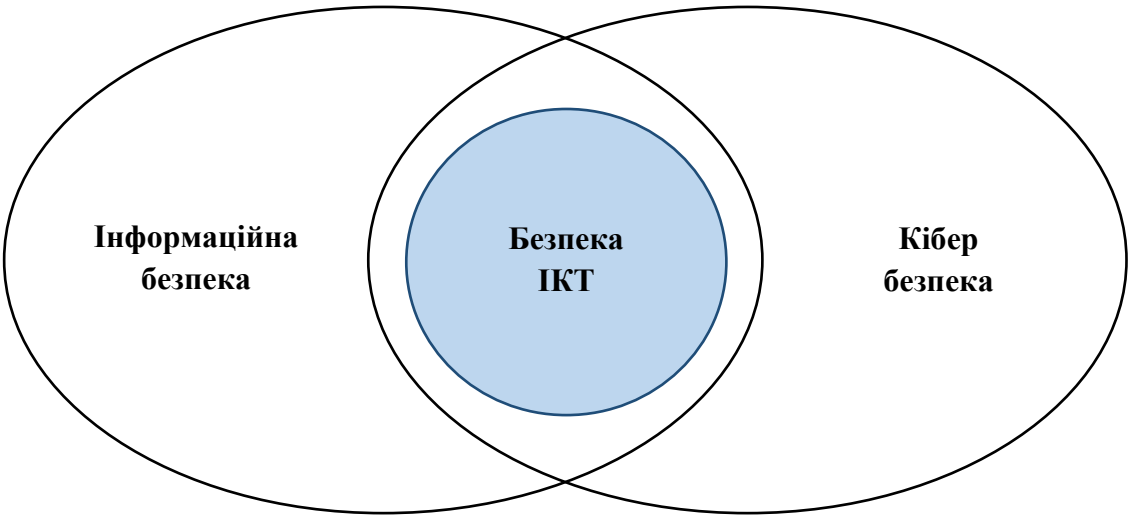

Рис. 5.2. Сфери інформаційної безпеки, кібербезпеки та безпеки ІКТ

Безпека ІКТ є місцем перетину інформаційної безпеки та кібербезпеки. Безпека ІКТ охоплює інфраструктуру інформаційних технологій, таку як

комп’ютери, комп’ютерні мережі, центри обробки даних. Крім того, ці активи можуть бути розширені в інформаційній безпеці на будь-яку інформацію, яку потрібно захистити. Згідно з цим розумінням, інформаційна безпека охоплює не тільки дані в ІКТ, але й інформацію, яка не зберігається та не передається через ІКТ. Тим не менше, як було зазначено вище, кібербезпека концептуально охоплює як інформаційні, так і неінформаційні активи, що становлять ризик за допомогою ІКТ. Типи цих активів включають широкий спектр того, що також охоплює критичну національну інфраструктуру, побутову техніку та навіть людину. Власне кажучи, у віртуальному просторі активами, які слід враховувати, може бути будь-хто чи будь-що, що є доступним через кіберпростір.

Коротко кажучи, інформаційна безпека має намір захистити цілі IT-інфраструктури та процеси, але через величезні розміри це може не забезпечити захист всього кіберпростору. Замість цього кібербезпека фокусується на усуненні вразливостей IT-активів.

З розширенням кіберпростору концепція інформаційної безпеки стає неадекватною для вирішення багатовимірних та складних кібератак. Наприклад, одна з передових шкідливих програм для кібершпигунства, «Червоний жовтень», була націлена на дипломатичні та державні установи у всьому світі щонайменше на п’ять років, що було виявлено в січні 2013 року [380]. Іншим прикладом є доповідь Департаменту національної безпеки США «Про комп’ютерні системи управління системами комп’ютерного реагування на надзвичайні ситуації» [361]. Згідно з цією доповіддю, у 2013 році найвищий відсоток інцидентів, про які повідомляли ICS-CERT, мав місце в енергетичному секторі – 53%. Інший приклад: як зазначено у звіті про безпеку Verizon 2020, лише за 2019 рік було 47000 інцидентів безпеки, і це свідчить про те, що зростання останніх порушень даних підштовхує організації для запровадження нових заходів і дій у відповідь.

Подібні практичні приклади та аналітичні узагальнення призвели до появи нових концепцій у сфері кібербезпеки, таких як національна

кібербезпека, індивідуальна та корпоративна інформаційна безпека, кіберінформованість (c-saw) тощо. І це цілком виправдано, адже постійні зусилля, у тому числі публікації різноманітних рекомендацій, з інформаційної безпеки на національному та міжнародному рівні вже не відповідали належним чином ризикам кіберпростору. Багато у чому це сталось через те, що інформаційна безпека ґрунтується на системах управління, які розроблені відповідно до міжнародних стандартів, таких як ISO 27001, серія NIST-800 та COBIT. Поточні версії цих міжнародних стандартів не відповідають повністю вимогам кібербезпеки. Тому, як зазначалось раніше, багато країн та міжнародних організацій розробили свої стратегії кібербезпеки, які зосереджуються головним чином на управлінні, співпраці та активній обороні. Однак на інституційному рівні не існує міжнародних стандартів чи настанов, які б включали співпрацю, інтеграцію до національної безпеки та активну оборону для боротьби з кіберзагрозами, такими як APT.

Через складний характер кібербезпеки виникло багато викликів, проблем та дилем як з національної, так і з інституційної точки зору. Наприклад, у Національному рамковому посібнику з кібербезпеки, підготовленому Центром кіберзахисту НАТО (NATO CCD COE), визначено такі дилеми, з якими стикаються зараз країни, встановлюючи, підтримуючи та застосовуючи заходи з кібербезпеки [385]:

1. Стимулювання економіки проти покращення національної безпеки.
2. Модернізація інфраструктури проти захисту інфраструктури.
3. Приватний сектор проти публічного сектора.
4. Захист даних проти обміну інформацією.
5. Свобода вираження поглядів проти політичної стабільності.

Подібно викликам на національному рівні, публічним організаціям і установам також потрібно вирішувати деякі дилеми, а саме:

1. Вартість IT-безпеки проти інституційної кібербезпеки.
2. Конфіденційність проти обміну інформацією.

3. Власний людський ресурс проти аутсорсингу.

4. Відкритий код проти ліцензійного програмного забезпечення.

5. Співпраця проти втрати репутації.

Через широко розповсюджені кібератаки, визначені вище, стабільна кібербезпека більше не є виключною відповідальністю технічного персоналу, це є спільною відповідальністю усіх працівників, стейкхолдерів та партнерів. Наприклад, працівник, не маючи достатньої кількості знань та обізнаності з питань кібербезпеки, або який недооцінює норми кібербезпеки, прийняті організацією, може в будь-який час спричинити досить суттєві, навіть критичні, для організації збитки, як матеріального, так і нематеріального характеру.

Поряд із національними та організаційними дилемами, для розуміння всього спектра проблем необхідно визначити також інституційні проблеми в галузі кібербезпеки. До основних таких проблем належать такі: відсутність більш широкого сприйняття кібербезпеки, обмін інформацією, правові проблеми, лідерство, людські ресурси, розширення кіберпростору, недостатність інфраструктури, наявні стандарти, побудова спільної картини кібербезпеки, відсутність метрик кібербезпеки, відсутність координації та обміну інформацією, питання безпеки та зручності використання, бюрократія, інсайдерські загрози, незахищені системи для захисту інших систем, технологічна сумісність тощо.

Зрозуміло, що виклики та проблеми кібербезпеки можуть диверсифікуватися ендемічно для країн та організацій відповідно до їхнього погляду на кібербезпеку. Наприклад, за словами Дмитра Айрапетова, директора з управління продуктами Dell SonicWALL, основними викликами в галузі кібербезпеки для підприємств на даний час є такі: збільшення наборів експлуатуючих програм, збільшення загроз кібербезпеки мобільних пристроїв та підвищення складності загроз [480].

Проте, з нашої точки зору, проблемою номер один для кібербезпеки як на національному, так і на інституційному рівні є відсутність більш

широкого сприйняття кібербезпеки. І приведення секторів та організацій до рівня стандартів безпеки в значній мірі залежить від національного сприйняття питань кібербезпеки, що також породжує зазначену проблему номер один. Наприклад, деякі уряди можуть вибрати централізацію більшості механізмів прийняття рішень, тоді як інші можуть перенести це на нижчий рівень відповідно до конкретної потреби (наприклад, для формування стійкості та реагування на надзвичайно децентралізовану та переважно приватну критичну інфраструктуру) [379]. Це рішення в основному вплине на загальнонаціональну проблему кібербезпеки. Навантаження на кібербезпеку для приватного сектору може бути небажаним, однак, терористичним організаціям або іншим суб'єктам, що фінансуються ворожими державами, так само легко напасти на суб'єкта приватного сектору, що реально вплине на національну економіку або безпеку [235].

Тому, як зазначалось у попередніх розділах, з урахуванням нових кіберризиків та більш складних шкідливих програм, країни та міжнародні організації, такі як НАТО, ENISA тощо, шукають нових способів боротьби зі складними проблемами у галузі кібербезпеки. Суттєвим кроком для країн є формування національної стратегії кібербезпеки та відповідних політик. Проте незважаючи на те, що ці стратегії та політики інтенсивно охоплюють військову, розвідувальну та критичну інфраструктури, кібербезпека на рівні організацій часто ігнорується. Але ми впевнені, що для забезпечення надійної кібербезпеки на національному рівні має бути забезпечена кібербезпека і на рівні організацій.

Тому ми пропонуємо структуру інституційної кібербезпеки (рис. 5.3), яка включає увесь спектр акторів (приватні особи, публічні та приватні установи, національні безпекові структури та міжнародні організації). У запропонованій моделі ми розглядаємо організаційних акторів як основних, таких, що разом утворюють «тілесну» основу організації кібербезпеки. Саме ця «тілесна» основа відіграє, на наш погляд, вирішальну роль у взаємодії всіх

інших акторів, і впливає на успіх кібербезпеки верхнього рівня.

Рис. 5.3. Структура інституційної кібербезпеки

Хоча найслабшим ланкою в інформаційній безпеці вважається людина, з точки зору національної безпеки найслабшою ланкою є найслабша організація, що підлягає впливам кіберризиків. Але на відміну від зазначених у національних стратегіях кібербезпеки положеннях, з точки зору моделі інституційної кібербезпеки, для забезпечення надійної кібербезпеки слід брати до уваги не лише організації, які управляють критичною інфраструктурою, а й всі інші організації, що мають кіберзахист. Наприклад, програмна компанія, не маючи жодної критичної інфраструктури, може стати мішенню для кібератак через викрадений програмний код або кореневий драйвер (справа SIEMENS та STUXNET) [408]

Поточні атаки, такі як випадок STUXNET, роблять потребу у

впровадженні моделі інституційної кібербезпеки неминучою. Для вирішення цієї потреби запропоновану нами модель можна визначити як комплексну модель забезпечення надійної та стійкої кібербезпеки на інституційному рівні шляхом:

– забезпечення кіберситуативності;

– регулювання нових кіберризиків;

– заохочення між- та внутрішньоорганізаційної співпраці та координації;

– представлення гнучкої основи для її застосовності для публічних та приватних організацій, що мають критичну інфраструктуру або кіберризики для безперервності своєї діяльності.

Запропонована нами модель забезпечує загальний підхід, за допомогою якого кожна організація може адаптувати дану модель до власних потреб безпеки для розвитку своїх можливостей із забезпечення кібербезпеки. Для досягнення цієї мети визначимо основні принципи інституційної кібербезпеки, що випливають з нашої моделі, до яких віднесемо такі:

1. Підхід до кібербезпеки повинен бути холістичним.

2. Слід застосувати гнучкий стиль управління.

3. Слід впроваджувати методи постійного вдосконалення діяльності, орієнтовані на управління ризиками.

4. На додаток до координації діяльності публічних, приватних, академічних та неурядових організацій, міжнародна співпраця та обмін інформацією також мають складати базис забезпечення кібербезпеки.

5. Мають заохочуватись прозорість, підзвітність, етичні цінності, свобода слова.

6. Важливим є встановлення балансу між безпекою та застосовністю ІТ-продуктів і технологій.

У світлі цих принципів, щоб бути ефективною, інституційна кібербезпека повинна мати основні компоненти, які представлено на рис. 5.4.

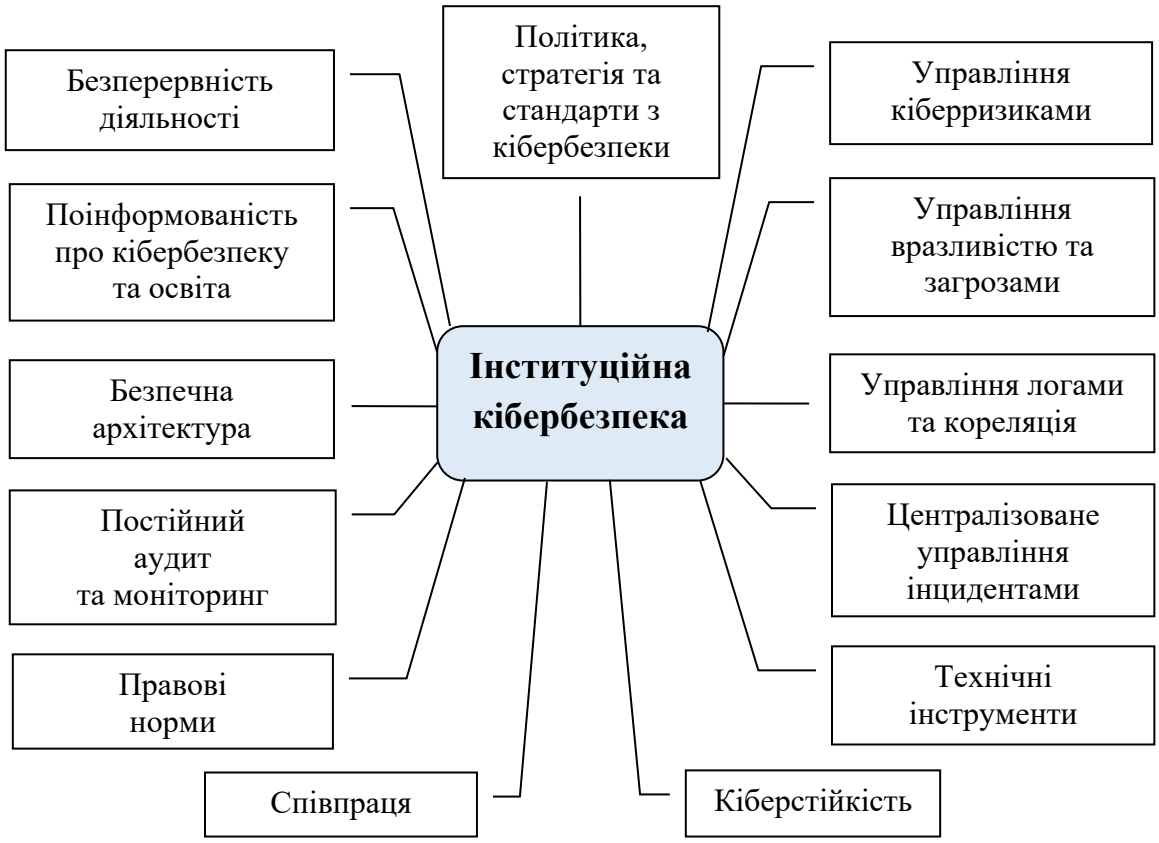

Рис. 5.4. Модель інституційної кібербезпеки

Розглянемо ці компоненти.

Політика, стратегія та стандарти з кібербезпеки. Відповідна політика, стратегія та стандарти можуть допомогти організаціям та іншим інституціям зробити перші кроки у напрямку забезпечення кібербезпеки.

Управління кіберризиками. Кіберризики можна мінімізувати та управляти ними, використовуючи ефективний механізм управління ризиками, який дозволяє розкрити всі загрози та уразливості.

Управління вразливістю та загрозами. Згідно з дослідженнями управління вразливістю та загрозами у кіберпросторі може здійснюватися під управлінням кібернетичними ризиками. Управління вразливістю повинно підтримуватися періодичним аналізом / тестами на вразливість та тестами на проникнення.

Централізоване управління інцидентами. Ефективне запобігання,

швидке реагування та пом’якшення наслідків кібератак можна отримати завдяки централізованому управлінню інцидентами.

Поінформованість про кібербезпеку та освіта. Людина є найслабшою ланкою в ланцюзі безпеки. Тому програми обізнаності з питань кібербезпеки та освіти повинні зосереджуватись переважно на людському факторі.

Управління логами та кореляція. Можливі атаки та витік даних можуть бути виявлені заздалегідь, а попереджувальні дії можуть бути виконані за допомогою ефективного управління логами та відповідної кореляції.

Безпечна архітектура. Усі інституційні інфраструктури та архітектури інформаційних технологій, включаючи партнерів, слід переглянути та поставити під сумнів з точки зору кібербезпеки.

Правові норми. Правові норми завжди є найважливішим чинником забезпечення кібербезпеки. Щоб запобігти порушенню конфіденційності та забезпечити процеси відповідальності, необхідно встановити відповідні правові норми. В іншому випадку контрзаходи щодо забезпечення кібербезпеки, такі як моніторинг особистої інформації, можуть створювати ризики для організацій та окремих осіб.

Технічні інструменти. Подібно до захисту ІКТ, для забезпечення всебічної кібербезпеки необхідно використовувати належне програмне та апаратне забезпечення, включаючи брандмауери, IPDS, антивірусне програмне забезпечення тощо.

Безперервність діяльності. Плани безперервності бізнесу повинні бути узгоджені з організаційними стратегіями та планами кібербезпеки.

Постійний аудит та моніторинг. Аудит – це безперервний процес, який містить певні тести або процедури перегляду. Помилки, порушення політики, шахрайство та проступки слід своєчасно перевіряти, щоб заповнити прогалини та недоліки у контролі. Моніторинг – це механізм, який можна використовувати для автоматизації ручного контролю та процесів або регулярних та частих аналізів, щоб уникнути потенційного порушення нормативних вимог, кібератак та зловмисних дій.

Співпраця. Співпраця з іншими партнерами, у тому числі міжнародними, з кібербезпеки є життєво важливою для організацій з метою встановлення механізмів раннього попередження та ефективного розподілу ресурсів. Крім того, через протистояння асиметричним та організованим кіберзагрозам неминуча координація органів влади з іншими установами, зокрема, з приватними.

Кіберстійкість. Усі зусилля в інституційному управлінні кібербезпекою повинні бути досить гнучкими, щоб адаптуватися до динамічного розвитку кіберпростору. Кіберстійкість часто визначається як здатність нації, організації чи місії чи бізнес-процесу передбачати, витримувати, відновлюватись та розвиватися для поліпшення можливостей протистояти стресам або атакам на підтримуючі кіберресурси, необхідні для функціонування [269]. Організація, що має властивість кіберстійкості, здатна протистояти систематичним атакам та адаптуватися до нових середовищ ризику або динамічно винаходити моделі діяльності та стратегії в міру зміни обставин у кіберпросторі та його розвитку. Згідно з [269], система кіберстійкості здатна забезпечувати комплекс заходів з передбачення загроз, витримування атак, відновлення нормального функціонування та організаційного/інституційного розвитку.

Досягнення мети ефективного використання всіх цих компонентів інституційної безпеки вимагає досягнення цілей кібербезпеки на інституційному рівні. Для цього необхідним є об’єднання цих компонентів у інтегровану структуру в стійкій перспективі. Крім всього іншого, це забезпечить впровадження адаптивної і гнучкої моделі управління кібербезпекою як на рівні окремих органів публічної влади, так і на національному рівні.

Отже завдяки вищезазначеним принципам та компонентам запропонованої моделі можна значно вирішити проблеми та дилеми у галузі кібербезпек. Також дана модель може забезпечити кращу реалізацію стратегії кібербепеки, розробці якої присвячено наступний параграф.

5.2. Теоретико-методологічна модель розробки національної стратегії кібербезпеки

Поки національні уряди борються із зростаючою кількістю широкомасштабних прихованих та публічних актів кібервійни, кіберзлочинності та кібершпигунства, науковці також не стоять осторонь цієї проблеми, адже стратегії національної безпеки, спрямовані на припинення хвилі цих атак, стають дедалі менш ефективними. Однією з можливих причин цього може бути розрив зв'язку між традиційними теоріями безпеки, які базуються на реальних реакціях на кінетичні загрози, та набагато іншим та складним середовищем кіберпростору. Цей теоретичний розрив був головною проблемою в галузі кібербезпеки, змусивши багатьох захищати агресивну політику наступу або політику стримування, намагаючись запобігти погрозам у кіберпросторі. Але дотримуватись принципів традиційних теорій безпеки, якщо застосовувати їх до кіберпростору, часто важко або навіть неможливо.

Крім того, у застосуванні до питань, що стосуються кібербезпеки, стратегії, породжені традиційними безпековими теоріями, як правило, зосереджуються лише на окремих аспектах, суб'єктах та / або одному типі вирішення проблеми. Можливо, тому перша реакція будь-якої розвиненої у технологічному плані держави у відповідь – почати власні кібератаки або створити загрози, спрямовані на іншу державу або державного актора, від якого вони відчувають загрозу. Приклади такої теоретичної однозначності можна знайти в корпоративному світі. Фірми, як правило, розглядають кібербезпеку через приціл негайних прибутків і збитків, а не розглядають її з точки зору довгострокових витрат проти вигод. Відповідно, вони порівнюють можливі короткострокові прибутки від недіяння на тлі значних фінансових витрат та логістичних труднощів у забезпеченні кращої безпеки. Коли трапляється велика атака, то стає вже занадто пізно. Суворе дотримання таких моделей прибутку часто робить корпоративну безпеку

короткозорою.

На щастя, уряди, схоже, мають більшу стурбованість цілісністю своєї інформації, головним чином через залежність сучасного суспільства від неї. Однак уряди також регулярно винні у короткозорості, коли справа стосується кіберстратегій, їх реалізації та адміністрування. Національна кібербезпека часто непропорційно будується на макрорівні. Це, як правило, спрощує захист лише для стратегічних дій, які можуть бути реалізовані в широкому, послідовному спектрі. За іронією долі, але саме цей широкий спектр обмежує органам влади сферу цих загроз лише охопленням конкуруючих держав або великих ворожих груп. Відповідно, держави спрямовують свої ресурси майже виключно на те, що цілком може бути для них великою загрозою, але, звичайно, не єдиною. При цьому держави часто нехтують альтернативними рішеннями.

Поступова, але послідовна мілітаризація та централізація управління у сфері національної кібербезпеки часто надає пріоритет безпеці над логістикою, а також тому, як ці дії уряду можуть впливати на поведінку та безпеку своїх громадян. Можливо, чистий негативний ефект ігнорування цих вужчих аспектів кіберстратегій є більшим, ніж загрози, які представляють державні актори або великі міжнародні групи.

Цей шлях до централізації та мілітаризації кібербезпеки посилюється в країнах, які є головними об’єктами кібератак, таких як США чи країни ЄС. Тому не дивно, що в цих країнах перспективи кібербезпеки та результуючі стратегії найбільше нагадують перспективи неореалізму. З точки зору неореалізму, рівень аналізу зосереджений на державах, а влада та безпека розглядаються як функції відносної вигоди від конкуруючих суперників. Це видається найбільш логічним, оскільки напади державних утворень є реальними, найбільш очевидними та представляють серйозну небезпеку для національної безпеки. Однак, як загальна кіберстратегія, неореалізм не розпізнає загрози та можливості для більшої цілісності систем, які представляють недержавні актори та технології.

Теорій безпеки, які зосереджені виключно на недержавних суб'єктах, таких як окремі люди та групи, та динаміці влади, якою вони діляться з державами, також недостатньо, щоб охопити всю загрозу кібербезпеці. Групи із спільною ідентичністю та цілями часто розглядають кіберпростір та баланс сил лише в контексті цих спільних норм. Ця ідея має тенденцію до зіткнення з цілями національної безпеки, що забезпечує верховенство держави над побудованими ідентичностями індивідів та колективів. Тим не менше, теорії соціальної конструктивістської безпеки вміють аналізувати спільне сприйняття як всередині, так і поза суспільством, і вміють розпізнавати як функцію ідентичності в динаміці національної безпеки, так і те, як ці сприйняття впливають на безпеку. Однак реалізувати цілком соціальну конструктивістську стратегію національної безпеки в середині зони кібервійни не є ані практичним, ані здійсненним. За таких умов існує необхідність координації кібербезпеки та звичайних стратегій та планів безпеки.

Однак неореалістичний та соціально-конструктивістський підходи на кібербезпеку поділяють подібну проблему. Вони обидва розроблені як інтерпретації традиційної міжнародної безпеки, і по суті, жоден з них не включає інформаційні технології у значній мірі, що є самим суттю кібербезпеки. Незважаючи на зручність обрамлення цифрових технологій в рамках традиційної теореми безпеки, цього в кращому випадку недостатньо. Однак існує дедалі більша спільнота дослідників питань безпеки, які намагаються встановити кібербезпеку в основному в цифровому, а не кінетичному вимірах. Серед цих теорій найбільш помітною є теорія «кібервестфальської» системи. Ця теорія базується на розвитку можливих або ймовірних майбутніх технологій, і стверджує, що державна централізація Інтернету в багатьох країнах, спільно з розвитком цих майбутніх технологій, призведе до появи національних «кібермеж». Дана теорія розглядає такі важливі аспекти кібербезпеки, як технології, міжнародні аспекти кіберсередовища, а також як державних, так і недержавних акторів. Однак ця

теорія не приділяє уваги ролі, яку відіграють чи можуть відігравати окремі громадяни та їх поведінці у кіберпросторі. Нехтування включенням цих суб'єктів у розгляд не дає можливості визначити переваги, які вони можуть принести національній кібербезпеці, й ігнорує нездійснення секвестру в Інтернеті активності людей у демократичному суспільстві. Кібервестфаліанство також дещо обмежене за своїм обсягом (кіберпростір) та підходом до рішень (технологія). Воно також не враховує економічну, політичну та військову динаміку між великими, середніми та регіональними державами. З цих причин ця теорія також є недостатньою перспективою, з якої можна сформувати особливу методологічну основу для національної стратегії кібербезпеки.

Усунути ці проблеми може певним чином теорія інтерсекційності, якщо її застосувати до кіберзбезпеки. Тому, на наш погляд, теоретико-методологічна основа розробки національних стратегій кібербезпеки має ґрунтуватись на інтегративному підході, що містить елементи інтерсекційності, неореалізму, соціального конструктивізму та кібервестфаліанства. Розглянемо докладніше унікальні та застосовні аспекти цих теорій.

Інтерсекційність.

Вперше визначена Кімберле Креншоу в 1989 році для пояснення расових відхилень у фемінізмі, теорія інтерсекційності пояснює проблеми з точки зору перетину окремих факторів [286]. Згодом ідеї цієї теорії були розширені для вирішення інших питань соціальних наук. Ця теорія стверджує, що такі проблеми, як соціальна несправедливість, породжуються не лише одним аспектом, подією чи системою, скоріше вони є результатом зближення чи перетину численних факторів на різних рівнях та з різних середовищ, що вимагають проведення різних типів аналізу. Нещодавно цю теорію застосували до галузі кібербезпеки такі вчені, як Бен Фіцджеральд [326] та Тара Давенпорт [289]. З цієї точки зору проблеми в кібербезпеці не розглядаються як виключно політичні, соціальні чи технічні, а є перетином

усіх трьох факторів [326].

Саме ці «правильні набори перехресть», можливо, мали місце протягом останніх п’ятнадцяти років під час великих кібератак. У політичному плані багато державних керівників обирали внутрішню політику шифрування, яка здавалася обґрунтованою та сприяла національній безпеці. Така політика може бути розглянута в контексті політичної науки, де досліджуються політична мотивація, політика влади та законодавчі фактори. Як варіант, аналіз згаданої політики можна розглядати через приціл неореалізму. Такий підхід розглядав би втрату або виграш відносної сили певної держави через її національну політику щодо публічних ключів. Кібервестфальці також можуть розглядати це як захисний механізм, який служить типом кіберкордону.

Цілком на іншому рівні проблему можна вивчати як функцію групової чи культурної ідентичності кінцевих користувачів або кіберзлочинців або обох цих груп. Багато хто вирішив розглядати будь-яку проблему, пов’язану з кібербезпекою, як технічну проблему, і вважають, що відповідь знаходиться в технологіях. Усі ці підходи, події та актори перетинаються між собою в різних точках на часовій шкалі, що, на наш погляд, сприяє проясненню проблем кібербезпеки та їх вирішенню.

Креншоу визначає проблему особливого аналізу, який розділяє соціальну несправедливість на різні виклики, що стоять перед певними групами (раса, стать, сексуальна орієнтація або соціально-економічний статус) [286, с. 158]. Окремо ці аналізи пропускають загальну картину, створюючи конкуренцію та розподіл між проблемами та розриви у перспективах, які затуманюють важливі проблеми. Аналогічно аналіз кібератак може припустити, що вони були просто проблемою поганої безпеки мережі або неминучим результатом цілеспрямованого хакерського злому. І хоча кібербезпека та соціальна справедливість є помітно різними сферами, але основне розуміння інтерсекційності справедливо для обох.

Сфера кібербезпеки, на наш погляд, повинна вийти за межі дискусій

щодо того, чи основне питання стосується проблеми А чи проблеми Б, теорії А чи теорії Б. Натомість кібербезпека повинна розуміти взаємозв'язок між усіма проблемами та використовувати всі відповідні теорії для підходу до цих проблем [326, с.4].

Неореалізм.

Неореалістичний погляд на політичні та міжнародні відносини, викладений Кеннетом Вальцом наприкінці 1970-х років, окреслює дії націй як реакцію на структурні обмеження відносної влади [510]. Теорія Вальца про відносний баланс сил є досить всебічною для визначення того, як держави взаємодіють одна з одною в міжнародній системі, яка є децентралізованою та анархічною. Тому цілком зрозуміло, чому багато нинішніх науковців з питань кібербезпеки та політиків вважають неореалізм корисним у формуванні стратегії кібербезпеки. Керуючись власним виживанням у міжнародній структурі, держави розвивають свої кібернетичні можливості для того, щоб або збільшити, або захистити свій відносний баланс сил [там само].

Кібербезпека добре вписується в неореалістичну модель з кількох причин. Інтернет за своєю природою є анархічним. Ця децентралізація віртуального простору ускладнює координацію зусиль на міжнародному рівні або повсюдне запровадження міжнародного законодавства Це дозволяє застосовувати стратегії кібербезпеки, які є менш загальними, відтак, краще пристосованими до особливостей окремих держав. Через це держави можуть вільніше мілітаризувати свої можливості як в обороні, так і в атаці. Уряди також можуть намагатися контролювати доступ своїх громадян до зовнішньої інформації, коли ця інформація є політичною, підриває державний авторитет або загрожує національній безпеці. Такий контроль може поширюватися і за межі держави, як це було у відомому випадку, що стосувався шкідливого впливу Росії на Естонії.

У квітні 2007 року серед етнічного російського населення почалися акції протесту з приводу знесення естонським урядом пам'ятника радянської

війни. За підтримки Кремля антиурядові настрої в Естонії переросли за межі вулиць і перекинулись на кіберпростір. Те, що спочатку починалося з опорочення веб-сайтів естонських урядів, незабаром переросло у кібервійну. Державні хакерські групи, що базувались у Росії, змогли використати мільйони комп'ютерів, заражених шкідливим програмним забезпеченням «зомбі», для запуску атак відмови в обслуговуванні, які поклали зв'язок та банківські мережі в Естонії. Вважалося, що ці групи підтримуються та використовуються російським урядом і є частиною зростаючого співтовариства підпільних хакерів у Росії, які використовують свої навички для отримання нелегальної вигоди. Це був спосіб для Росії покарати свого колишнього сателіта, який приєднався до ЄС, і рухався до більш міцних зв'язків з НАТО [278]. По суті, російський уряд використав протест як привід для спроби розширення сфери свого впливу в регіоні.

Захист національної безпеки та міжнародного впливу в моделі з нульовою сумою (котра, як правило, пов'язана з ресурсами, військовою потужністю та відносною економічною перевагою) є загальноприйнятою ідеєю серед таких адептів неореалізму, як Джон Мірсхаймер [411]. В наступальному реалізмі держави проектують владу на міжнародному рівні, щоб запобігти посяганню на їх відносну владу таким чином, що відповідає ідеї «найкраща оборона - це хороший злочин». Ці держави вступатимуть у конфлікт лише тоді, коли результатом буде чистий прибуток для держави та чистий збиток для його супротивника. Такі стратегії можна спостерігати в міжнародному кіберконфлікті. Як і у випадку з Росією та Естонією, деякі потужні держави здійснюватимуть превентивні кібератаки та кібератаки помсти (часто приховано), оскільки їх непропорційна перевага влади у вигляді більших ресурсів, кваліфікованої робочої сили та більш досконалих технологій, найімовірніше, призведе до відносного виграшу. Однак потужні держави атакують й інші потужні держави, незважаючи на відсутність будь-якої переваги. Такі атаки часто трапляються в невеликому масштабі, оскільки існує побоювання, що атака іншої сторони є неминучою, а не

попереджувальна атака представляє чисту втрату відносної сили.

Річард Кларк таким чином характеризує мілітаристський аспект неореалістичного аргументу, описуючи кібератаку Північної Кореї на Південну Корею в 2009 році:

«Нові кібер-воїни (у Північній та Південній Кореї) та велика частина засобів масової інформації оголошують ці випадки як перші публічні зіткнення національних держав у кіберпросторі. Є й інші приклади, зокрема операції Китаю, Тайваню, Ізраїлю та ін. Деякі називають справу Естонії «Першою веб-війною» [278, с. 15].

Однак існують потенційні підводні камені в тому, щоб розглядати кібербезпеку суворо з неореалістичної точки зору. По-перше, єдиним рівнем аналізу тут є держави та національні інтереси. Проте багато кібератак часто ініціюються особами з мотивами, що не відповідають національним інтересам та фінансовій вигоди. Хактивістські групи, такі як «Анонім», часто мають політичні програми, не пов’язані з жодним урядом чи державою, і зазвичай проводяться без державної підтримки. Хакери часто координують транскордонну діяльність та соціальні групи для досягнення цілей, які мають мало спільного із співвідношенням сил у міжнародній системі. На відміну від національних військових та інших урядових структур, що використовуються для захисту або збільшення відносного співвідношення сил, доступ до Інтернету не обмежується лише державою. Крім того, суб’єкти, що користуються Інтернетом, які не включені в неореалістичні спостереження (тобто особи, політичні групи та корпорації), також не обов’язково мотивовані інтересами національної безпеки.

По-друге, неореалізм припускає, що держави з найбільшими ресурсами мають найбільшу владу, а отже, вони більш безпечні, ніж держави з меншими ресурсами та меншою відносною владою. Однак великі армії, передові технології та великий ВВП не потрібні для ведення кібервійни. Будь-яка країна може завдати серйозної шкоди, все що для цього потрібно – це комп’ютери з доступом до Інтернет та спеціалізовані особи, які мають

досвід для здійснення нападів. Це ми вже спостерігали в таких країнах, як Північна Корея, де загалом, інфраструктура та суспільство менш залежать від кіберпростору. Відсутність кіберінфраструктури заважає більш прогресивним у технологічному відношенні країнам не порушувати оперативну логістику більш слабких країн через Інтернет, а отже, робить менш просунуті країни, що розвиваються, більш захищеними від кібератак. І навпаки, висока залежність від Інтернет та складна, комп'ютерно-інтегрована інфраструктура в таких країнах, як США, роблять їх більш вразливими до електронних атак [278]. Отже, асиметричний та децентралізований характер кібернетичних можливостей у країнах, що розвиваються, ускладнює адаптацію цілком неореалістичної філософії до кіберзахисту.

Соціальний конструктивізм.

Оскільки наше дослідження стосується у тому числі можливостей, мотивів та поведінки окремих недержавних суб'єктів, важливо вивчити елементи соціального конструктивізму, що стосуються кібербезпеки. Накопичення особистих даних як кіберзлочинців, так і кінцевих користувачів відіграють важливу роль у забезпеченні кібербезпеки багатьох країн. Однак, вибір такої теоретичної бази, на якій можна інтерпретувати дані кібератак з точки зору окремих суб'єктів був предметом наукових дискусій. Однією з таких теоретичних баз все більше фахівцями з кібербезпеки розглядається зараз соціальний конструктивізм. Конструктивісти, як правило, розглядають Інтернет як провідник для груп людей із спільною регіональною, культурною або нормативною ідентичністю для пропаганди ідеації. Зокрема, Ерікссон, Джакомелло та Ранспорт вже писали про те, як на кібератаки впливають побудовані ідентичності [316, с. 181].

Хоча в ній нічого не згадується про кібербезпеку, теорія «сек'юритизації», розроблена «Копенгагенською школою» в рамках конструктивістського підходу, пропонує аналіз політики загроз на основі сприйняття та побудованих ідентичностей. Питання безпеки формуються політичними суб'єктами на основі їх сприйняття загроз. Ці спільні уявлення

формуються навколо того, як і коли виникають загрози та з якими наслідками. На думку «Копенгагенської школи», сприйняття формується за допомогою «мовленнєвих актів», тому її дослідження частково спрямовані на вивчення мови, що використовується для формування загроз. Таким чином, повідомлення, що передують кібератаці якоїсь держави на іншу, можна розглядати як явні урядові «мовленнєві акти», покликані сформувати уявлення про певну агресивну поведінку. Це дуже корисно при вивченні політичної риторики, яка супроводжує напади. Однак при вивченні кіберзагроз, представлених окремими державними акторами, також потрібна система, більш відповідна колективним діям та поведінці людей у кіберпросторі.

Йохан Ерікссон розвиває концепцію «Копенгагенської школи» на крок далі і пов'язує її з кібербезпекою у своєму дослідженні сек'юритизації ІТ у шведській політиці. Однак замість того, щоб виявити слабкі місця у поведінці шведських ІТ чи шведській політиці щодо ІТ, його аналіз зосереджується на тому, хто винен чи що винно у кіберзагрозах, і як розподіляється відповідальність за боротьбу із ними [317, с. 211-212]. Знову ж таки, мова стає важливою, оскільки відповідальність за «кіберзлочинність» та «кібервійну» підпадає під різні сфери діяльності. Кіберзлочинністю повинна займатися поліція, роблячи злочинців учасниками аналізу.

Влада частково знаходиться у цивільних руках. Тоді як кібервійна є відповідальністю військових, і держави потім стають аналізованими суб'єктами. Це має сенс з точки зору організації величезної кількості кіберзагроз, спроби встановити особу зловмисників та делегування відповідальності за захист від них. Однак таке рішення виглядає скоріше post-hoc, оскільки воно не стосується властивих слабких місць соціальної системи.

Конструювання ідентичностей спрямоване назовні (до злочинця, держави чи установи), а не колективних ідентичностей самості [521]. Аналіз кібератак та того, як їх можна запобігти, спершу слід розпочати з дій людини

щодо колективного розуміння Інтернету. Важко було б виправити системні проблеми, переслідуючи окремі події та різні мотивації окремих акторів. Однак вже існують конструктивістські теорії, які зосереджуються на колективізмі з огляду на конкретні кіберподії. Так, Джакомелло описує конструктивістський підхід до міжнародної кібербезпеки, який включає метод нападів [316]. У своєму аналізі Джакомелло зосереджує увагу на індивідуальному та колективному сприйнятті всього, що стосується ІТ. Однак він все ще орієнтований на мову і розглядає, як використовуються такі терміни, як «вірус», «шкідливе програмне забезпечення», «помилки», «брандмауери» тощо:

«Використання таких термінів, як «інформаційна війна» та «електронний Перл-Харбор», надає особливого значення: те, що є цифровим за своєю природою, має, однак, фізичні наслідки, порівнянні з наслідками звичайної війни. Конструктивістський аналіз може сприяти виявленню та розумінню значення такої риторики та символічних дій» [316, с. 21].

Хоча, можливо, і дещо заглиблений у терміни та символіку, Джакомелло робить вагому аргументацію щодо використання конструктивістської системи для вивчення кібератак та їх впливу на міжнародну безпеку. Його аналіз можна винести за межі символізму, включаючи інші види дій, а саме соціальні норми та поведінку в Інтернеті. Наприклад, в Україні індивідуальне та колективне сприйняття кібербезпеки сягає своїм корінням не лише з українського «онлайн-світу», а й із культури та дій «поза Інтернетом».

Еріксон згадує про ці дії, аналізуючи успіх вербування Аль-Каїди по територіях [317]. Він описує, як Аль-Каїда змогла поєднати колективні ідеї у переконання, що об’єднана поведінка перетворюється на заклик до дії. Він також спростовує твердження про те, що існує відсутність теорії стосовно відносин між окремими агентами та міжнародною безпекою. Він заявляє: «Конструктивізм, схоже, пропонує цінний шлях до цієї загадки (тобто розрив між структурними теоріями міжнародної системи та мікропрактиками

окремих суб'єктів, що займаються просуванням нормативних програм). Дії можна концептуалізувати як низку аргументів щодо певної ідентичності» [317, с. 32].

У випадку з Україною, «нормативні дії» вже об'єднані (за допомогою владних дій або української культури), і ми можемо легко судити про їхній вплив не тільки на кібербезпеку, але і те, як вони пов'язані з міжнародною безпековою системою.

«Соціальну теорію міжнародної політики» Олександра Вендта, ще одного представника конструктивізму, також можна адаптувати для інкапсуляції кіберзагроз та їх запобігання. Хоча теорія конкретно не стосується кібербезпеки, вона включає як культурні, так і міжнародні аспекти, що переважають під час кібератак останнього десятиріччя. З точки зору Вендта, колективна ідентичність і соціальні норми та практики пов'язані з міжнародною структурою через сприйняття суспільством елементів цієї структури [519]. Його теорія також добре поєднується з динамікою української культури та суспільства. Спостережувана колективна поведінка може бути використана для пояснення не лише сприйняття Україною безпосередньо зовнішніх кіберзагроз, а й сприйняття їх зв'язку з міжнародною системою безпеки.

Вендт визначає колективну ідентичність як колективну ідентифікацію спільних характеристик Я (у нашому випадку українців) від інших (не-українців). Вендт стверджує, що помітність колективної ідентичності для окремих людей визначає силу прихильності суспільства до неї. Колективна ідентичність створює структури у формі органів влади та корпорацій, які підсилюють ідентичність та поведінку шляхом централізації та інтерналізації [519]. Ці самоукріплюючі структури колективної ідентичності проявляються у централізації та інтерналізації норм та поведінки в Інтернет українськими приватними організаціями та органами влади. Вендт також вважає, що участь у громадській діяльності пов'язує людей з подіями та практиками. Ці практики посилюються шляхом інтерналізації. Отже, поведінка, як

ідентичність, може бути спільною.

Зв’язок колективної ідентичності з міжнародною системою безпекою залежить не тільки від структури міжнародної безпеки, але й від того, як ви розглядаєте цілі окремих суб’єктів системи. Для неореалізму це означає анархічну систему з державними суб’єктами, кінцева мета яких є матеріальною (наприклад, економічною, владною, гегемоністською, військовою тощо). Для неоліберaлів і конструктивістів це означає структуровану міжнародну систему безпеки також із державними суб’єктами, але метою якої є співпраця задля більшої, стабільнішої колективної винагороди. Вендт стверджує, що науковці повинні думати про зв’язок з міжнародною системою безпеки в соціальному, а не матеріалістичному плані. Навіть анархію можна розбити на певні елементи, які сприймаються як актори (тобто нації, індивіди, суспільство). Він пише: «Структура анархії змінюється залежно від змін у розподілі ідей» [519, с. 310].

Якби поведінка в Інтернеті була лише продуктом обмежень, встановлених урядом, тоді зміни в такій поведінці (і директивах) також повинні були б виходити виключно від держави. Проте, як показує практика, ці зміни можуть відбуватися і через дії колективної ідентичності. З огляду на велику роль, яку індивідуальна та колективна ідентичність та поведінка відіграють у проблемі забезпечення кібербезпеки, надзвичайно важливо, щоб ці аспекти вимірювались та аналізувались в конструктивістській перспективі. Поведінка та ідентичність повинні вимірюватися у джерелі а також повинні вимірюватись вплив на них відповідної політики. Однак конструктивістський аналіз може пояснити технологію лише з точки зору того, як вона впливає на колективні ідентичності, а не ефективність цих технологій як кіберзахисту.

Незважаючи на переконливий опис конструктивістами кібердинаміки, її акторів та зв’язків із міжнародною системою безпеки, важко буде переконати тих, хто знаходиться за межами конструктивізму (особливо тих, що знаходяться в уряді), що кіберінфраструктуру можна адекватно захистити

виключно шляхом визнання ідентичності як ідеї. Крім того, конструктивізм не може пояснити технологічні прогалини між кінцевими споживачами та не пояснює, як технологія може вплинути на проблему кібербезпеки та запропонувати відповідні рішення.

Кібервестфальська теорія.

Кріс К. Демчак та Пітер Домбровський у своїй роботі «Підйом кібернетичної Вестфалії» [294] стверджують, що відносно некерований кордон кіберпростору, як і всі кордони, не триває вічно, коли задіяні людські суспільства. Врешті-решт національні держави поширять свій суверенітет на Інтернет і здійснюватимуть контроль над електронною інформацією, яка надходить і виходить до/із їхніх національних доменів. По суті, нації створюватимуть електронні кордони. Демчак і Домбровський наводять останні події в політиці кібербезпеки розвинених країн як свідчення того, що держави вже рухаються до межевого Інтернету. Тому ця теорія вже визначає певні умови національної кібербезпеки та процес, через який країни створюватимуть кібермежі за допомогою технологій.

За словами Демчака та Домбровського, перетворення від кордону до субстрату через кіберпростір почалося з відкриття вірусу Stuxnet у 2010 році. Stuxnet був вірусом, закладеним в системах іранської ядерної центрифуги, і врешті-решт він повернув іранську ядерну програму на роки назад. Вважалося, що зловмисне програмне забезпечення було завантажено в іранську безпечну офлайн-систему через флеш-накопичувачі USB. Геніально розроблений, вірус застосував багато нових складних методів і кодів, розроблених з урахуванням конкретних знань про його мету. Такі зусилля вимагали ресурсів передової країни з розгалуженою розвідувальною мережею, що привело багатьох експертів до думки, що вірус був створений США, Ізраїлем або обома ними.

Не маючи віддалених вказівок, Stuxnet прискіпливо шукав і знищував заздалегідь визначену секцію центрифуги і продемонстрував, що сильно захищені системи, не підключені до кіберпростору, все ще вразливі до

кібератак. На думку Демчака та Домбровського, це був переломний момент у політиці кібербезпеки, і зараз розвинені країни мають конкретний приклад кіберзагрози з реальним катастрофічним потенціалом. Що ще важливіше, тепер у них є причина провести межі та встановити суверенітет над Інтернетом.

Демчак і Домбровський стверджують, що реакцією на подібні можливі загрози буде подальший рух до закритої межевої системи Інтернету, яка зможе більш ретельно вивчати іноземні дані і тим самим запобігти потенційним загрозам національній безпеці. Це видно з того, як держави адмініструють кібербезпеку. Кіберпростір більше не під юрисдикцією державних комунікаційних та комерційних установ. Зараз багато промислово розвинених країн ставляться до кіберпростору як до ще однієї оперативної військової сфери. Такі країни, як Китай та США, розробляють технології та оборонні стратегії, які б створили кордони в кіберпросторі та дозволили б країнам боротися із загрозами; навіть коли ці загрози надходять від власних громадян. Ці країни вже продемонстрували свою готовність піти в наступ, щоб захистити національні інтереси. Завдяки «кіберкомандуванню» кожної нації військові технологічно розвинених країн вступають у кібервійну, яка виходить за рамки простого шпигунства або вандалізму, оскільки вони прагнуть поширити свою парадигму регіональної та міжнародної безпеки на кіберпростір. Такі дії змусили менш розвинені в технологічному відношенні країни підштовхнути своїх більш розвинених союзників до захисту свого кіберпростору за допомогою традиційних механізмів безпеки та організацій, таких як НАТО та ООН, оскільки кібервестфальська карта починає формуватися [294].

Концепція розділеного, визначеного, організованого та контрольованого кіберпростору суперечить тому, як більшість людей сприймає Інтернет. Це не далекий, малонаселений регіон країни, а також не ізольована нічия земля. Кордон кіберпростору – це мережа мільярдів систем практично в усіх частинах світу, в якій є рівна кількість різноманітних

учасників. Експоненціальне прискорення технологічної еволюції та інновації в ній сформували середовище, в якому агресорам вдається випередити оборонні стратегії та системи. Програмне та апаратне забезпечення, призначене для крадіжки інформації, підриву систем, порушення публічної політики та маскування особистості користувача, вільно ділиться між хакерами. Також користувачі комп'ютерів у ліберальних демократіях звикли до свободи, яку надає безмежний кіберпростір. Спроби урядів закрити скриньку Пандори часто зустрічають опір, який виливається на політичну арену і має значний вплив на державну політику. На відміну від фізичного кордону, стримування у віртуальному просторі здається неможливим. Однак Демчак та Домбровські стверджують, що повернення суверенітету через Інтернет є технологічно можливим, психологічно комфортним і системно та політично керованим.

Демчак і Домбровський стверджують, що нова карта кіберпростору, укомплектована межами та кордонами, які приймають усі держави, є неминучою [294]. Початок цього з різним ступенем вже можна побачити в таких країнах, як США, Китай, Південна Корея та країни ЄС. Однак вивчення не лише кібервійськової політики цих держав, але також їх державної та комерційної політики в Інтернеті виявляє, що ліберально-демократичним країнам буде важко здійснювати та застосовувати навіть багато основних обмежувальних кіберполітик. Крім того, створення кіберкордонів залежить від розподілу віртуального простору за допомогою технологій та національних державних стандартів. Хоча держави можуть мати спільні програми щодо кібербезпеки, вони рідко мають спільні стандарти щодо реалізації кібербезпеки. Такі роз'єднання в кіберполітиці перешкоджатимуть потоку кібертрафіку, необхідного для багатьох форм міжнародного спілкування та комерційної взаємодії.

Деякі дослідники застосовують підхід теорії ігор до бінарних варіантів (відомий як взаємозалежне рішення щодо інвестицій у безпеку) до міжнародної кібербезпеки, який підкреслює два моменти. По-перше,

ймовірно, що держава адекватно інвестує в кібербезпеку, безпосередньо пов’язану із рівнем загрози, на якому вона сприймає кіберпроникнення. По-друге, для того, щоб кіберкордони були ефективними, у процесі їх визначення та визнання повинні брати участь усі нації.

Так, Хейр використовує власну модель взаємозалежних ліберальних демократій, щоб також показати, що для того, щоб кіберкордони були ефективними, у їх визначенні повинні брати участь усі відповідні країни. Чим менше держав бере участь, тим більша ймовірність успішного нападу однієї держави на іншу [345]. На думку Хейра, побудова кіберкордонів майже не принесе користі державам, якщо вони підтримують зв’язок із союзниками, які не визнають таких кордонів. У той же час, оскільки корисність Інтернету розширює свою залежність від комунікацій, керованих Інтернетом, і в міру збільшення торгівлі, створеної в безмежному кіберпросторі, держави можуть бути менш схильними до участі. Таким чином створюється більше перешкод для кіберкордонів, що робить кібервестфальську систему менш імовірною.

З цього приводу можна навести приклад Південною Кореї, який є досить показовим. Ця країна вже зазнала труднощів, пов’язаних з обмеженням кіберпростору. На додаток до ранньої політики у цій сфері, яка вимагає використання технології SEED, південнокорейській уряд також почав обмежувати анонімність, вміст та доступ до іноземних сайтів, намагаючись зберегти моральну та соціальну цілісність свого кіберпростору. Однак ці дії мали непередбачені наслідки обмеження комерційного потенціалу Інтернет та сприяння крадіжці особистої інформації його громадян. Як не дивно, але ці нові заходи безпеки фактично зробило південнокорейські системи більш вразливими до вторгнень, і протягом останніх п’ятнадцяти років Південна Корея стала жертвою багатьох успішних широкомасштабних кібератак.

Як і у випадку з Південною Кореєю, державам, які переслідують кордони в кіберпросторі, доведеться або різко змінити характер і обсяг

планів націоналізованого кіберпростору, або взагалі відмовитись від цієї концепції. Крім того, модель Демчака та Домбровського базується на твердженні, що віртуальні кордони технологічно можливі, психологічно та політично керовані. Однак це, на наш погляд, не зовсім так. Технологічно кажучи, було здійснено низку нововведень, які роблять можливими кордони в кіберпросторі. Однак вони не позбавлені логістичних обмежень. Хоча розвинені країни цілком можуть бажати кіберкордонів, їх реалізація може бути неможливою. На жаль, у сукупності кіберзлочинці історично мали перевагу над тими, хто захищав національні кіберсистеми. В рамках параметрів поточної архітектури Інтернет все ще не вдається виявити нові шкідливі коди, знайти та ідентифікувати зловмисників або повністю захистити життєво важливі офлайн-системи. Навіть якщо майбутні технологічні досягнення дозволять країнам секвеструвати їх національну кіберінфраструктуру, немає гарантії, що такі дії роблять системи більш безпечними.

Технології, що забезпечують кордони в кіберпросторі, повинні мати можливість сканувати всю інформацію, що надходить через його мережі, з метою виявлення шкідливих або незаконних кодів, розмежування національного та міжнародного вмісту, а також виявлення та визначення місцезнаходження їх джерел. Загальноприйнята думка полягає в тому, що такі заходи безпеки просто неможливі, і що жодна оборона не є непроникною. Незалежно від того, яку стратегію оборони або технології можуть розробити держави, надавши достатньо часу, кожна система може бути зламана. Сучасна технологія не може сканувати всі вхідні дані, щоб визначити їх національне походження та потенціал загрози, а також сучасні криміналістичні методи не завжди можуть відстежувати джерело зламу та особу хакера. Втім, Демчак і Домбровський сперечаються проти цього [294].

Те, як громадяни сприймають роль свого уряду в кіберпросторі, сильно відрізняється від держави до держави. Культура, історія та демографія є визначальними факторами менталітету нації щодо таких питань, як

приватність, свобода інформації, інтелектуальна власність, наклеп та довіра до уряду. Кіберкордони можуть бути психологічно прийнятними в одному суспільстві, але не в іншому. Ці елементи національного менталітету можуть також перешкоджати переходу до вестфальського Інтернету.

Наприклад, у Китаї уряд відчув дуже малий опір своїй обмежувальній політиці в Інтернеті. Починаючи з середини 1990-х років, послідовні нормативні акти все більше обмежували те, що громадяни Китаю можуть говорити або отримувати доступ до Інтернету. Це призвело до створення розділу п’ятого «Положень комп’ютерної інформаційної мережі та Інтернет», що стосуються безпеки, захисту та управління, затвердженого Державною радою 11 грудня 1997 р. Цей закон передбачає кримінальну відповідальність за використання Інтернет для створення, тиражування, отримання чи передачі будь-чого, що підбурює не лише до злочинних та зрадницьких дій, але до всього, що завдає шкоди національному об’єднанню та пропагуванню неправди, пороків та наклепів [349].

На додаток до цензури урядової критики в Інтернеті, багато комерційних та соціальних мереж, таких як Google та Facebook, заборонені та замінені їхніми внутрішніми аналогами. Існує 18 000 веб-сайтів, заблокованих урядом Китаю [там само]. Штрафи за порушення цих правил або використання віртуальних приватних мереж для обходу політики можуть бути жорсткими. Але, незважаючи на загрозу позбавлення волі, досі існує приглушена зустрічна реакція на дії уряду, часто через сатиру та сарказм. Так, китайські веб-сайти висловили тонкі скарги на державну цензуру, саркастично назвавши дату 4 червня (річницю різанини на площі Тяньаньмень) 1989 року «Днем підтримки китайського Інтернету».

Існують і ті країни, які прагнули контролювати потік певної чутливої зовнішньої та внутрішньої інформації лише для того, щоб виявити, що їх зусилля підриваються громадянами, які не бажають відповідати державним стандартам. Найкращий приклад цього – «Арабська весна». Незважаючи на заборону соціальних мереж та зовнішніх сайтів ЗМІ, громадяни Тунісу,

Єгипту, Лівії, Ємену, Сирії та Бахрейну змогли використовувати заборонені сайти для організації протестних рухів, розповсюдження цензурованої інформації та врешті-решт змінити багато з правлячих режимів у цих країнах.

З огляду на характер громадянського суспільства в ліберальних демократіях, непевно, що кіберкордони також можуть бути політично керованими. У деяких суспільствах свобода слова витісняє питання кібербезпеки всередині політики. Для цих країн кіберкордони не є політично керованими. Крім того, демократичний процес у багатьох країнах часто перешкоджає формуванню політичного консенсусу, необхідного для прискорення нової кіберполітики. Швидкість технологічного розвитку, порівняно зі швидкістю формування політики, також надзвичайно ускладнює урядам формування адекватного законодавства щодо IT-технологій.

Як зазначалось, можливі віруси на зразок Stuxnet стали поштовхом для розробки кібервестфальської моделі. Але чи відповідає Stuxnet характеристиці Демчака та Домбровського як каталізатора для нової парадигми Інтернет? Stutnex був великим, щільно закодованим комп'ютерним вірусом, розробленим спеціально для атаки механізмів синхронізації уранової центрифуги на іранському ядерному об'єкті. Вірус розмножився і поширився по цільовій системі, використовуючи експлойт нульового дня, дуже рідкісний і небезпечний код. Шкідливе програмне забезпечення з відповідною назвою «нульовий день» – це типи згубного кодування, раніше невідомі в кіберпросторі. Воно унікальне за кодом і структурою, а отже, може бути не виявленим і не знищеним. Нульові дні користуються перевагами вразливостей програмного забезпечення свого хоста, які невідомі розробнику програмного забезпечення на момент вторгнення. Не маючи оборонних перешкод для протистояння та жодної можливості виявлення, експлойт поширюється дуже швидко, роблячи стримування надзвичайно складним, а то й неможливим. Перший експлойт Stuxnet за нульовий день поширився на інші розділи систем центрифуг через заражені USB-накопичувачі, введені в систему працівниками установи [499].

Цей експлойт був необхідним, оскільки різні ділянки системи центрифуг, як і багато інших високозахищених систем з катастрофічним потенціалом, не були пов’язані ані між собою, ані з кіберпростором.

Варто зазначити, що сьогодні основна місія кодування вірусу Stuxnet по суті мертва. У нього була одна конкретна мета, і ця мета була досягнута. Хоча залишковий ефект від Stuxnet відчували системи у віртуальному просторі ще деякий час, закодовані команди мали б лише передбачуваний вплив на іранську центрифугу. Після виявлення та деконструкції вірусу фірми з кіберзахисту змогли позначити його специфічні характеристики, що дозволило більшості програм безпеки та брандмауерів виявити та заблокувати вірус. З тих пір весь код Stuxnet є відкритим, проте побоювання, що певний міжнародний актор може застосувати ті самі або подібні методи, знайдені в Stuxnet, все ще залишається.

З досвіду Stuxnet можна зробити висновок, що кіберкордони будуть неефективними проти такої складної загрози нульового дня. Вірус показав, що для проникнення в безпечні, закриті системи зв’язок не потрібен. Зрештою, успіх вірусу залежав від інформації, зібраної для його створення та впровадження. Реально припустити, що розповсюдження такої кіберзброї могло б так само легко розповсюджуватися в національному кібердомені.

Тому хоча кібервестфальська теорія дійсно підходить до загроз кібербезпеки з технічної точки зору, вона не враховує міжнародну кібердинаміку, а також соціальні та політичні норми людей. І тому ми знов повертаємось до необхідності використання інтегрованого підходу до забезпечення кібербезпеки, який би об’єднав кращі аспекти всіх розглянутих вище теоретичних підходів. Інтегровану теоретико-методологічну модель розробки національної стратегії кібербезпеки, що пропонується, наведено на рис. 5.5.

Відповідно до запропонованої моделі актори у кіберпросторі (державні актори, недержавні актори, кінцеві користувачі та кіберзлочинці) здійснюють дії (проводять політику, слідують політиці, атакують, захищаються від

нападів, отримують і передають інформацію, здійснюють комунікацію, використовують ІКТ для роботи й у побуті тощо), які перетинаються з різними аспектами кіберпростору та кібербезпеки (політичними, соціальними, культурними, технологічними) та породжують явища кібербезпеки, такі як вразливості, цілісність системи, шкідлива поведінка, ідентичність, мотивація тощо.

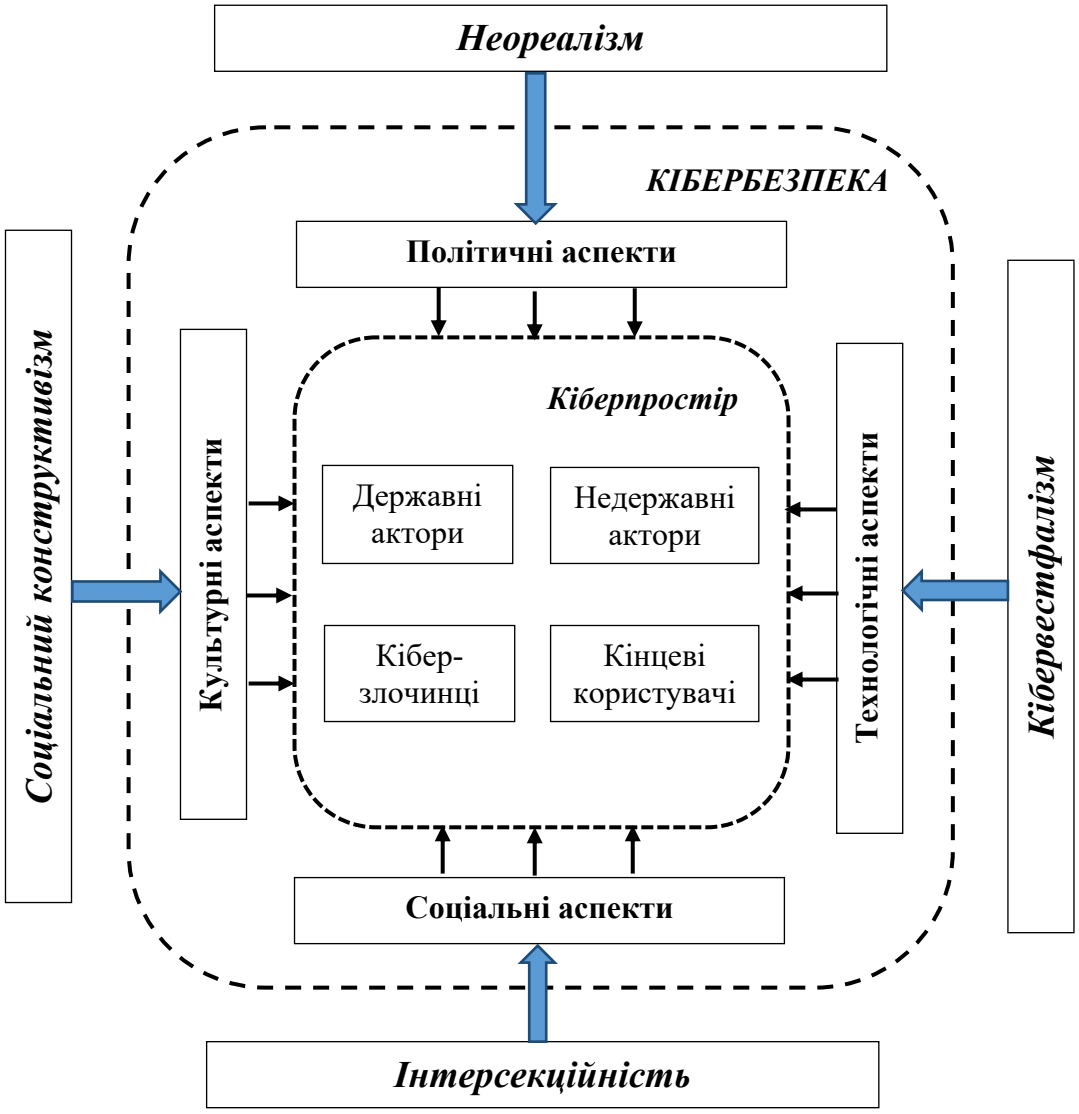

Рис. 5.5. Теоретико-методологічна модель розробки національної стратегії кібербезпеки

Державні та недержавні актори, конкуренція за відносні вигоди та

політичні аспекти кібербезпеки вимагають неореалістичного підходу до її забезпечення і формулювання відповідних положень стратегії кібербезпеки. У той же час, інтерсекційність дозволяє врахувати у стратегії кібербезпеки соціальні аспекти, зокрема, такі як рівність і справедливість у кіберпросторі, адже ці фактори часто становлять причини злочинної групової поведінки у кіберсередовищі. Кінцеві користувачі, кіберзлочинці та їх поведінка є продуктом їхньої ідентичності як представників певного національного культурного середовища, так і користувачів Інтернет. Врахувати культурні аспекти кібербезпеки допоможе соціальний конструктивізм. Нарешті, кібервестфалізм дозволяє врахувати у стратегії кібербезпеки сучасні технологічні аспекти та їхній вплив на інші аспекти кіберпростору та кібербезпеки.

Таким чином, запропонована модель створює теоретико-методологічну основу для розробки національної стратегії кібербезпеки, що враховує різні її аспекти. Проте для забезпечення дієвості та ефективності даної стратегії необхідно розглянути кіберпростір не лише з точки зору наявних у ньому акторів, як це зроблено у запропонованій моделі, а ще і як своєрідний домен влади, здатний впливати на різні сфери суспільної життєдіяльності. Дане питання розглядається у наступному параграфі.

5.3. Побудова та урахування різних типів владних відносин у політиці та стратегіях забезпечення кібербезпеки

Можливості, які надає кіберпростір, є такими, що навіть найбільш медіа-репресивні режими розглядають його використання як вигідне для їхнього політичного режиму. У той же час демократичні держави хочуть за допомогою кіберпростору забезпечувати участь громадян і соціально-економічне зростання, водночас покращуючи власне стратегічне становище.

Це завдання реалізується через відповідні стратегії, у тому числі

стратегію кібербезпеки, яка охоплює як захист державних інтересів у кіберпросторі, так і проведення більш широкої безпекової політики шляхом використання багатьох можливостей, які пропонує кіберпростір. Отже, зі стратегічної точки зору кібербезпека реагує на захист національних інтересів та активно реалізує ці інтереси, а кіберпростір сприймається як середовище загроз та можливостей, в якому держава повинна діяти задля власного збереження та досягнення власних цілей. Крім того, кіберпростір проблематизується як місце і як джерело небезпеки. У цьому сенсі логічно з точки зору держави, що кіберпростір вимагає регулювання та втручання, також за допомоги відповідної стратегії.

Як випливає з попередньо викладеного, кіберпростір можна розглядати як суму двох компонентів. Перший – це фізичний субстрат кіберпростору: комп'ютери та мережі, в які вони зібрані та через які вони «спілкуються». Другий – це комунікації, яким сприяє цей фізичний рівень: мережева, цифрова діяльність, що включає вміст і дії, які здійснюються через цифрові мережі. Обмін інформацією залежить від існування фізичного рівня, який апріорі необхідний для існування кіберпростору. Кіберпростір є як фактичним, так і віртуальним, у тому сенсі, що кіберпростір є частково віртуальним середовищем, що ґрунтується на суттєвості фізичних систем.

Інформація, якою обмінюються та на яку реагують, може бути далі розмежована на синтаксичний та семантичний рівень. Синтаксичний рівень – це місце, де комп'ютери взаємодіють між собою, і містить домовленості, за якими вони це роблять, такі як протоколи TCP / IP, які керують маршрутизацією інтернет-трафіку. Семантичний рівень – це той, де інформація створюється, зберігається та маніпулюється акторами для соціальних, економічних та політичних цілей. В основному саме цей семантичний рівень можна назвати цифровою діяльністю. Отже, кіберпростір є середовищем як технологічної, так і соціальної дії, хоча сам по собі не є інфраструктурою. Тому безпека кіберпростору (кібербезпека) повинна функціонувати як у технологічному, так і в соціальному вимірах.

Що важливо для публічної політики, кіберпростір часто розглядається не лише як сукупність людської та машинної діяльності. Наприклад, NSS 2009 говорить про «низку фізичних та технологічних середовищ, таких як суша, море та космос, які ми можемо охарактеризувати як домени. ...Кіберпростір є одним із таких доменів» [265, с.103-104.]. Це, зокрема, передбачає розширення традиційної концепції військового домену від геопросторового до когнітивного та технологічного. Крім того, NSS 2009 називає кіберпростір «найважливішим новим доменом національної безпеки останніх років». Він тісно пов'язаний з іншим із нових визнаних у NSS 2009 доменів – «громадською думкою, культурою та інформацією», що становить інформаційний вимір інших сфер діяльності національної безпеки. Подібна позиція визначена у військовій доктрині США, яка описує кіберпростір як «глобальний домен в інформаційному середовищі» [там само].

Таким чином, як стратегічна сфера, кіберпростір також повинен бути доменом влади. «Домен» слід розуміти як у просторовому розумінні – кіберпростір настільки фізичний, скільки і віртуальний, але також і у вужчому розумінні – як колективність соціальних суб'єктів, які зазнають впливу певної форми влади. У міжнародних відносинах відповідними суб'єктами є держави, і деякі консервативні автори з ентузіазмом розглядають можливості, що надаються державам, здійснювати владу в кіберпросторі, як правило, за допомогою застосування військової сили. Подібним чином ліберальні інституціоналісти відзначають, що кіберпростір (і інформація в цілому) пропонує значні можливості для реалізації національних інтересів через багатосторонні інституції в глобалізованому світі.

Не існує єдиного всеохоплюючого визначення влади, але ми впевнені, що недостатньо обмежитися переважаючим трактуванням влади як сили примусу, якою володіє один суб'єкт над іншим. Тому для цілей нашого дослідження ми використовуватиме чотиристоронню типологію, запропоновану Барнеттом і Дюваллом у їхній статті 2005 року «Влада в

міжнародних відносинах» [240].

Барнетт і Дювал визначають владу як «виробництво, в соціальних відносинах та через них, наслідків, що формують можливості суб'єктів визначати їх обставини та долю» [240, с. 42]. Вони стверджують, що в основі концепції влади є два «виміри». Перший вимір - це види соціальних відносин, за допомогою яких впливає (та реалізується) спроможність суб'єктів, а другий вимір – специфіка цих соціальних відносин. Перший вимір відрізняється тим, як виражається влада: або через взаємодію між соціальними суб'єктами, або через регуляторні соціальні відносини. Коли влада діє через дії попередньо створених соціальних суб'єктів щодо інших, це приблизно можна порівняти з «владою над» цими іншими соціальними суб'єктами. Як зазначають автори, влада майже стає атрибутом, яким володіє актор, і який може свідомо використовуватися як ресурс для формування дій інших акторів. У другому випадку влада функціонує через соціальні відносини, які передують соціальним або суб'єктним позиціям суб'єктів і які створюють їх як соціальних суб'єктів зі своїми можливостями та інтересами. Іншими словами, актори не володіють внутрішньою владою в силу своїх властивостей, а лише відчувають владу завдяки соціальним відносинам у соціальних структурах. Соціальні відносини визначають, хто є актором і які можливості вони мають для здійснення соціальних практик, аналогічно акторові, який має «силу» формувати умови свого власного існування.

Другий вимір влади стосується специфіки соціальних відносин влади, будь то прямі та безпосередні, або опосередковані та дифузні. Прямі соціальні відносини виникають між суб'єктами, які перебувають у фізичній, історичній чи соціальній позиційній близькості. Прямі відносини між суб'єктами є помітними, і що відносини є «механістичними, контактними, прямими, або логічно необхідними» [240, с. 46]. Прямі відносини не виключаються труднощами емпіричного встановлення відносин між суб'єктами, і принцип логічної необхідності є кращою умовою для їх встановлення. На відміну від цього, коли соціальні відносини є непрямими

або дифузними, влада діє через опосередковані зв'язки і активна навіть тоді, коли діючі особи соціально, тимчасово або фізично віддалені.

Перехресним зіставленням цих чотирьох категорій влади Барнет і Дювал створюють просту таксономію (рис. 5.6). Кожна клітинка квадранта представляє концептуальний тип, для кожної з яких як наведено приклад теоретичного підґрунтя, що робить наголос на тому чи іншому типі влади:

		Специфіка соціальних відносин	
		Прямі	*Опосередковані*
Вираження влади	*Через взаємодію між соціальними суб'єктами*	**Примусова влада** (напр., реалізм)	**Інституційна влада** (напр., неолібералізм)
	Через регуляторні соціальні відносини	**Структурна влада** (напр., марксизм)	**Продуктивна влада** (напр., постструктуралізм)

Рис. 5.6. Типологія влади за Барнетом і Дювалом.

Примусова влада діє через безпосередній контроль одного суб'єкта над умовами існування та поведінкою іншого. Інституційна влада виявляється у непрямому контролі актора над умовами існування соціально віддалених інших суб'єктів. Структурна влада діє через прямі регуляторні соціальні відносини. Продуктивна влада виявляється через опосередковані регуляторні соціальні відносини.

Хоча дана типологія представлена в контексті теорії міжнародних відносин, однак її цілком можна використовувати і стосовно кібербезпеки, яка стосується національної безпеки та відносин між державами та відносин цілого ряду соціальних суб'єктів. Тому нижче розглянемо кібербезпеку в кожній з чотирьох категорій влади, визнаючи, що вони не обов'язково взаємовиключні. З цієї точки зору примусова влада стосовно кібербезпеки надає можливості для безпосереднього контролю одного актора з боку

іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кібербезпекою.

Примусова влада.

Примусова влада визначається як «діапазон відносин між суб'єктами, що дозволяють одному безпосередньо формувати обставини чи дії іншого» [240, с. 49.]. Здійснення примусової влади безпосередньо впливає як на екзистенційні умови інших суб'єктів, так і на їх можливості для самостійних дій. Можливо, не дивно, що саме така форма влади найбільше перегукується з політичним реалізмом, хоча було б неправильним стверджувати, що реалізм має єдину претензію на теоретичне обґрунтування чи здійснення примусової влади. У різноманітних течіях реалістичної теорії держава є головним референтом для політичних дій, і вона діє у власних інтересах, виключаючи всі інші інтереси. Хоча подібна точка зору апріорі не є неправильною, вона зайнята визначенням безпеки з точки зору національних інтересів і ґрунтується на логіці збройних загроз та військових реакцій. А у подібних дослідженнях політики та безпеки аналіз влади найчастіше перекошений у бік наймогутніших держав та здійснення військової сили для досягнення їх національних інтересів. Наприклад, важко обговорювати проблеми безпеки будь-якої країни без посилання на якийсь момент на Сполучені Штати, гегемонічний статус яких забезпечує центральне місце в західному (та і глобальному) дискурсі безпеки.

Звичайно, держава не повинна бути єдиним референтним об'єктом безпеки. Є багато інших суб'єктів, починаючи від окремих людей, соціальних груп та рухів, закінчуючи суспільствами і цивілізаціями, або навіть людством чи біосферою. Можливо, через труднощі приписування фіксованості сутностей на мікро- та макро-кінцях цього спектра, «обмежені

колективні угруповання» середнього рівня, такі як держава та нація, зберігаються як домінуючі референтні об’єкти в дослідженнях безпеки. Хоча у багатьох стратегіях кібербезпеки приділяється багато уваги безпеці людей, але зазвичай держава залишається головним референтом для всіх форм безпеки в урядовому дискурсі. Наприклад, у кібербезпеці Великобританії безпека держави нерозривно пов’язана зі здоров’ям національної економіки, і вони пов’язані між собою як ті, що мають бути забезпечені за допомогою заходів кібербезпеки [266]. Це слідує переважаючому реалістичному погляду, що економічне процвітання є як передумовою національної безпеки, так і засобом здійснення впливу на неї. Також часто приділяється увага забезпеченню належного управління та державних послуг, хоча вони в значній мірі залежать від національної безпеки та економічного добробуту.

Стратегія кібербезпеки є частиною національної стратегії безпеки, і тому слід очікувати, що за необхідності держава використає свої безпекові можливості для захисту держави від супротивників у кіберпросторі. Ці дії повинні включати можливість «втручатися проти супротивників», і саме цей компонент кібербезпеки ми розглянемо як форму примусової влади.

Можна визначити п’ять категорій супротивника або суб’єкта загрози у кіберпросторі: держави, державні довірені особи, злочинці, терористи та «інсайдери». Можливість втрутитися проти цих суб’єктів загрози є функцією наявної розвідки та можливостей для підтримки політики безпеки. Втручання – це більше, ніж просто здатність реагувати на певні події або відповідати на них, це здатність ініціювати наступальні або превентивні операції проти супротивників у кіберпросторі. Це означає використання підходу «активна оборона», якій на даний час приділяється значна увага в контексті кібербезпеки як оборонних, так і промислових спільнот, і яка передбачає прийнятне пом’якшення загроз шляхом автоматичної або ручної відповіді проти їх джерел. Успіх такої відповіді залежить від можливості ідентифікувати зловмисників та охарактеризувати їх наміри, а також від можливості поважати нейтралітет третіх сторін, на яких можуть ненавмисно

вплинути контрзаходи.

Отже, втручання призначені для здійснення контролю над іншими суб'єктами, намагаючись безпосередньо змінити їхню поведінку та обставини. Може виникнути очевидна критику, яка випливає з нашого нинішнього твердження, що ці форми втручання є «прямими»: чи не здійснюється ця діяльність також на відстані, особливо з огляду на місце розташування суб'єктів за межами суверенної території певної держави? Відповідь – «ні», оскільки йдеться про віртуальний простір. Просторова відстань фактично знижується через швидкість електронного зв'язку, яка має майже світлову швидкість, і це має наслідки для характеру контакту між суб'єктами в кіберпросторі. Одночасність причинно-наслідкових наслідків у кіберпросторі є однією з причин, чому держави вважають її настільки небезпечною: дії, розпочаті в одному місці, можуть мати миттєві наслідки в іншому, незалежно від їх географічного розташування. Прямий контроль над віддаленими комп'ютерами безпосередньо змінює діапазон опцій, доступних для певного актора, він також може змінити умови існування таким чином, що актори більше не перебуватимуть в Інтернеті та взагалі не зможуть працювати в кіберпросторі.

Примусова влада не повинна залежати від навмисності дій та існує, навіть якщо винуватець негативної дії не знає про наслідки, які це може мати для інших. Як приклад можна згадати дії США проти джихадистського веб-форуму, який, як згодом стало відомо, був активом Центрального розвідувального управління (ЦРУ) [472]. Стурбований можливою роллю форуму в сприянні іракському повстанню, Пентагон та Агентство національної безпеки (АНБ) закрили форум у 2008 році нерозкритими операціями комп'ютерних мереж. Незважаючи на те, що сайт вважався створеним і підтримуваним ЦРУ, і що закриття вплинуло на можливості збору розвідданих ЦРУ, американські дії також завдали додаткової шкоди понад 300 стороннім серверам в Саудівській Аравії, Німеччині та США. Мимоволі, американський персонал у Форт-Мід, штат Меріленд, здійснював

безпосередній контроль над можливістю користувачів Інтернет в Північній Америці, Європі та Аравійському півострові отримувати доступ до ресурсів та контролювати власні дії в Інтернеті.

Стратегія кібербезпеки має, на наш погляд, обов'язково містити елементи примусової влади для того, щоб розвинути більші можливості для здійснення безпосереднього контролю над діями суб'єктів, які є шкідливими для національних інтересів. Ця форма примусової влади включає типи активних оборонних та наступальних дій, які згадувались вище, але може також включати розгортання нематеріальних ресурсів, таких як правові та нормативні режими, з метою безпосереднього впливу на дії інших. Символічні ресурси, такі як загроза воєнних дій, також слід розглядати як негативну санкцію, доступну державі в цій категорії, і тісно пов'язані із стримуючими та примусовими ефектами, сильно вираженими в прагненні зменшити мотивацію та спроможність противника.

Проте слід враховувати, що здійснення влади в режимі стримування, орієнтованого на актора (а не на вектор загрози), відрізнятиметься спробами стримувати державних та недержавних суб'єктів, не в останню чергу через проблеми ідентифікації та атрибуції в кіберпросторі. Необхідно також, щоб потенційні та відомі супротивники знали, що проти них було створено ресурси, і вважали, що загроза проти них достовірна.

Як зазначалось, кіберпростір через свої характеристики є середовищем, яке сприяє діям агресора. У поєднанні зі значною здатністю зникати після нападу це ускладнює стримування супротивників за допомогою традиційних застосувань контролю та примусу. тому доцільно, щоб примусова влада діяла тут також через вплив на процеси прийняття рішень ряду супротивників, навіть вилучаючи їх із мереж, якщо це можливо.

Інституційна влада.

Очевидно, що державам не завжди можливо безпосередньо контролювати суб'єктів як таких – повинні бути посередники, за допомогою яких можна здійснювати владу та отримувати результати. Отже, держава

повинна діяти через цих агентів, щоб контролювати дії та можливості інших. Це форма непрямої дії, роз'єднання між акторами, що створює «соціальну дистанцію», яка може діяти як у просторовому, так і в часовому аспектах. Подібне спричиняє чітку артикуляцію влади, коли держава та супротивник є соціально віддаленими, але пов'язаними через посередницьку установу, яка може або не може бути повністю під контролем держави. Тобто інституційну владу можна у даному разі визначити як вплив на суб'єктів, які працюють за визначеними для них правилами та процедурами, що направляють, керують та обмежують дії (або бездіяльність) та умови існування соціально віддалених інших суб'єктів.

У випадку установ, над якими домінуючий суб'єкт здійснює повний контроль, ці правила та процедури можуть розглядатися як інструменти примусової влади. Там, де це не так, або коли кілька суб'єктів здійснюють контроль над даними інструментами, існує певна форма інституційної влади. Іноді, наприклад, щодо відносин між урядом та спецслужбами, може бути важко зробити висновок, чи є ці правила та процедури інструментами примусової влади чи вони обумовлюють інституційну владу. Однак ми вважаємо, що більшість із цих установ законодавчо пов'язані з державою і діють суворо за її розпорядженням, і тому їх слід розглядати в режимі примусової влади, навіть якщо їм надається оперативна широта самостійних дій.

Однак, оскільки кібербезпека – це не лише питання захисту національних активів від загроз, це також не лише відповідальність військових, розвідки чи правоохоронних органів. Уряд, організації всіх секторів, громадськість та міжнародні партнери також мають свою роль у забезпеченні кібербезпеки. Тому у контексті інституційної влади необхідно розробляти та реалізовувати програми, що спрямовані на впровадження змін у поведінці та робочій культурі, які вимагає наша залежність від кіберсередовища, насамперед у публічному секторі.

Однією із специфічних сфер, в якій зміна культури сприймається як

необхідна, є захист інформації. У цьому також ми бачимо функціонування інституційної влади через посередників, завданням яких є частково змінити поведінку не тільки техніків та фахівців з інформаційної безпеки, але й державних службовців та компаній щодо забезпечення безпечного проходження та зберігання економічно та політично конфіденційних дані. Це випливає із власне сенсу захисту інформації, який у даному разі слід розуміти, як впевненість, що інформаційні системи захищатимуть інформацію, яку вони несуть, і функціонуватимуть, як їм потрібно, коли це потрібно, під контролем законних користувачів [527].

У багатьох країнах існує цілий ряд організацій (з різних секторів), які співпрацюють з урядом з питань забезпечення кібербезпеки. Усі ці організації беруть участь у практиках, які можна інтерпретувати як форми інституційної влади. Тому національна стратегія кібербезпеки має реалізовуватись широким колом представників органів публічної влади, служб безпеки, бізнесу та громадянського суспільства, спрямованих на технічне вдосконалення та зміну робочої поведінки та культури. Уряд не міг би досягти своїх цілей у цій галузі без цих організацій, які мають різну ступінь незалежності від уряду, але залишаються відповідальними за досягнення результатів, визначених ними спільно.

Крім того, згідно з визначенням інституціональної влади, уряд має працювати, щоб спрямовувати та обмежувати діяльність цих організацій з тим, щоб вони здійснювали зміни у діях та поведінці різних суб’єктів, таким чином, що вони забезпечують покращене інформаційне забезпечення як основу економічного добробуту та національної безпеки. Упередженість та власні інтереси цих організацій будуть додатково модулювати динаміку формування та реалізації політики кібербезпеки. Конкуренція у сфері послуг, що стосуються кіберпростору, також може бути суттєвим фактором формування організаційних результатів.

Інституційна влада діє через взаємодію конкретних суб’єктів у дифузній мережі соціальних відносин, де більшість акторів не є державними

службовцями які, як правило, несуть відповідальність за безпеку. Швидше, вони потрапляють у систему безпеки через твердження, що обов'язок та відповідальність усіх працівників усіх організацій – вдосконалити інформаційне забезпечення як необхідну умову національної та економічної безпеки. Уряд не може досягти цього лише через діяльність виконавчих органів чи законодавством, а повинен діяти через інституційних посередників, використовуючи владу для того, щоб спричинити поведінкові зміни у соціальних суб'єктів та технічні вдосконалення в системах, над якими люди все ще здійснюють головний контроль.

Структурна влада.

На відміну від інституційної влади, яка спирається на існуючі соціальні відносини, структурна влада стосується того, як взаємно створюються відносини між суб'єктами. Структури, в цьому сенсі, є співконститутивними, внутрішніми відносинами структурних позицій, класичним прикладом яких є, наприклад, відносини господар-раб і капітал-праця, в яких «соціальні відносини, суб'єктивність та інтереси суб'єктів безпосередньо формуються із зайнятих ними соціальних позицій» [240, с. 52-53]. Важливо, що структурна влада може замаскувати визнання акторами своїх структурних позицій по відношенню до інших, так що вони стануть готовими «прийняти свою роль у існуючому порядку речей» [там само, с. 53]. Таким чином, структурна влада може формувати поведінку та можливості, навіть коли даний суб'єкт не активно прагне здійснювати контроль над іншим прямими (примусовими) або опосередкованими (інституційними) засобами.

У кібербезпеці більшості сучасних держав дифузна структурна сила пронизує соціальні відносини. Одним із прикладів є взаємозв'язок між урядом та промисловістю, який відтворюється та модифікується заборонами політики кібербезпеки та практикою, яку вона пропагує. Зараз звичним є те, що в умовах ринкової економіки переважна частка критично важливих інфраструктур, на які покладається національна безпека та економічне здоров'я, насправді належить приватному сектору та управляється ним.

Історично це є результатом дерегуляції та приватизації державного сектору, які передали націоналізовані галузі в руки приватних компаній та їх акціонерів. Ситуація ускладняється глобалізацією капіталу таким чином, що критично важлива інфраструктура в одній країні може контролюватися або належати компанії в іншій, а на неї впливають відмови в третій. Це створює численні проблеми для урядів. По-перше, уряд не може забезпечити безпеку критично важливих інфраструктур самостійно. По-друге, уряд повинен знайти способи стимулювання приватного сектору забезпечити цю безпеку. По-третє, уряд повинен збалансувати переваги можливого втручання в критично важливу інфраструктуру та її дефіцит, особливо в умовах, що не допускають регулювання. По-четверте, уряду, можливо, доведеться покладатися на галузеві навички та досвід для захисту державних мереж, оскільки надання та обслуговування ІКТ, як правило, передається в приватний сектор.

Найкращим рішенням у такій ситуації стає публічно-приватне партнерство (ППП), в рамках якого публічний та приватний сектор працюють у партнерстві для досягнення стратегічних результатів. Результатами такого партнерства може бути обмін розвідданими, плани безперервності бізнесу, регуляторні питання, взаємні поради, навички та досвід, спільні стратегії дій, дослідження та розробки, інновації та інвестиції, управління ризиками, найкращі практики тощо.

ППП можуть приймати різні форми, але ми пропонуємо використати типологію, розроблену Ліндером, для розгляду ППП [398]. Типологія Ліндера передбачає, що кожне різне використання ППП як поняття «посилається на певні передумови щодо того, які відповідні проблеми слід вирішити та як само їх вирішити» [там само, с. 42]. Ми розглянемо тут чотири з них, щоб розрізнити структурну силу, що діє в цих відносинах.

Перший тип ППП стосується «реформи управління». Основна передумова полягає в тому, що менеджмент та робочі практики приватного сектору можуть використовуватися органами влади для забезпечення

підвищення ефективності. Передача знань є фактично односторонньою, оскільки публічні управлінці отримують вигоди від навичок та досвіду приватного сектору, а не навпаки. Колишній керівник GCHQ Девід Пеппер описав, як для того, щоб впоратись із мінливим операційним середовищем глобальних ІКТ, його організація консультувалась із експертами приватного сектору для перегляду своєї практики управління та роботи [446]. Це дало змогу розробляти та керувати постійною інвестиційною програмою уряду в інфраструктуру ІКТ. Пеппер також відзначає прийняття стандартів управління галузевими технологічними послугами.

Другий тип ППП стосується «перетворення проблем», при якому публічні управлінці прагнуть комерціалізувати проблеми, щоб залучити для їх вирішення приватний сектор, його знання та капітал. В даному разі приватний капітал розглядається як інструмент вирішення низки проблем кібербезпеки, а роль уряду полягає в розвитку даного ринку шляхом стимулювання досліджень, розробок та реалізації проектів кібербезпеки на підтримку цілей національної економіки та безпеки. Інновації тут стають основним напрямом державної політики у сфері кібербезпеки. Одним з прикладів є Інноваційна платформа мережевої безпеки (NSIP), розроблена у Великобританії, яка в даний час зосереджена на управлінні інформаційними ризиками.

Перетворення проблем тісно пов’язане з третім типом ППП, в якому уряд розглядає ППП як можливість для «перенесення ризиків». Різниця полягає у відносній ролі уряду та промисловості. При перетворенні проблем урядові функції перетворюються на приватні, при цьому уряд виконує підпорядковану роль ринковим можливостям. Переносячи ризик, уряд спонукає приватний сектор до допоміжної ролі, зокрема, щоб накласти на проекти у сфері кібербезпеки фіскальні обмеження та забезпечити їх фінансову життєздатність. На цій ранній стадії на відносно новому ринку та при нестачі наявних даних важко розрізнити ці дві форми ППП, хоча сучасний економічний клімат може свідчити про те, що перенесення ризику

стає більш поширеним, можливо, як попередник приватизації функцій кібербезпеки.

Четвертий тип ППП зумовлений бажанням заохотити «моральну регенерацію» за допомогою «ринкових рис характеру», таких як ініціативність, наполеглива праця, чесність, розсудливість тощо. Ми не змогли знайти явної згадки про такі риси в поточній політиці кібербезпеки розглянутих у попередніх розділах країн, але подібне партнерство є важливим, на нашу думку, й у даній сфері, оскільки воно дає можливість виявити талановитих людей, здатних стати частиною професійного середовища в галузі кібербезпеки через низку відкритих заходів та конкурсів. Подібні заходи і конкурси можуть спільно організовуватись і фінансуватись органами влади та приватним сектором. Яскравим прикладом такого партнерства є програма USCC (United States Cyber Challenge). USCC має помітний громадянський елемент, прагнучи знайти людей та розмістити їх в організаціях, де їхні навички можуть мати найбільшу цінність для нації. На домашній сторінці USCC сказано: «Будь наступним найкращим інструментом кібербезпеки. ... Допоможи США перемогти поганих хлопців. Захищай, виживай, перемагай» [502]. У публічних заявах USCC часто використовується такий вислів: «Йдеться про вирощування наступного покоління кібервоїнів для захисту нації» [там само].

На даний час і в багатьох інших країнах приватний сектор залучається урядом для надання певних форм навичок, знань та капіталу, що підтримують цілі державної економічної та національної безпеки. Уряд використовує ринкову логіку, щоб використовувати організації приватного сектора як своїх партнерів з кібербезпеки, з різним рівнем рівності. Відносини між публічними та приватними партнерами певним чином обмежують їхні дії, проте дають можливість для саморозуміння та досягнення інтересів інших. Наприклад, з точки зору приватного сектора, кібербезпеку можна вважати зростаючою сферою, в якій слід шукати прибуток, хоча дії, які вони заохочують або дозволяють здійснювати, у

більшості обставин вирішуються урядом.

У цілому, ринкова логіка та імператив національної безпеки тісно переплітаються, стимулюючи приватний сектор для надання знань, персоналу та фінансових інвестицій для здійснення функцій національної безпеки в обмін на прибуток. Докладніше ППП розглядається у параграфі 5.4.

Продуктивна влада.

Продуктивна влада стосується «систем виявлення та визначення мереж соціальних сил, що постійно формують одна одну» [240, с. 55]. У той час як структурна влада працює через бінарні відносини, які служать для розширення можливостей тих, хто має структурні переваги, та позбавлення можливостей тих, хто таких переваг не має, продуктивна влада пов’язана з дифузними та непередбачуваними соціальними процесами, які виробляють певні види суб’єктів, фіксованими значеннями та категоріями, та створює те, що береться як само собою зрозуміле і звичайне у світовій політиці [там само, с. 57]. Дискурс, а не структура, створює ідентичність та спроможність соціальних суб’єктів.

Із зростаючою залежністю від ІКТ також виникає більша кількість нових загроз і ризиків. Так, існують технічні проблеми, такі як системні помилки, властиві технологічним системам, які, можливо, спричиняють каскадні збої в інших системах через їх взаємозв’язок та взаємозалежність. Існують також соціальні загрози та ризики, які походять від людських акторів, які бажають завдати шкоди як самим фізичним системам, так і тим практикам та процесам, які залежать від них. Отже, технічне та соціальне глибоко переплітаються, але у стратегії кібербезпеки, на наш погляд, слід надавати соціальним агентам пріоритет над технічними аспектами, хоча не завжди приписувати людську діяльність як причину «розладу» інфраструктури.

Цього можна очікувати: в той час як захисні заходи, такі як інформаційна безпека та управлінські процеси, такі як забезпечення

інформації, є давно встановленою оперативною практикою, характер та еволюція образливих загроз державним інтересам, зрозуміло, представляють більший інтерес для стратегічних планувальників, які мислять не лише у категоріях безпосередньої підтримки цілісності мереж та інформації. Адже дуже важливим є виявлення потенційних або фактичних зловмисників для розробки загальних та спеціальних контрзаходів. Їх можна розуміти як акторів, що діють на місцях, акторів, які впливають на динаміку даної сфери, як функціональних суб'єктів. Функціональний суб'єкт – це той, хто суттєво впливає на рішення у сфері безпеки, але насправді не відповідає за формулювання політики безпеки. Крім того, функціональних суб'єктів можна розрізнити на «внутрішніх», тих, хто є частиною спільнот, що формують безпекову політику, та «зовнішніх» суб'єктів, які повністю розташовані за межами цих спільнот. У цьому сенсі можна визначити чотири типи зовнішніх функціональних суб'єктів, які вже згадувались вище: держави, державні довірені особи, злочинці, терористи. П'ята категорія, інсайдери, стирає різницю між внутрішніми та зовнішніми суб'єктами. Розглянемо ці суб'єкти докладніше.

Відомо, що понад 140 країн розвивають можливості для кібернаступальних дій, і ця кількість, ймовірно, буде зростати в найближчі роки. знаходиться на першому рівні серед таких держав, поряд з США, Великобританія, Франція, Китай, Ізраїль, Росія. Другий рівень активних держав включає такі країни, як Північна Корея та Іран. Наприклад, Генеральний директор Служби безпеки Великобританії заявив у Комітеті з питань розвідки і безпеки в січні 2010 року, що «немає сумнівів, що Інтернет є сильним вектором загрози, що стосується шпигунства», і двічі визначив Китай як значну загрозу [362, с.11]. Загальне занепокоєння з цього приводу полягає в тому, що держави прагнуть зібрати розвідувальні дані щодо урядових, військових, промислових та економічних цілей та противників своїх режимів. Отже, широкий спектр заходів кібершпигунства спрямований проти державних та недержавних структур, включаючи, як можна

припустити, політичну опозицію у власних національних кордонах.

Держави можуть використовувати ці та подібні методи для розповсюдження дезінформації та зриву нормального функціонування критичних інфраструктур і служб. Це, зокрема, передбачає дії впливу як підмножину інформаційної війни, включаючи пропаганду та політичну диверсію. Держави можуть також встановлювати шкідливе програмне забезпечення на комп'ютерні системи, що активується у часи підвищеної напруженості або конфлікту.

Також слід відзначити такий допоміжний компонент державної діяльності як заохочення «патріотичних хакерів». З огляду на проблеми присвоєння ідентичності та розташування у віртуальному просторі, використання або заохочення державою недержавних суб'єктів може дозволити державам правдоподібно заперечувати свою причетність до наступальних дій проти іноземних цілей. Часто вважається, що Китай, Іран та Росія дотримуються цих форм взаємодії з націоналістичними утвореннями, для реалізації зловмисних кібердій, що зачіпають урядові та промислові активи інших держав. Хоча тут слід визнати, що недержавні суб'єкти не виступають виключно як довірені особи або сурогати держав, і ними не лише безпосередньо чи опосередковано керують державні агенти. «Довірених осіб» так само може легко мотивувати прибуток, як націоналістична чи ідеологічна спорідненість із «спонсорською» державою. У той же час слід розуміти і те, що держави можуть отримати вигоду від недержавних суб'єктів, навіть якщо вони не заохочують їх безпосередньо.

Однією з найбільш поширених загроз для економічної безпеки сучасних держав слід вважати організовану кіберзлочинність, яка за останні десять-двадцять років зросла в геометричній прогресії. Тут можна визначити два основних типи кіберзлочинів. По-перше, «нові злочини, нові засоби» – це злочини, вчинені проти систем ІКТ, які не можуть бути вчинені будь-яким іншим способом або проти будь-якої іншої жертви, такі як хакерські атаки та атаки на відмову в обслуговуванні. По-друге, «старі злочини, нові засоби» –

це усталені види злочинів, які знаходять нове вираження за допомогою ІКТ, включаючи шахрайство, крадіжку особистості, переслідування, відмивання грошей. Боротьба з обидвома цими типами має бути відображеною у стратегії кібербезпеки, з акцентом на другому типі. Тут слід враховувати, що гроші, отримані в результаті цієї діяльності (та інших злочинів) можуть бути відмиті у віртуальному просторі, в тому числі за допомогою використання онлайн-ігор.

Ще однією серйозною проблемою є терористичне використання Інтернету, чому також слід приділити значну увагу в стратегії кібербепеки. Проте, з цього приводу у фахівців існує досить консолідована точка зору, яка полягає у такому. Визнається, що кіберпростір надає додаткові можливості терористичним комунікаціям, координації, пропаганді, залученню коштів, радикалізації та вербуванню. Але при цьому кібертероризм, як пошкодження або підрив критичних інформаційних інфраструктур терористами або використання терористами кіберпростору для негативного впливу на національні критичні інфраструктури, вважається досить низьким ризиком. Фахівці схильні вважати, що терористи продовжуватимуть віддавати перевагу гучним звичайним терактам над кібератаками, але попереджають про пильність щодо майбутніх розробок можливостей у цій галузі. Відсутність будь-яких чітко визначених кібертерористичних актів дотепер є головним чином функцією розриву між терористичними намірами та можливостями, хоча ми не можемо припустити, що це буде так завжди.

«Інсайдерські загрози» вже багато років турбують фахівців з інформаційної безпеки, і ризики, що виникають всередині приватних компаній чи державних структур, продовжують створювати незручні питання для процедур безпеки та перевірки організацій. Фахівці зазначають, що участь інсайдера в будь-якому з різноманітних методів кібератаки, збільшує ймовірність її успіху. Це фактично стирає межу між внутрішніми та зовнішніми функціональними суб’єктами, оскільки інсайдери за своєю природою можуть бути внутрішніми для груп, на яких покладена

відповідальність за кібербезпеку. Крім того, це дає розуміння того, що не всі зовнішні загрози насправді є зовнішніми.

Таким чином, зовнішні суб'єкти кіберзагрози поділяються на державні та недержавні, при цьому держави представляють найскладнішу загрозу. Держави та довірені особи можуть співпрацювати, і може існувати суттєве перетинання між терористами та довіреними особами. Протистояти діяльності цих суб'єктів можливо лише через співпрацю акторів всіх трьох секторів, на чому вже неодноразово наголошувалось, і на чому ґрунтується продуктивна влада.

Вирішальним моментом цієї форми влади є те, що контроль над інформацією свідомо обмежується членами елітних спільнот знань. Дискурс контролюється цими спільнотами для своїх цілей та слугує їхнім власним інтересам, фактично закриваючи дискурсивний простір для тих, хто є зовнішнім для цих спільнот. Такі документи, як стратегії кібербезпеки, можуть відкрито заявляти про свій контроль над інформацією, посилаючись на оперативні причини та причини національної безпеки. А там, де пропонується місце для розбіжностей та дискусій, наприклад, у парламенті, воно використовується лише для запитань механіки кібербезпеки, а не її принципів чи необхідності. Подібне простежувалось, наприклад, в процесі створення Американського кіберкомандування, в ході якого громадський контроль був слабо запроваджений слуханнями в Сенаті [390].

Тобто продуктивна влада працює над побудовою «іншого», тим самим виправдовуючи розширені функціональні можливості та витрати кібербезпеки. Будь-яка емпірична основа для прийняття рішень не повідомляється громадськості і, натомість, залежить від дискурсивної конструкції суб'єктів, приписування значення цим суб'єктам, а також заходів та дій, які пропонуються для боротьби з ними.

5.4. Розвиток публічно-приватного партнерства у галузі кібербезпеки

Сучасні бізнес-конструкції створюють цілі середовища, де публічний і приватний сектор активно та успішно співпрацюють – іноді як клієнт і постачальник, іноді через нагляд і дотримання, іноді як партнери. Ці домовленості зазвичай переслідують спільні цілі отримання певних позитивних результатів, але в деяких випадках партнерські відносини формуються як захисна відповідь спільним противникам. Саме така мета партнерства є головною у сфері забезпечення кібербезпеки. Гівенс [336] стверджує, що значення публічно-приватного партнерства (ППП) у сферах безпеки полягає в «зменшенні дублювання зусиль, посиленні міжгалузевої комунікації, підвищенні ефективності та досягненні цілей захисту краще, ніж у ситуації, коли уряд або бізнес діють незалежно». Коли ці цілі досягнуті, інвестиції в ППП є цінними, життєздатними та змушують учасників продовжувати партнерство і надалі. Якщо ці цілі не досягнуті, учасники можуть втратити віру в домовленості, робити менший внесок, можливо, звинуватити один одного у неефективності та, ймовірно, шукатимуть альтернативні шляхи вирішення своїх потреб у кібербезпеці. На жаль, практика ППП у багатьох країнах, що демонструє негативне ставлення сторін до цих партнерських відносин, а також стабільно високі показники вразливості та експлуатації зловмисними організаціями операцій з комп'ютерними мережами (CNO) свідчать про те, що багато цілей ППП не досягаються повною мірою.

ППП як захисна модель покладається на те, що кожен учасник вносить щось унікальне в партнерство, що може пом'якшити слабкі сторони та посилити сильні сторони. Але у той час як публічний сектор в першу чергу мотивований питаннями національної безпеки, приватний сектор в першу чергу мотивується прибутком. Карр пише, що «саме ця диз'юнктура лежить в основі напруженості у цьому партнерстві» [271, с. 44]. Часто, і підживлюючись цими відмінностями, партнерство захмарюється уявленням

про те, що одна сторона робить недостатній внесок або вносить більше, ніж інша. Це сприйняття дисбалансу у відносинах викликає подальшу напругу. Тому хоча велика увага науковців і практиків приділяється необхідності створення ППП для поліпшення кіберзахисту, необхідними є також дослідження, що стосуються того, чому ці партнерства є неефективними. Зокрема, слід постійно отримувати відповіді на наступні запитання, пов'язані зі зниженням ефективності ППП у кібердоменах:

1. Які існують проблеми в обміні інформацією між партнерами і яким чином це впливає на партнерство у цілому?

2. Чи демонструють члени ППП взаємно вдосконалений кіберзахист в результаті своїх партнерських відносин?

3. Які об'єктивні відмінності впливають на спонукання сторін рухатись до ефективного та взаємовигідного партнерства?

Загроза зловмисних CNO є динамічною та екзистенціальною: вона завжди змінюється та постійно присутня. Протидія загрозі в міру її розвитку вимагає від ключових лідерів та осіб, що приймають рішення в публічному та приватному секторі, запроваджувати ППП як життєздатну оборонну модель, робити адекватний та необхідний внесок у партнерство та постійно вимірювати й оцінювати зміни в кібербезпеці відповідних організацій в результаті ППП. Усі партнерські відносини прагнуть зменшити індивідуальні витрати на спільні завдання та використати загальні дії та заходи членів на свою користь. Однак, щоб досягти ці дві цілі, партнери також повинні справедливо враховувати внески іншою сторони. З цього приводу Ліндер зазначає, що у партнерствах: «Актори з кожного сектору приймають характеристики та точки зору, які колись визначали та стабілізували особистість їхніх колег. ...Публічним суб'єктам потрібно буде думати і поводитись як підприємці, а суб'єктам бізнесу потрібно буде враховувати суспільні інтереси та очікувати більшої підзвітності громадськості» [398, с. 36].

Цей опис відображає значну частину імпульсу, який органи влади

використовують для запровадження та реалізації ППП у багатьох галузях. Ймовірно, найбільш очевидний прояв цих партнерських відносин відбувається стосовно критичної інфраструктури: публічний сектор має вимоги до технологій чи можливостей і платить приватному сектору за створення, інтеграцію чи інше управління цією вимогою. Публічний сектор реінвестує себе в партнерство, коли потім включає готовий продукт або послугу в якісь національні можливості. Але оскільки це стосується кібербезпеки, використання та цілі впровадження моделей партнерства можуть бути дещо складнішими. Тим не менше, Граймен [340] бачить у цих партнерствах великі можливості, зазначаючи, що дедалі більш розподілена та взаємопов'язана природа сучасних технологічних систем повинна створювати більш динамічні партнерські відносини, які швидко розвиваються та йдуть в ногу із загрозами та вразливими місцями.

Втім, не всі дослідники налаштовані оптимістично з цього питання. Наприклад, Карр називає ППП у сфері забезпечення кібербезпеки «однозначно проблематичним» і стверджує, що «небажання політиків претендувати на повноваження держави вводити жорсткіші заходи з кібербезпеки ... поряд із неприязним ставленням приватного сектору до прийняття відповідальності або підзвітності за національну безпеку, залишає партнерство без чітких меж відповідальності та підзвітності» [271, с. 43]. Подібним чином, Грайман [340] стверджує про існування свого роду «кіберпарадоксу», де перетинання між публічним та приватним секторами призвело до переплутування операцій національної безпеки та розвідки з кібербезпекою та конкурентоспроможністю підприємств, викликаючи зіткнення цілей. Звичайно, парадокс полягає в тому, що цілі діяльності обох сторін вимагають отримання певних кіберданих, але жодна зі сторін не хоче, щоб її використовувала для цього інша. Цей парадокс суттєво сприяє виникненню проблем у партнерстві, тому питання «балансу» завжди має посідати у ньому важливе місце. Також важливо постійно наголошувати, що вплив зловмисного CNO є спільним знаменником, необхідним для

об’єднання публічних та приватних організацій для забезпечення їхньої безпеки. До того ж, кожна ітерація з боку публічного сектору має заохочувати приватний сектор розробляти технології, необхідні для посилення кіберзахисту критичної інфраструктури країни, інвестувати в системи виявлення та запобігання і розробляти найкращі практики, необхідні для вимірювання ефективності ППП.

Для ППП, орієнтованих на кібербезпеку, саме ступінь спільних наслідків пов’язує його учасників. Таке призначення зумовлює для публічного сектора необхідність визначити кібербезпеку приватних організацій як проблему національної безпеки, а отже, визнати відповідальність уряду за її забезпечення. Приватний сектор, у свою чергу, створює, управляє та підтримує системи, технології та процеси, що складають критичну інфраструктуру, забезпечення кібербезпеки якої є складовою забезпечення національної безпеки.

Загрози в кіберпросторі вимірюються двома факторами: вони повинні мати намір заподіяти певної шкоди, і вони повинні мати здатність це зробити. Наявність можливостей, але відсутність наміру використовувати їх, по суті, усуває будь-які загрози. Звичайно, намір стосується мотивації зловмисників, того, що рухає їх до якоїсь мети. Мотивація у цій сфері може варіюватися від простого хуліганства, до політичної активності та шпигунства, спрямованого на інші держави. Часто мотивація визначає, наскільки стійкою може бути певна загроза, і якщо її можна з’ясувати, то це може мати певний зв’язок із можливостями, які може використовувати загроза. У широкому розумінні можливості стосуються тактики, техніки та процедур, до яких загроза має доступ і буде використовувати їх для заподіяння шкоди у відповідності до визначеної мети. У суто технічному розумінні можливості щодо кіберзагроз конкретно стосуються експлойтів та шкідливих програм, якими користується загроза. Можливості також можуть містити широкий спектр інструментів - від програм з відкритим кодом до спеціально розроблених шкідливих програм, що надаються державними

спецслужбами. Звичайно, мотивацію можна затуманити, оголошуючи незрозумілі цілі, і багато можливостей можна отримати в Інтернеті, що у сукупності ускладнює виявлення типу загрози. Тим не менше, впевненість у з'ясуванні як умислу, так і передбачуваних для використання можливостей може допомогти у визначенні категорії загрози.

У своєму дослідженні з економіки поліпшення кібербезпеки Мур визначив чотири основні проблеми в кіберпросторі: крадіжка інтернет-ідентифікаційних даних, промислове кібершпигунство, порушення захисту критичної інфраструктури та ботнети [419, с. 4]. Мур пропонує ці категорії не лише як основу для розгортання кібербезпеки, але і як цілі, що спрямовують усі зусилля з кібербезпеки. Накладання цих цілей на ППП ілюструє, що як публічний, так і приватний сектор чутливі до впливу цих проблем, і це має бути достатньою причиною для стимулювання співпраці та більш підзвітного партнерства.

Однак Мур [419, с. 7] також визначає три бар'єри для покращення кібербезпеки, – невідповідні стимули, інформаційні асиметрії та зовнішні ефекти, – які, якщо їх не врахувати належним чином, закладають основу для неминучої неефективності кібербезпеки. У своїй роботі Мур описує «невідповідні стимули» як явища, що виникають в результаті компромісу між безпекою та ефективністю [там само]. Чим складнішою є система безпека або чим більше шарів безпеки вона має, тим менша ефективність буде відчуватися. Так, Мур зазначає, що якби банки не пропонували Інтернет-банкінг, вони були б значно менш схильні до злому. Однак їхні клієнти також мали б менший доступ до своїх грошей, а витрати на управління філіями були б для банку значними. Окремо вимоги до низьких витрат можуть вплинути на придбання дешевшого, але менш безпечного програмного забезпечення, що потенційно може створити вразливі місця або можливості для зловмисників.

Як правило, «інформаційна асиметрія» – це нездатність знати правду про інформацію (наприклад, що є точним, що є перебільшеним) або які

мотивації передують тому, якою інформацією обмінюються, і чому. По суті, інформаційні асиметрії вселяють сумнів у надійності даних, якими обмінюються сторони. Якщо розглядати їх як елементи ризику, стає зрозумілим, що цей бар'єр може суттєво вплинути на точні розрахунки поширеності загрози, масштабу вразливості, впливу шкідливого CNO чи ефективності контрзаходів. Це, звичайно, може вплинути на готовність, пріоритети безпеки чи інвестиції та може призвести до додаткових проблем. Мур зазначає, що на охоронні компанії не можна тиснути, щоб вони виводили на ринок нові технології, які захищають від найбільш суттєвих загроз, якщо їх забезпечують ненадійними даними про загрози та вразливості [419, с. 8]. Подібним чином повторення надання ненадійних даних у рамках ППП створює помилкове відчуття реальності та недовіру між партнерами, що, без сумніву, зменшує рівень участі у партнерстві та його ефективність.

Нарешті, Мур описує зовнішні ефекти, або ефекти «переливу» в кібербезпеці. У даному разі зовнішні ефекти стосуються того, як взаємозв'язок речей може або надати користь, або бути вразливим для великих спільнот користувачів. По суті, оскільки технологічна галузь має тенденції до домінуючих фірм, їх потреба полягає в тому, щоб бути сумісними з більшістю сторонніх постачальників, а звернення до найширшої бази спонукає їх спочатку до зростання частки ринку, а лише потім – до впровадження безпеки [там само]. Така мотивація сприяє впровадженню незахищеного програмного забезпечення для користувачів з подальшим постійним його виправленням та удосконаленням. Тобто заохочується розповсюдження небезпечного програмного забезпечення на ринку, що перешкоджає розробці та впровадженню захищеної інфраструктури та стримує інвестиції в безпеку.

Поряд із зазначеними бар'єрами ще однією проблемою, яка негативно впливає на ППП, є те, що влучно висловила Карр: те, що відповідає найкращим інтересам суспільства щодо кібербезпеки не завжди відповідає найкращим інтересам приватного сектору; соціальні вигоди не є значущими з

точки зору прибутковості, яким би бажаним не був результат [271, с. 57].

У своїй роботі над ідеологічною філософією ППП Ліндер описує партнерство як «акомодаційне – вони стримують привид оптової продажу та в обмін обіцяють вигідну співпрацю з державою» [398, с. 39]. Цей опис свідчить про те, що за певного моменту учасники очікують на більше, ніж дають самі, тобто утримуються від надто активних дій, покладаючись у цьому на інших. Але проблема полягає в тому, що якщо всі партнери підуть таким чином, виграш для всіх буде мінімальним, а партнерство взагалі стане марним зусиллям. Дві складові ППП демонструють цю ідею «стримування»: обмеження ролей та обмін інформацією. Розглянемо їх.

Обмеження ролей.

Ролі партнерства визначаються менше альтруїзмом, а більше унікальними обставинами, які визначають рівень прихильності сторін до цього партнерства. Наприклад, приватна організація може брати участь у партнерстві через певні, колись визначені, зобов'язання. Цей вид обов'язкової участі може не перетворитися на активну участь і, натомість, може бути пасивним, тобто сторона партнерства прийматиме інформацію, але не надаватиме її іншим партнерам. Як зазначає також з цього приводу Гівенс, хоча «актори в ППП можуть виявляти прихильність до партнерства, вони також стикаються з напругою між індивідуальними та колективними цілями, і вони, як правило, інвестують у партнерство якомога менше, щоб збільшити власні прибутки» [336, с. 42]. Таким чином, хоча спільне занепокоєння може бути обов'язковим, ролі та обов'язки для суб'єктів у партнерських відносинах повинні бути чітко визначені, або інакше партнерства стикаються з невдачею.

Як зазначає Віатер: «Оманливим є той факт, що органи державної влади говорять про свою «спільну відповідальність» із приватними зацікавленими сторонами, ця мова може відволікти від основної відповідальності держави гарантувати національну безпеку .. [і] держава не може сліпо довіряти приватним суб'єктам у виконанні охоронних

зобов’язань щодо критичної інфраструктури добровільно – до тих пір, поки ці зобов’язання не мають юридичної сили або поки не існує адекватної компенсації витрат, пов’язаних з виконанням цих завдань» [522, с. 257].

Іншими словами, публічний партнер зобов’язаний виконувати свої обов’язки та юридичні повноваження, тоді як приватний партнер чимось заохочується. Хоча і дещо ненауково, але прихильність до ППП може вимірюватися загальним розподілом часу, ресурсів, грошей, впливом на суспільне сприйняття або навіть порогами, за якими ризик буде прийнятий, або проігнорований.

Центральні органи влади можуть встановити певні стандарти у сфері кібербезпеки і вони наділені повноваженнями забезпечувати дотримання цих стандартів. Однак, як показує практика інших країн, уряди останнім часом широко встановлюють операційні стандарти та стандарти безпеки у публічних організаціях, але неохоче роблять це для приватного сектору. І це ставить потенційні сторони партнерства у нерівні умови. Тобто подібний підхід зводить повноцінне двобічне партнерство лише до «залучення» приватного сектора до здійснення заходів з кібербезпеки. Втім, це не позбавлене певного сенсу, оскільки занадто велике втручання уряду може мати негативні наслідки для економічної потужності приватного сектору. Як зазначають Данн-Кавелті і Сутер, будь-яка політика щодо захисту критичної інфраструктури повинна поглинати негативні наслідки лібералізації, приватизації та глобалізації, не скасовуючи позитивних наслідків [303, с. 76].

Таким чином, публічний сектор часто виявляє, що пропонує ті чи інші стимули приватному сектору для поліпшення співпраці та передачі даних, включаючи рішення та дії щодо пом’якшення негативних наслідків та винагороди за дотримання вимог і стандартів. Хоча з точки зору публічних осіб ці заохочення можна розглядати і як потенційні проблеми, чекаючи, що з часом заохочення трансформуватимуться у зростаючі витрати для публічного сектора. Тобто публічний сектор значною мірою покладається на таке собі «саморегулювання» приватного сектора стосовно забезпечення

кібербезпеки. Але у такому разі публічний сектор повинен самостійно оцінити, чи саморегулювання в приватному секторі належним чином захищає інформаційні системи критичної інфраструктури від кіберзагроз і чи адекватно правила партнерства примушують приватний сектор ділитися з публічним партнером даними про кіберзагрози, вразливості та шкідливий вплив.

Приватні організації схильні зосереджуватися на короткотермінових витратах та вигодах на шкоду довгостроковим наслідкам [318]. Такий підхід до діяльності керує розумінням приватним сектором кіберзагроз, їх впливу та їхнього внеску в ППП. Наприклад, стався злам бази особистих даних працівників приватної компанії з вантажоперевезень. Хоча цей злам, ймовірно, вплине на осіб, які працюють у компанії, але вплив на безперервність ділових операцій буде майже відсутнім. І якщо цей тип порушення даних не призведе до передбачуваних перебоїв у роботі, витрати на поліпшення кібербезпеки навколо того, як, де і чому зберігаються ці дані, швидше за все, не будуть пріоритетними.

Зосередження уваги на короткотермінових витратах також сприяє зменшенню кількості повідомлень про зловмисні CNO з двох, здавалося б, протилежних причин: 1) це занадто шкідливо і може коштувати грошей, або 2) це не має значення і не варто витрат. У першому випадку існує думка, що обмін подібною інформацією може спричинити шкоду для публічності або призведе до судових процесів щодо відповідальності за шкоду приватним особам [318]. Це може також стосуватися витрат, що стосуються зовнішніх факторів – наслідків поширення порушень кібербезпеки на інші організації або на інших осіб. Наприклад, зловмисник може зламати приватну комп’ютерну мережу і зробити її частиною бот-мережі, що спричинить відмову в обслуговуванні екстреної служби, такої як швидка допомога. Тобто вразливість у першій, не критично важливій системі, сприяла віктимізації критично важливої системи. Подібному можна було б запобігти, якщо б власник першої мережи вкладав достатньо коштів у її кіберзахист.

Обмін інформацією.

Обмін інформацією, як правило, є найбільш часто рекламованою перевагою ППП, однак цінність практики та даних, що передаються, зменшується за рахунок внутрішнього контролю як у публічному, так і в приватному секторах. Маркетинг цих партнерських відносин часто описує результат обміну інформацією як своєчасну, актуальну, точну та ефективну інформацію. Що стосується кібербезпеки, обмін даними, як очікується, має інформувати загальну базу знань про загрози, можливості, вразливості, які використовують зловмисники, і методи, за допомогою яких їх можна виявити, заперечити або порушити. Обмін інформацією може створити спільноти інтересів, покращити відносини між внутрішніми та зовнішніми партнерами і є основою для поліпшення кібербезпеки.

Проте Карр [271] визначає кілька безпосередніх проблем у даному процесі: не завжди зрозуміло, що означають дані або яка їх цінність у більшому контексті або для партнерів; певна інформація може виявити слабкі місця, якими може скористатися конкуренти; існують проблеми з класифікацією інформації, що обмежують те, як дані можуть використовуватися і з ким можна ділитися тими чи іншими даними. Додаткові бар'єри для ефективного обміну інформацією можуть також включати побоювання щодо розголошення наданої інформації з негативними наслідками від цього, а також певне постійним потоком інформації, що представляє сумнівну цінність для сторони партнерства.

Цінність обміну інформацією як вигоди зменшується, коли партнери не розуміють, що від них очікується, якщо не передбачено заходів, які забезпечують відповідність внесків партнерів, а також коли партнери роблять припущення щодо недостатнього внеску свого партнера. Щодо останнього пункту, Гівенс [336] описує це як причину, що дозволяє апатії просочуватися в партнерство. Коли один учасник припускає, що він непропорційно порівняно з іншими виграє від партнерства, незалежно від якості поданих ним даних, він, як правило, інвестує у партнерство менше.

Обмін інформацією може спричинити нерозуміння інформаційних потреб партнерів. Одне з проведених досліджень щодо обміну інформацією в рамках ППП з питань кібербезпеки показало, що інформаційні потреби в публічному та приватному секторі дуже різняться, перш за все, це стосувалося конфіденційності [394, с. 33]. Так, дослідження виявило, що спільна інформація поділялась на дві категорії: технічні індикатори загроз та контекстна інформація. Технічні індикатори загроз – це специфічні, загальні та повторювані форми інформації, які піддаються анонімізації, стандартизації та швидким формам розповсюдження. Контекстна інформація, навпаки, стосується детальної інформації про учасників партнерства та можливі загрози і створює більший ризик для конфіденційності та несанкціонованого розкриття секретної інформації. Розмежування двох зазначених категорій мало на меті визначити те, як із цими даними слід поводитись: обробляти, передавати (і кому саме) чи ділитися (і з ким саме). Але на практиці далеко не завжди було присутнім розуміння, що ці дві категорії даних мають різну аудиторію, різні наслідки від їх використання і вимагають різних режимів розповсюдження та обробки, що призводило до різного роду інцидентів і негативно впливало на партнерство у цілому

Це та інші подібні дослідження актуалізують три важливих питань. Перше питання – це питання вимірювання ефективності партнерства, для того, щоб однозначно з’ясувати, чи демонструють члени ППП взаємно вдосконалений кіберзахист в результаті своїх партнерських відносин? Номінальні зміни в показниках вторгнення за рік, зібрані компаніями з кібербезпеки та реагування на інциденти, не дозволяють говорити про ППП як джерело вдосконалення, хоча не можна і вважати, що партнерства не мають певного впливу. Натомість можна обґрунтовано припустити, що навіть пасивне залучення до обміну інформацією повинно призвести до певного поліпшення, але без вбудованої системи показників, що вимірює вдосконалення, ці партнерські стосунки приречені на посередність.

Як ніщо інше, ці партнерські відносини повинні висувати на перший

план союз потенційних жертв, мета яких повинна бути чітко мотивована перевагами повного співробітництва в процесі посилення безпеки. Знову використовуючи підходи управління ризиками, можна зазначити, що посилена безпека повинна співвідноситися із зменшенням успішної експлуатації відомих вразливостей, стримуванням або затриманням зловмисників, виявлених в результаті обміну інформацією або впровадженням вдосконалених захисних стратегій для виявлення та захисту критичної інформації або доступу до неї. Крім того, впровадження системи показників ефективності може бути корисним як публічним, так і приватним партнерам, оскільки може заохотити додаткову участь та визначити сфери партнерства, які потребують вдосконалення. Для публічного сектора показники можуть бути зосереджені на показниках участі в галузі, кількості унікальних шкідливих підписів, внесених групами-членами, або на деякий розрахунок часу та ресурсів, що витрачаються на виконання завдань партнерства, таких як зустрічі чи розповсюдження інформації.

Друге питання – це питання зобов'язань. Майже всі дослідження з ППП, у тому числі, у сфері кіберзахисту, показують, що існують проблеми між державними та приватними членами цих партнерств через мотиваційні чинники. Як вже зазначалось раніше, загалом публічний сектор мотивується прагненням забезпечення національної оборони та національної безпеки, а приватний сектор мотивується фінансовими аспектами – або витратами, або доходами. Ці спонукання проникають в інші аспекти відносин і можуть негативно впливати на партнерство, особливо, якщо існує ситуація «перебільшених очікувань». Для того, щоб це не відбувалось має бути встановлений і прийнятий всіма членами партнерства чіткий розподіл зобов'язань кожного члена, причому до реального початку партнерства.

Третє питання – це питання стримування. Відповідні дослідження чітко показують, що довіра є наріжним каменем, головною складовою партнерських відносин. Довіра впливає на участь, на внески членів та на те, як вони взагалі сприймають цінність цих партнерських відносин. Саме з

довіри чи її відсутності випливає питання того, що ми зазначили як «стримування». Саме відсутність повної довіри призводить до того, що члени партнерства «стримуються» у відносинах один з одним. Вони стримують результати тестів на проникнення, які можуть визначити, як зловмисники отримали доступ, бо бояться впливу на свій імідж. Вони стримують обмін інформацією, щоб не дати конкурентам уявлення про свою незахищеність. Вони стримують надання даних про тактику, прийоми та процедури фінансованих державою кіберкампаній через страх висвітлення своєї діяльності. Вони стримують фінансування для розробки або придбання ефективних систем попередження, які можуть миттєво обмінюватися даними про загрози, виявляти вразливі місця та надавати програмні виправлення. Вони стримують навчання своїх працівників щодо розуміння кіберзагроз, розуміння того, як поведінка користувачів забезпечує віктимізацію, або як донести цю проблему до керівництва. Вони стримуються, висуваючи чіткі цілі та очікування щодо цих відносин. Але в основному вони стримують свою чесність щодо того, що насправді працює, а що не працює. І існує єдиний шлях подолання всього цього стримування – це встановлення дійсно довірчих відносин у партнерстві.

Виходячи із розглянутого, можна запропонувати декілька принципів для підвищення результативності ППП у галузі кібербезпеки.

1. Перехід від «класичного» партнерства до взаємовигідної співпраці.

ППП є товариствами в тому сенсі, що публічні та приватні організації мають стурбованість загрозою у галузі кібербезпеки, але статус «партнера» заважає визначити те, що кожен член партнерства повинен розумно очікувати від іншого. Коли кожен член є у всьому рівний іншому, очікування можуть стати неоднозначними. Крім того, дане ППП не може бути справжнім партнерством, оскільки мотивація сторін занадто розбіжна, а внесок у партнерство занадто регулюється внутрішніми та зовнішніми силами. А зменшення ролі органів влади до ролі «партнера» зводить до мінімуму їхні можливості щодо імперативної та санкційної функції по

відношенню до приватних організацій, задіяних у партнерстві.

Певним чином, класичне партнерство може також звільнити публічний сектор від необхідності впроваджувати інноваційні способи обміну секретною інформацією про загрози з приватним сектором, приховуючи ці дані за своїми стандартами класифікації інформації та подалі від партнерських відносин.

Тому, на наш погляд, доцільно замість встановлення партнерства (суті, не обов'язково за назвою) укладати угоди щодо взаємовигідної співпраці з питань обміну інформацією та координації кіберризиків, визначивши, що метою такої співпраці є зменшення ризику (шляхом обміну інформацією, пов'язаною із загрозами, вразливими місцями та активами), та координувати дії і заходи для цього (знову через зосередження дій проти загроз, вразливостей або активів). Це буде відрізнятися від традиційної конструкції ППП тим, що чітко визначатиме передбачуваний внесок кожної із сторін.

2. Визначення ролей за допомогою управління ризиком.

Замість того, щоб обмінюватися будь-якою інформацією, яка потрапляє до них, з використанням окремих фільтрів як у публічних, так і у приватних організаціях, було б більш ефективним, якщо б сторони використовували елементи управління ризиком для розподілу відповідальності за свою участь. Виходячи з цього публічна установа повинна взяти на себе ініціативу в розумінні загрози – яка її сутність, як вона діє, які її можливості та ким вона мотивована. Публічний сектор для цього має у своєму розпорядженні розвідувальне співтовариство, контррозвідку та правоохоронні органи, які можуть розкрити ці дані. Урядові структури розуміють мотиви шпигунських агентів та злочинних угруповань, ймовірно, знають, як можна визначити їх цілі та має здатність впливати на їх операції.

У свою чергу, приватний сектор повинен взяти на себе ініціативу у визначенні активів або цілей зловмисних CNO. Тільки приватний сектор по-справжньому розуміє вплив шкідливих CNO на дані, процеси, системи, продукти та людей. У приватному секторі здебільшого створюються

технології, які є об’єктом шпигунства, технології, яка забезпечують створення та функціонування баз даних та захист важливої інформації; приватний сектор підтримує та керує системами, що складають критичні інфраструктури.

І ті, й інші мають спільну стурбованість щодо вразливостей, тому можуть діяти спільно: публічний сектор може розкрити вразливі місця, які здатні використовувати загрози, а приватний сектор може визначити, де ці вразливості перетинаються з їхніми активами, розрахувати імовірний негативний вплив, і надати ці висновки публічному сектору. Тоді рішення щодо курсу дій можуть дійсно прийматися спільно у рамках співпраці. Для прийняття таких рішень публічний сектор надає партнерам зібрану, оброблену та проаналізовану розвідувальну інформацію, яка описує загрозу, її можливості та цілі.

За деякими винятками, приватний сектор набагато більш реактивний, він проводить аналіз загрози після зіткнення з нею. До того ж, як зазначалось, організації приватного сектору набагато більше турбуються про те, щоб запобігти перебоям у своїй діяльності та мінімізувати найближчі наслідки. Знаючи це, публічний сектор повинен підтримувати короткострокові цілі приватного сектору; надавати йому інформацію, яка гарантує, що діяльність приватних організацій не переривається, через що вони, швидше за все, будуть більш охочі ділитися активами, інформацією про вразливості та аккаунти компрометації мереж або даних з публічним сектором. Звичайно, це представляє ризик втрати розвідувальних даних для публічного сектору внаслідок того, що обмін розвідувальними даними із занадто широкою аудиторією виявляє, а отже, і компрометує джерела та методи розвідки. Це ризик, на який слід зважати, але у кіберпросторі час є ворогом, інформація про кіберзагрози знецінюється швидко, враховуючи динамічний характер інфраструктури загроз, і посилюється щоденним розвитком нових злочинних можливостей та виявленням вразливостей програмного забезпечення.

Тому беручи до уваги стабільний успіх CNO іноземної розвідки проти приватної промисловості та швидкість, з якою супротивники переходять від розвідки до компрометації даних, більше не має сенсу надмірно захищати джерела та методи, одночасно вимагаючи від жертв компрометації даних негайно повідомляти про напади на них. Якщо метою є зменшення впливу шкідливих CNO та швидше виявлення та стримування супротивника і покращення стійкості кіберсистем у приватному секторі, тоді публічний сектор повинен бути більш готовим прийняти певний негативний вплив на себе від передачі інформації приватному сектору, навіть, отриманою від розвідувального співтовариства.

Звісно, це є певним компромісом з боку публічного сектора, але цей компроміс підсилює партнерство. Має зробити певні «кроки назустріч» і приватний сектор. Насамперед, він має взяти на себе ініціативу щодо інвентаризації та присвоєння вартості кожному активу. У багатьох випадках приватні компанії також краще розуміють цінність певної технології або даних для конкурентів, у тому числі для іноземних держав. Часто публічні та приватні організації мають різні погляди на вартість активів, що спричиняє розриви між присвоєнням пріоритетів захисту конкретним даним, програмам, технологіям тощо. Ці ускладняється ще й тим, що ці відмінності часто не ураховуються, що змушує публічний сектор зосередити свої зусилля на зборі даних про загрози, які можуть мати мало або зовсім не мати значення для приватного сектору, не зумівши спонукати їх витрачати ресурси на покращений захист.

Природно, приватний сектор, швидше за все, надаватиме значення даним, програмам та технологіям, що є суб’єктивно важливими для кожної компанії, що вимагає певного методу для стандартизації проблем. Тут як раз і потрібна координація. Публічний сектор повинен повідомляти про свої пріоритети з точки зору національної безпеки, тоді як приватний сектор повинен формулювати свою турботу про певні активи з економічної точки зору. І виходячи з цього приватний сектор повинен звернутися за допомогою

задля поліпшення захисту, а публічний сектор повинен взяти на себе певну роль, допомагаючи зробити це. Цього можна досягти шляхом надання коштів, ресурсів або додаткового доступу для боротьби із загрозами, після чого приватний сектор має розробляти системи, програми та процеси для покращення захисту цих активів, ініціюючи постійну оцінку цього захисту.

3. Запровадження спільної відповідальності щодо загроз і вразливостей.

Виявлення, передача та усунення вразливих місць є надзвичайно важливими для пом'якшення впливу шкідливих CNO. Однак з багатьох причин дані про вразливість також можуть бути приховані за внутрішніми обмеженнями, тому на практиці публічний сектор часто надає інформацію приватному сектору про загрози та вразливості, яка є корисною і такою, що не потребує отримання офіційного допуску, проте є неповною. Натомість оскільки це стосується партнерських відносин, подібна ситуація є недоречною, тому публічний сектор має брати на себе відповідальність за надання повної інформації, а приватний – за її збереження та нерозголошення. Наприклад, якщо певний спонсорований державою хакер проводить розвідку для визначення вразливостей веб-серверів, публічні члени партнерства повинні надавати інформацію про цю активність та її результати приватним членам своїх партнерств. Тоді ці вразливості можна використати як для визначення загроз, що становлять занепокоєння для публічного сектору, так і підштовхнути приватний сектор до оцінювання його схильності до вразливості. І навпаки, багато приватних компаній проводять тестування на проникнення в своє середовище, щоб визначити його вразливості. Виявлені в цих тестах вразливості слід передавати публічному сектору, щоб той міг визначити, чи загрожують йому ці вразливості.

4. Впровадження системи оцінювання партнерства.

На даний час системи для збору та оцінки показників, пов'язаних з ефективністю ППП, майже відсутні. У той же час, цілком природно, що якщо

кожна сторона має цілі приєднатися до партнерства, вона також повинна мати можливість оцінити, чи досягнуто ці цілі. Дані, які врешті-решт дадуть можливість зробити таку оцінку, слід отримувати на заздалегідь визначеній основі для того, щоб постійно мати уявлення про результати та ефективність партнерських заходів. Потім ці дані можна використовувати для коригування цілей, очікувань, аудиторій або процесів.

Показники також повинні доповнюватися чесними відгуками членів партнерства про сприйняту цінність партнерства. Але при цьому не слід застосовувати негативні зауваження щодо партнерства, хоча вони повинні ґрунтуватися на фактичних даних. Прикладами чесної критики можуть бути скарги на те, що уряд надав дані у форматі, який не використовується сучасними пристроями безпеки, такими як системи виявлення вторгнень, або що приватні організації не змогли вчасно ліквідувати вразливість і були через це неодноразово скомпрометовані. Дана система показників має бути індивідуально розробленою для кожного партнерства, і бути визнаною всіма партнерами, проте і з можливістю її коригування у подальшому.

Висновки до п’ятого розділу

Розгляд можливих напрямів удосконалення забезпечення кібербезпеки в публічному секторі в сучасних умовах дав можливість зробити такі висновки:

1. З’ясовано, що у кіберсередовищі існують певні кіберризики. Кіберризик, який за своєю суттю існує у всіх ІТ-активах, є різновидом ризику, який виникає у різних акторів, від приватних осіб до міжнародних організацій, які мають критично важливі ІТ-активи. Кіберризик відрізняється від «звичайного» не лише одним конкретним ризиком, а й технологією, переносниками, засобами тощо. Більше того, кіберризики мають дві характеристики: великий потенційний вплив та низьку ймовірність.

2. Як показала практика останніх двадцяти років, можна визначити

такий основний перелік кібератак: атаки соціальної інженерії в Інтернеті; мережеві сніфери та спуфінги пакетів; знаходження та використання вразливостей у програмному забезпеченні без вихідного коду; кіберзагрози та кібербулінг; автоматизовані зонди та скани; інструменти вторгнення графічного інтерфейсу; DDOS-атаки; промислове шпигунство; атаки на виконувані коди (проти браузерів); викрадення сесій; поширені атаки на інфраструктуру DNS та використання NNTP для розповсюдження атаки «Stealth» та інших вдосконалених методів сканування; трояни віддаленого доступу на базі Windows (Back Orifice); поширення шкідливого коду електронною поштою; широкомасштабне розповсюдження троянів; атака на конкретних користувачів; широкомасштабне використання хробаків; складні атаки ботнет-команд; експлойти мобільних пристроїв на Android; Advance Persistent Threat (APT); хмарні атаки; вбудовані шкідливі програми; шкідливі компоненти на базі апаратного забезпечення; шкідливі програми Old School (MiniDuke).

3. Визначено, що з урахуванням нових кіберризиків та більш складних шкідливих програм, країни та міжнародні організації, такі як НАТО, ENISA тощо, шукають нових способів боротьби зі складними проблемами у галузі кібербезпеки. Суттєвим кроком для країн є формування національної стратегії кібербезпеки та відповідних політик. Проте незважаючи на те, що ці стратегії та політики інтенсивно охоплюють військову, розвідувальну та критичну інфраструктури, кібербезпека на рівні організацій часто ігнорується. Доведено, що для забезпечення надійної кібербезпеки на національному рівні має бути забезпечена кібербезпека і на рівні організацій. Виходячи з цього було запропоновано модель інституційної кібербезпеки, яка включає увесь спектр акторів (приватні особи, публічні та приватні установи, національні безпекові структури та міжнародні організації). У запропонованій моделі організаційні актори розглядаються як основні, такі, що разом утворюють основу організації кібербезпеки. І хоча найслабшою ланкою в інформаційній безпеці вважається людина, з точки зору

національної безпеки найслабшою ланкою є найслабша організація, що підлягає впливам кіберризиків. Але на відміну від зазначених у національних стратегіях кібербезпеки положеннях, з точки зору моделі інституційної кібербезпеки, для забезпечення надійної кібербезпеки слід брати до уваги не лише організації, які управляють критичною інфраструктурою, а й всі інші організації, що мають кіберзахист.

4. Запропонована модель інституційної кібербезпеки забезпечує загальний підхід, за допомогою якого кожна організація може адаптувати дану модель до власних потреб безпеки, для розвитку своїх можливостей із забезпечення кібербезпеки. Для досягнення цієї мети було визначено основні принципи інституційної кібербезпеки, що випливають з моделі: підхід до кібербезпеки повинен бути холістичним; слід застосовувати гнучкий стиль управління; слід впроваджувати методи постійного вдосконалення діяльності, орієнтовані на управління ризиками; на додаток до координації діяльності публічних, приватних, академічних та неурядових організацій; міжнародна співпраця та обмін інформацією також мають складати базис забезпечення кібербезпеки; мають заохочуватись прозорість, підзвітність, етичні цінності, свобода слова; важливим є встановлення балансу між безпекою та застосовністю ІТ-продуктів і технологій.

5. Обґрунтовано інтегровану теоретико-методологічну модель розробки національної стратегії кібербезпеки, відповідно до якої актори у кіберпросторі (державні актори, недержавні актори, кінцеві користувачі та кіберзлочинці) здійснюють дії (проводять політику, слідують політиці, атакують, захищаються від нападів, отримують і передають інформацію, здійснюють комунікацію, використовують ІКТ для роботи й у побуті тощо), які перетинаються з різними аспектами кіберпростору та кібербезпеки (політичними, соціальними, культурними, технологічними) та породжують явища кібербезпеки, такі як вразливості, цілісність системи, шкідлива поведінка, ідентичність, мотивація тощо.

6. Визначено, що державні та недержавні актори, конкуренція за

відносні вигоди та політичні аспекти кібербезпеки вимагають неореалістичного підходу до її забезпечення і формулювання відповідних положень стратегії кібербезпеки. У той же час, інтерсекційність дозволяє врахувати у стратегії кібербезпеки соціальні аспекти, зокрема, такі як рівність і справедливість у кіберпросторі, адже ці фактори часто становлять причини злочинної групової поведінки у кіберсередовищі. Кінцеві користувачі, кіберзлочинці та їх поведінка є продуктом їхньої ідентичності як представників певного національного культурного середовища, так і користувачів Інтернет. Врахувати культурні аспекти кібербезпеки допоможе соціальний конструктивізм. Нарешті, кібервестфалізм дозволяє врахувати у стратегії кібербезпеки сучасні технологічні аспекти та їхній вплив на інші аспекти кіберпростору та кібербезпеки.

7. Встановлено, що зі стратегічної точки зору кібербезпека реагує на захист національних інтересів та активно реалізує ці інтереси, а кіберпростір сприймається як середовище загроз та можливостей, в якому держава повинна діяти задля власного збереження та досягнення власних цілей. Крім того, кіберпростір проблематизується як місце і як джерело небезпеки. Відповідно, кіберпростір можна розглядати як суму двох компонентів. Перший – це фізичний субстрат кіберпростору: комп'ютери та мережі, в які вони зібрані та через які вони «спілкуються». Другий – це комунікації, яким сприяє цей фізичний рівень: мережева, цифрова діяльність, що включає вміст і дії, які здійснюються через цифрові мережі. Обмін інформацією залежить від існування фізичного рівня, який апріорі необхідний для існування кіберпростору. Кіберпростір є як фактичним, так і віртуальним, у тому сенсі, що кіберпростір є частково віртуальним середовищем, що ґрунтується на суттєвості фізичних систем. Інформація, якою обмінюються та на яку реагують, може бути далі розмежована на синтаксичний та семантичний рівень. Синтаксичний рівень – це місце, де комп'ютери взаємодіють між собою, і містить домовленості, за якими вони це роблять, такі як протоколи TCP / IP, які керують маршрутизацією інтернет-трафіку. Семантичний рівень

– це той, де інформація створюється, зберігається та маніпулюється акторами для соціальних, економічних та політичних цілей. В основному саме цей семантичний рівень можна назвати цифровою діяльністю. Отже, кіберпростір є середовищем як технологічної, так і соціальної дії, хоча сам по собі не є інфраструктурою. Тому безпека кіберпростору (кібербезпека) повинна функціонувати як у технологічному, так і в соціальному вимірах. Таким чином, як стратегічна сфера, кіберпростір також повинен бути доменом влади. «Домен» слід розуміти як у просторовому розумінні – кіберпростір настільки фізичний, скільки і віртуальний, але також і у вужчому розумінні – як колективність соціальних суб'єктів, які зазнають впливу певної форми влади.

8. Визначено, що публічно-приватне партнерство (ППП) у сфері кібербезпеки актуалізує три важливі питання. Перше питання – це питання вимірювання ефективності партнерства для того, щоб однозначно з'ясувати, чи демонструють члени ППП взаємно вдосконалений кіберзахист в результаті своїх партнерських відносин. Впровадження системи показників ефективності може бути корисним як публічним, так і приватним партнерам, оскільки може заохотити додаткову участь та визначити сфери партнерства, які потребують вдосконалення. Для публічного сектора показники можуть бути зосереджені на показниках участі в галузі, кількості унікальних шкідливих підписів, внесених групами-членами, або на деякий розрахунок часу та ресурсів, що витрачаються на виконання завдань партнерства, таких як зустрічі чи розповсюдження інформації. Друге питання – це питання зобов'язань. Майже всі дослідження з ППП, у тому числі, у сфері кіберзахисту, показують, що існують проблеми між державними та приватними членами цих партнерств через мотиваційні чинники. У цілому, публічний сектор мотивується прагненням забезпечення національної оборони та національної безпеки, а приватний сектор мотивується фінансовими аспектами – або витратами, або доходами. Ці спонукання проникають в інші аспекти відносин і можуть негативно впливати на

партнерство, особливо, якщо існує ситуація «перебільшених очікувань». Для того, щоб це не відбувалось має бути встановлений і прийнятий всіма членами партнерства чіткий розподіл зобов'язань кожного члена, причому до реального початку партнерства. Третє питання – це питання стримування. Відповідні дослідження чітко показують, що довіра є наріжним каменем, головною складовою партнерських відносин. Довіра впливає на участь, на внески членів та на те, як вони взагалі сприймають цінність цих партнерських відносин. Саме з довіри чи її відсутності випливає питання того, що ми зазначили як «стримування». Саме відсутність повної довіри призводить до того, що члени партнерства «стримуються» у відносинах один з одним. Вони стримують результати тестів на проникнення, які можуть визначити, як зловмисники отримали доступ, бо бояться впливу на свій імідж. Вони стримують обмін інформацією, щоб не дати конкурентам уявлення про свою незахищеність. Вони стримують надання даних про тактику, прийоми та процедури фінансованих державою кіберкампаній через страх висвітлення своєї діяльності. Вони стримують фінансування для розробки або придбання ефективних систем попередження, які можуть миттєво обмінюватися даними про загрози, виявляти вразливі місця та надавати програмні виправлення. Вони стримують навчання своїх працівників щодо розуміння кіберзагроз, розуміння того, як поведінка користувачів забезпечує віктимізацію, або як донести цю проблему до керівництва. Вони стримуються, висуваючи чіткі цілі та очікування щодо цих відносин. Але в основному вони стримують свою чесність щодо того, що насправді працює, а що не працює. І існує єдиний шлях подолання всього цього стримування – це встановлення дійсно довірчих відносин у партнерстві.

ВИСНОВКИ

У дисертації вирішено актуальну наукову проблему щодо розробки теоретико-методологічних засад забезпечення кібербезпеки в публічному секторі в сучасних умовах. Отримані в процесі дослідження результати свідчать про реалізацію поставлених мети й завдань і дають можливість зробити такі основні висновки:

1. Визначено, що кібербезпека охоплює широкий набір практик: оцінка ризиків і тестування проникнення; аварійне відновлення; криптографія; контроль та спостереження за доступом; мережева архітектура, програмне забезпечення та безпека; безпекові операції; фізична безпека тощо. При цьому кібербезпека має три основні складові: 1) інформаційно-комунікаційні системи, які є надійними і можуть протистояти атакам; 2) методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; 3) забезпечення системної реактивності на кібератаки. Встановлено, що впровадження систем кібербезпеки має важливі наслідки для публічних інтересів інформаційного суспільства, оскільки це дає можливість належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології. Виходячи з цього, кібербезпеку слід розглядати як суспільне благо. Було зазначено, що три важливі переваги випливають із управління кібербезпекою як суспільним благом: системний підхід до безпеки, спільна відповідальність між різними стейкхолдерами, розвиток співпраці у сфері кібербезпеки.

2. З’ясовано, що поняття кібербезпеки у цілому та в публічному секторі зокрема безпосередньо пов’язане з феноменом інформаційного суспільства та електронного врядування, що з’явилось внаслідок розвитку інформаційного суспільства. Електронне врядування ґрунтується на трьох «стовпах»: довірі, прозорості та підзвітності, які є нерозривно взаємопов’язаними. З іншого боку, на сучасний світ у цілому та публічне

управління зокрема впливають процеси глобалізації. Виходячи з цього, а також враховуючи особливості публічного сектора, для нього було визначено п’ять основних викликів щодо забезпечення кібербезпеки: 1) публічному сектору властива велика ступінь оперативної незалежності та «ізольованості» між різними його частинами, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного; 2) важливі загальнодоступні дані створюються, зберігаються та застосовуються відповідними суб’єктами поза органами публічної влади, тому визначення безпеки публічного сектора має бути розширеним та переосмисленим; 3) поведінка людини, раціональна або нераціональна, є стрижнем кібербезпеки, тому необхідними є заходи для формування безпечної поведінки у кіберпросторі; 4) існує зворотна залежність між використанням інформаційно-комунікаційних технологій і кібербезпекою, тому необхідним є забезпечення тут певної рівноваги; 5) користувачі електронного уряду потребують такого ж кіберзахисту від органів публічної влади, як органи публічної влади потребують захисту від третьої сторони, тому важливим є налагодження партнерства щодо забезпечення кібербезпеки.

3. Встановлено, що концептуальні засади забезпечення кібербезпеки в органах публічної влади складають, з одного боку, виміри кібербезпеки (людський, організаційний, інфраструктурний, технологічний, нормативний), з іншого боку – дії, необхідні для забезпечення кібербезпеки. Людський вимір є найбільш фундаментальним і, у той же час, найбільш слабким елементом кібербезпеки, оскільки хоча кіберпростір побудований на технологіях, людина управляє ними і контролює їх, а недостатня поінформованість і недостатні знання роблять людей найбільш вразливою ланкою в порівнянні з іншими. Організаційний вимір зосереджений на інститутах всередині кіберпростору, це функціональна структура, яка контролює кіберпростір, і зміцнення цього виміру може відбуватись за двома напрямами: 1) стратегічні дії орієнтовані всередині країни, такі як підвищення потенціалу і можливостей відповідної структури; 2) стратегічні

дії орієнтовані назовні, які активізують співпрацю для забезпечення безпеки кіберпростору. Інфраструктурний вимір є середовищем, яке створює кіберпростір, без інфраструктури кіберпростір – ніщо, тому зміцнення цього виміру необхідно для підтримки кіберсередовища у цілому; якщо цей вимір слабкий, транзакції в кіберпросторі можуть «впасти». Технологічний вимір розширює можливості кіберпростору, і оскільки кіберпростір включає в себе найбільш передові технології, зміцнення цього виміру означає впровадження новітніх та найбільш ефективних технологій, що забезпечують кібербезпеку і дозволяють проводити подальші дослідження і розробки у цій сфері. Нормативний вимір структурує кібербезпеку і створює певне імперативне середовище у кіберпросторі, цей вимір спрямований на формування національної кіберекосистеми шляхом створення і застосування нормативно-правової бази та розробки необхідних стандартів.

4. Узагальнення зарубіжних практик щодо забезпечення кібербезпеки у публічному секторі показало, що кожна з розглянутих країн має власні національні стратегії кібербезпеки (НСК) і відповідне законодавство для вирішення проблем кібербезпеки. В більшості НСК загрози для критичної інфраструктури та кіберзлочинність відіграють важливу роль і вказують на зростання шкоди для економіки, завданої кібератаками. У формальному сенсі, сфера кіберпростору вже включена до порядку денного з питань безпеки всіх держав, однак у підходах до її забезпечення є відмінності. Забезпечення кібербезпеки відрізняється за тим, як держави, по-перше, визначають референтний об’єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики. Відповідно до цих відмінностей їх можна віднести до двох категорій. Перша категорія – держави, що мілітаризують питання кібербезпеки. Ці держави більш точно визначають конкретні референтні об’єкти та називають захист цих об’єктів національним пріоритетом. Такий підхід піднімає кібербезпеку на найвищий рівень національної безпеки та зосереджує увагу на захисті ІКТ та державних

інформаційних ресурсів. Відповідно, відповідальність за реагування на кіберзагрози у цих державах передана воєнним та оборонним органам. Друга категорія – держави, що криміналізують питання кібербезпеки, покладаючись на економічний підхід у забезпеченні кібербезпеки. Їхні референтні об'єкти відрізняються і здебільшого стосуються належного функціонування системи національної економіки та приватної власності. ІКТ та державні цифрові ресурси не мають переваги над іншими законними референтними об'єктами. Унаслідок цього держави з домінуючим економічним підходом зосереджуються на кримінальній діяльності у кіберпросторі, а проблеми кібербезпеки розглядають як «ризики». Перелік потенційних джерел таких ризиків також фрагментований і включає не лише зовнішні міжнародні суб'єкти, але також внутрішні суб'єкти – хакерів, хактивістів, кримінальні організації і навіть ненавмисні злами мереж. На нашу думку, в Україні доцільно використовувати обидва зазначені підходи разом, оскільки це сприятиме кращому розумінню кібербезпеки як явища і допоможе пояснити перешкоди для співпраці держав, що займаються питаннями кібербезпеки на міжнародному рівні. Крім того, визначення особливостей різних підходів до кібербезпеки може пояснити конкретні дії держав у кіберпросторі. Розуміння відмінностей в сприйнятті державами кіберзагроз, референтних об'єктів і потенційних противників становить основу для обговорення так званої кіберідентичності держав та недержавних суб'єктів. Це може бути корисним теоретичним знаряддям для аналізу потенційних кіберконфліктів та моделей співпраці у цій сфері.

5. Встановлено, що за останній час загрози кібербезпеці в публічному секторі постійно зростають і стають більш складними, і певним чином це пов'язано із впровадженням соціальних мереж і Gov 2.0 у діяльність публічних організацій, які намагаються стати більш відкритими і прозорими. Однак, незважаючи на загрози, органи влади на всіх рівнях, і особливо місцеві органи влади, повинні продовжувати впроваджувати і сприяти розробці нових технологій і рішень Gov 2.0, щоб залишатися

надійними постачальниками публічних послуг та інформації. Тим не менше, органи влади повинні робити це обережно, стратегічно, маючи відповідну політику, розробляючи необхідні керівні принципи, використовуючи відповідні технологічні інструменти та навчання персоналу для захисту від загроз кібербезпеки. Наявність відповідної політики та керівних принципів у сфері кібербезпеки також є позитивним сигналом для громадян, нагадуючи про основоположну природу Gov 2.0 як про рух до відкритої, прозорої та безпечної арени діяльності публічних організацій. Громадяни в світі Web 2.0 очікують інтеграції таких технологій в свої взаємодії з публічними структурами, але як і раніше існують основні проблеми конфіденційності та обміну інформацією. Надання керівництв і політик може пом'якшити такі побоювання і відкрити для обговорення додаткові потреби і очікування громадян щодо ступеня розвитку сфери ІКТ. Публічні комунікації повинні мати свої власні керівні принципи, щоб гарантувати, що користувачі розуміють, куди направляється їх інформація, що очікується від її вмісту і яким чином цей вміст може бути видалено, показано або змінено. Рекомендації по загальнодоступним комунікаціям допомагають сформувати очікування, полегшують діалог і зменшують потенційні проблеми, які можуть виникнути в результаті видалення / зміни контенту. Слід також визначити правила у відношенні того, яким чином інформація надається для публічного доступу. У цілому, було визначено, що забезпечення кібербезпеки у середовищі Gov 2.0 має ґрунтуватись на реалізації таких заходів: модерування контенту публічних аккаунтів; запобігання несанкціонованому використанню і передачі конфіденційної інформації; використання браузерів з обмеженими привілеями; впровадження систем виявлення / запобігання вторгнень; використання сервісів Web-репутації; фільтрація універсального локатора ресурсів (URL) та Інтернет-протоколу (IP); фільтрація шкідливих програм по периметру мережі; використання інструментів попереднього перегляду скорочення URL.

6. Визначено, що з урахуванням нових кіберризиків та більш

складних шкідливих програм, країни та міжнародні організації, такі як НАТО, ENISA тощо, шукають нових способів боротьби зі складними проблемами у галузі кібербезпеки. Суттєвим кроком для країн є формування національної стратегії кібербезпеки та відповідних політик. Однак, незважаючи на те, що ці стратегії та політики інтенсивно охоплюють військову, розвідувальну та критичну інфраструктури, кібербезпека на рівні організацій часто ігнорується. Проте доведено, що для забезпечення надійної кібербезпеки на національному рівні має бути забезпечена кібербезпека і на рівні організацій. Виходячи з цього було запропоновано модель інституційної кібербезпеки, яка включає увесь спектр акторів (приватні особи, публічні та приватні установи, національні безпекові структури та міжнародні організації), та відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість.

7. Доведено необхідність реалізації комплексу взаємопов’язаних заходів, спрямованих на підвищення рівня кібербезпеки в публічному секторі. Вони передбачають реалізацію: заходів організаційного характеру, зокрема, через утворення спеціальних підрозділів в штатному розписі органів публічної влади; заходів фінансового характеру, які передбачають обов‘язкове фінансування в державному та місцевому бюджетах коштів на кіберзахист, інвестування в кібераналітику і хмарні технології; кадрових заходів, що включають регулярне підвищення кваліфікації всіх державних службовців і посадових осіб органів місцевого самоврядування з питань захисту організаційної та персональної інформації, електронного документообігу, онлайн комунікацій тощо; заходів матеріально-технічного характеру, метою яких є постійне оновлення комп‘ютерного обладнання та

його програмного забезпечення.

8. Показано, що запропонована модель інституційної кібербезпеки забезпечує загальний підхід, за допомогою якого кожна організація може адаптувати дану модель до власних потреб безпеки для розвитку своїх можливостей із забезпечення кібербезпеки. Для досягнення цієї мети було визначено основні принципи інституційної кібербезпеки, що випливають із запропонованої моделі, і до яких належать такі: 1) підхід до кібербезпеки повинен бути холістичним; 2) слід застосувати гнучкий стиль управління; 3) слід впроваджувати методи постійного вдосконалення діяльності, орієнтовані на управління ризиками; 4) на додаток до координації діяльності публічних, приватних, академічних та неурядових організацій, міжнародна співпраця та обмін інформацією також мають складати базис забезпечення кібербезпеки; 5) у забезпеченні кібербезпеки мають заохочуватись прозорість, підзвітність, етичні цінності, свобода слова; 6) важливим є встановлення балансу між кібербезпекою та застосовністю ІТ-продуктів і технологій.

9. З’ясовано, що поступова, але послідовна мілітаризація та централізація управління посилюється в країнах, які є головними об’єктами кібератак, таких як США чи країни ЄС. Тому в цих країнах підходи до забезпечення кібербезпеки найбільше нагадують підходи неореалізму, з точки зору якого, фокус зосереджений на державах, а влада та безпека розглядаються як функції відносної вигоди від конкуруючих суперників. Однак, неореалізм не розпізнає загрози та можливості для більшої цілісності систем, які представляють недержавні актори та технології. Зробити це можна з позицій соціального конструктивізму, який вміє аналізувати спільне сприйняття як всередині, так і поза суспільством, і вміє розпізнавати як функцію ідентичності в динаміці національної безпеки, так і те, як ці сприйняття впливають на безпеку. Проте неореалістичний та соціально-конструктивістський підходи обидва розроблені як інтерпретації традиційної міжнародної безпеки, і по суті, жоден з них не включає інформаційні

технології у свій дискурс. Уникнути цього недоліку дозволяє кібервестфаліанство, яке базується на розвитку можливих або ймовірних майбутніх технологій, і стверджує, що державна централізація Інтернету в багатьох країнах, спільно з розвитком цих майбутніх технологій, призведе до появи національних «кібермеж». Однак ця теорія не приділяє уваги ролі, яку відіграють чи можуть відігравати окремі громадяни, та їх поведінці у кіберпросторі. Кібервестфаліанство також дещо обмежене за своїм обсягом (кіберпростір) та підходом до рішень (технологія). Воно також не враховує економічну, політичну та військову динаміку між великими, середніми та регіональними державами. Усунути ці проблеми може певним чином теорія інтерсекційності, якщо її застосувати до кіберзбезпеки. Враховуючи зазначене було визначено, що теоретико-методологічна основа розробки національних стратегій кібербезпеки має ґрунтуватись на інтегративному підході, який містить елементи інтерсекційності, неореалізму, соціального конструктивізму та кібервестфаліанства.

10. Встановлено, що як стратегічна сфера, кіберпростір також повинен бути доменом влади. «Домен» слід розуміти як у просторовому розумінні – кіберпростір настільки фізичний, скільки і віртуальний, але також і у вужчому розумінні – як колективність соціальних суб’єктів, які зазнають впливу певної форми влади. З’ясовано при цьому, що в основі концепції влади є два «виміри». Перший вимір – це види соціальних відносин, за допомогою яких впливає (та реалізується) спроможність суб’єктів, а другий вимір – специфіка цих соціальних відносин. Перший вимір відрізняється тим, як виражається влада: або через взаємодію між соціальними суб’єктами, або через регуляторні соціальні відносини. Другий вимір влади стосується специфіки соціальних відносин влади, будь то прямі та безпосередні, або опосередковані та дифузні. Зазначені два виміри разом створюють чотири типи влади: примусова, інституційна, структурна, продуктивна. Було доведено, що стосовно кібербезпеки примусова влада надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада

надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кібербезпекою.

11. З'ясовано, що на даний час поширюється створення середовищ, де публічний і приватний сектор активно та успішно співпрацюють – іноді як клієнт і постачальник, іноді через нагляд і дотримання, іноді як партнери. Ці домовленості зазвичай переслідують спільні цілі отримання певних позитивних результатів, але в деяких випадках партнерські відносини формуються як захисна відповідь спільним противникам. Саме така мета партнерства є головною у сфері забезпечення кібербезпеки. Публічно-приватне партнерство (ППП) як захисна модель покладається на те, що кожен учасник вносить щось унікальне в партнерство, що може пом'якшити його слабкі сторони та посилити його сильні сторони. Для ППП, орієнтованих на кібербезпеку, саме ступінь спільних наслідків пов'язує його учасників. Таке призначення зумовлює для публічного сектора необхідність визначити кібербезпеку приватних організацій як проблему національної безпеки, а отже, визнати відповідальність уряду за її забезпечення. Приватний сектор, у свою чергу, створює, управляє та підтримує системи, технології та процеси, що складають критичну інфраструктуру, забезпечення кібербезпеки якої є складовою забезпечення національної безпеки. Виходячи з цього і враховуючи наявні проблеми у даній сфері було обґрунтовано основні принципи публічно-приватного партнерства у сфері забезпечення кібербезпеки, а саме: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Айрапетян М. С. Зарубежный опыт использования государственно-частного партнерства / М. С. Айрапетян // Государственная власть и местное самоуправление. – 2009. – №2. – С. 34–45.

2. Александров В. В. Інноваційне управління в державі та механізм його реалізації / В. В. Александров, О. А. Стороженко, В. П. Чеботаръов. – Х. : Основа, 1998. – 312 с.

3. Ансофф И. Стратегическое управление / И. Ансофф ; пер. с англ. – М. : Экономика, 1989. – 519 с.

4. Антология мировой правовой мысли. В 5-и т. – Т. 2. Европа: XV – XVII вв. – М. : Мысль, 1999. – 829 с.

5. Армстронг М. Практика управления человеческими ресурсами / М. Армстронг ; пер. с англ. ; под ред. С. К. Мордовина – 8-е узд. – СПб. : Питер, 2005. – 832 с.

6. Аронсон О. Богема: опыт сообщества. Наброски к философии асоциальности / О. Аронсон. – М. : Фонд науч. исследований "Прагматика культуры", 2002. – 96 с.

7. Бабак В. П. Інформаційна безпека та сучасні мережеві технології : англо-українсько-російський словник термінів / В. П. Бабак, О. Г. Корченко . – Київ : Видавництво Київського Національного авіаційного університету, 2003 . – 670 с.

8. Бакуменко В. Д. Парадигма інноваційного розвитку суспільства: сучасні концепції реформування публічного управління / В. Д. Бакуменко, С.А. Попов // Ефективність державного управління : зб. наук. пр. – Вид-во ЛРІДУ НАДУ, 2015. – № 43. – С. 21–28.

9. Бакуменко В. Д. Формування державно-управлінських рішень: проблеми теорії, методології, практики : монографія / В. Д. Бакуменко. – К. : Вид-во УАДУ, 2000. – 320 с.

10. Бауман З. Глобализация. Последствия для человека и общества /

З. Бауман. – М. : Весь мир, 2004. – 188 с.

11. Башук А. І. Комунікаційні стратегії державної влади в умовах інформаційного суспільства : монографія / А. І. Башук. - Кам'янець-Подільський : Друкарня "Рута", 2019. - 583 с.

12. Белл Д. Грядущее постиндустриальное общество / Д. Белл ; пер. с англ. – М. : Academia, 2004. - 958 с.

13. Белл Д. Социальные рамки информационного общества / Д. Белл // Новая технократическая волна на Западе. – М. : Прогресс, 1986. – 454 с.

14. Бережний В. О. Сучасні концепції публічного управління / В. О. Бережний // Актуальні проблеми державного управління : зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2013. – № 2 (44). – 296 с.

15. Бережний В. О. Основні світові моделі державного управління [Електронний ресурс] / В. О. Бережний // Державне будівництво. – 2011. – № 2. – Режим доступу : http://kbuapa.kharkov.ua.

16. Биков В. Ю. Відкриті web-орієнтовані системи моніторингу впровадження результатів науково-педагогічних досліджень [Електронний ресурс] / В. Ю. Биков, О. М. Спірін, Л. А. Лупаренко // Теорія і практика управління соціальними системами. – 2014. – № 1. – С. 3–25. – Режим доступу : http://nbuv.gov.ua/UJRN/Tipuss_2014_1_3.

17. Богомаз К. Ю. Методологічні орієнтири вивчення соціальних комунікацій в умовах інформаційного суспільства : монографія / К. Ю. Богомаз, Ю. С. Кравцов ; Дніпров. держ. техн. ун-т. - Кам'янське : ДДТУ, 2019. - 163 с.

18. Брайко Б. В. Професійна підготовка магістрів з кібербезпеки в університетах Великої Британії : автореф. дис. ... канд. пед. наук : 13.00.04 / Брайко Богдан Валерійович ; Хмельниц. нац. ун-т. - Хмельницький, 2020. - 20 с.

19. Брижко В. М. Інформаційне суспільство: Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок,

юриспруденція / В. М. Брижко, О. М. Гальченко, В. С. Цимбалюк та ін. – К. : Інтеграл, 2002. – 220 с.

20. Бутко М. П. Формування інформаційного забезпечення в системі державного управління : монографія / М. П. Бутко, М. Ю. Дітковська. – Ніжин : Аспект-Поліграф, 2010. – 244 с.

21. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : автореф. дис. ... канд. юрид. наук : 12.00.07 / Бухарєв Владислав Вікторович ; Сум. держ. ун-т. - Суми, 2018. - 20 с.

22. Бухтатий О. Є. Україна медійна: на порозі інформаційної революції [Текст] : монографія / О. Бухтатий, О. Радченко, Г. Головченко ; [за наук. ред. Радченка О. В.]. – Київ : Панасенко [вид.], 2015. – 207 с.

23. Василенко И. А. Административно-государственное управление в странах Запада: США, Великобритания, Франция, Германия : учеб. пособие / И. А. Василенко. – изд. 2-е, перераб. и доп. – М. : Логос, 2001. – 200 с.

24. Вебер. М. Избранные произведения / М. Вебер. – М. : Прогресс. – 1990. – 809 с.

25. Взаємодія громадських організацій, місцевої влади та підприємців / [Л. В. Беззубко та ін.] ; Проект «Голос громадськості», НГО Макіївська міська спілка підприємців «Сприяння». – Донецьк : Норд-компьютер, 2007. – 299 с.

26. Взаємодія органів державної влади та громадянського суспільства : навч. посіб. для студ. вищ. навч. закл. / [Ю. П. Сурмін та ін. ; за наук. ред. Ю. П. Сурміна, А. М. Михненка] ; НАДУ при Президентові України ; Ін-т пробл. держ. упр. та місц. самовряд. – К. : НАДУ, 2011. – 386 с.

27. Використання інформаційних та комунікаційних технологій в сучасному цифровому суспільстві : колективна монографія. - Херсон : Вишемирський В. С., 2020. - 148 с.

28. Вінникова Н. А. Парадокси політичних рішень в епоху постдемократії : монографія / Наталія Вінникова ; Харків. нац. ун-т ім. В. Н. Каразіна. - Харків : ХНУ ім. В. Н. Каразіна, 2019. - 423 с.

29. Вітте Л. Європейська соціальна модель і соціальна згуртованість: яку роль відіграє ЄС? / Лотар Вітте; Фонд ім. Фрідріха Еберта, Регіон. представництво в Україні та Білорусі. – К. : Заповіт, 2006. – 44 с.

30. Вылков Р. И. Киберпространство как социокультурный феномен, продукт технологического творчества и проективная идея : автореф. дис. ... канд.философ.наук / Р. И. Вылков. – Екатеринбург, 2009. – 32 с.

31. Гай-Нижник П. Солідаризм як соціально-політична концепція: нарис історії розвитку в Європі та Україні / П. Гай-Нижник // Гілея : наук. вісн. зб. наук. пр. / голов. ред. В. М. Вашкевич. – К., 2011. – Вип. 44. – 784 с.

32. Галета Я. В. Соціальна зрілість особистості в умовах оновлення інформаційної культури суспільства : [монографія] / Я. В. Галета. - Харків : Мачулін, 2018. - 414 с.

33. Гаман-Голутвина О. В. Мировой опыт реформирования систем государственного управления / О. В. Гаман-Голутвина // Вестник МГИМО-Университета [Электронный ресурс]. – Режим доступа : http://www.vestnik.mgimo.ru.

34. Гаман-Голутвина О. Меняющаяся роль государства в контексте реформ государственного управления: отечественный и зарубежный опыт / О. Гаман-Голутвина // Полис. – 2007. – № 4. – С. 46–58.

35. Гидденс Э. Устроение общества: Очерк теории структуризации / Э. Гидденс ; пер. с англ. – М. : Академический проект, 2003. – 526 с.

36. Голобуцкий О. П. Електронний уряд / О. П. Голобуцкий, О. Б. Шевчук. – К. : ЗАТ “Атлант UMS”, 2002. – 174 с.

37. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія / С. Ф. Гончар ; НАН України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. - Київ : Альфа Реклама, 2019. - 175 с.

38. Гриценко О. А. Неформальні інститути в контексті реалізації економічних та соціальних прав людини [Електронний ресурс] / О. А. Гриценко, Ю. І. Золотарьова // Вісник НУЮАУ ім. Я. Мудрого – 2015.

– № 2. – С. 224–239. – Режим доступу : http://nbuv.gov.ua/UJRN/Vnyua_2015_2_25.

39. Даник Ю. Г. Основи кібербезпеки та кібероборони : підручник / Ю. Г. Даник, П. П. Воробієнко. - Одеса : ОНАЗ , 2019. - 320 с.

40. Даниленко С. А. Відкритість та прозорість влади: механізм регулювання взаємодії зі ЗМІ на регіональному рівні : автореф. дис. ... канд. наук з держ. упр. : 25.00.02 / Даниленко Сергій Анатолійович ; Нац. акад. держ. упр. при Президентові України, Одес. регіон. ін-т держ. упр. - Одеса, 2018. - 20 с.

41. Даниленко С. Громадянський вимір комунікаційної революції: модернізація суспільних комунікацій від друкарського верстата до соціальних мереж : монографія / Сергій Даниленко. - К. : ІМВ, 2010. - 312 с.

42. Демкура Т. В. Маркетингові комунікації глобальних компаній мережевого маркетингу: теоретичні та прикладні аспекти : монографія / Т. В. Демкура. - Тернопіль : Підручники і посібники, 2018. - 222 с.

43. Демократія. Антологія / Упор. Олег Проценко. – К. :, Смолоскип, 2005. – XXVIII + 1108 с.

44. Денисова Ж. А. Проблема информационного неравенства в мире / Ж. А. Денисова / /Общество и социология в XXI веке: социальные вызовы и альтернативы: тезисы докл. и выступлений на II Всерос. социол. конгрессе: в 3 т. Т. 2. – М. : Альфа-М, 2003. – С. 11–13.

45. Державне управління : навч. посіб. / А. Ф. Мельник, О. Ю. Оболенський, А. Ю. Расіна. – К. : Знання-Прес, 2003. – 344 с.

46. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / [Д. В. Дубов та ін. ; за заг. ред. Д. Дубова] ; Нац. ін-т стратег. дослідж. - Київ : НІСД, 2018. - 81 с.

47. Дзьобань О. П. Інформаційна безпека у проблемному полі соціокультурної реальності / О. П. Дзьобань . – Харків : Майдан, 2010 . – 259 с.

48. Дзюндзюк Б. В. Віртуальна реальність і публічне управління / Б. В. Дзюндзюк // Теорія та практика державного управління : зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2014. – № 4 (47). – С. 119–126.

49. Дзюндзюк Б. В. Віртуальний простір публічної влади / Б. В. Дзюндзюк // Філософія і психологія публічної влади : [кол. моногр.] / за заг. ред. д.держ.упр., проф. В. Б. Дзюндзюка. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2015. – С. 322–353.

50. Дзюндзюк Б. В. Оцінка готовності державних службовців до роботи в рамках електронного урядування [Електронний ресурс] / Б. В. Дзюндзюк // Теорія та практика державної служби: стратегія реформ 2020 : матеріали VIII Міжнар. наук.-практ. конф., 30 жовт. – 23 листоп. 2015 р. – Режим доступу : http://dridu.dp.ua/konf/konf_dridu/dums_konf_2015/index.html.

51. Дзюндзюк Б. В. Стан і перспективи розвитку у сфері інформатизації в Україні / Б. В. Дзюндзюк // Публічне управління XXI століття: від соціального діалогу до суспільного консенсусу : зб. тез до XIV Міжнар. конгресу. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2014. – С. 109–111.

52. Дзюндзюк В. Б. Ефективність діяльності публічних організацій : монографія / В. Б. Дзюндзюк. – Х. : Вид-во ХарРІ УАДУ «Магістр», 2003. – 236 с.

53. Дзюндзюк В. Б. Інформаційна війна як важлива складова сучасної гібридної війни // XVIII Міжнародний науковий конгрес «Публічне управління XXI століття: світові практики та національні перспективи». – Х. : ХарРІ НАДУ, 2018. – С. 169-172.

54. Дзюндзюк В. Б. Новий публічний менеджмент / В. Б. Дзюндзюк // Актуальні проблеми публічного управління : зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ, 2003. – №1. – С. 76–81.

55. Дзюндзюк В. Б. Публічне управління в Україні: рух з минулого у майбутнє // Актуальні проблеми державного управління. – 2019. – № 1. – С. 8-18.

56. Дзюндзюк В. Б. Вплив глобалізації на сучасну державу / В. Б. Дзюндзюк // Державне будівництво. – 2018. – Режим доступу : http://www.kbuapa.kharkov.ua/e-book/db/2018-2/doc/1/1_1.pdf.

57. Дзюндзюк В. Б. Демократичне врядування : навч. посіб. / В. Б. Дзюндзюк. – Х. : ХарРІ НАДУ, 2019. – 203 с.

58. Дубас О. П. Інформаційно-комунікаційний простір: поняття, сутність, структура / О. П. Дубас // Сучасна українська політика. Політики і політологи про неї. – К., 2010. – № 19. – С. 223–232.

59. Дубов Д. В. Стратегічні аспекти кібербезпеки України / Д. В. Дубов // Стратегічні пріоритети. – 2013. – № 4. – С. 119–127.

60. Дятлов С. А. Принципы информационного общества / С. А. Дятлов // Информационное общество. – 2000. – № 2. – С. 77–85.

61. Електронне урядування : підручник / [А. І. Семенченко та ін. ; за заг. ред. Н. В. Грицяк, А. І. Семенченка] ; Нац. акад. держ. упр. при Президентові України. - Київ : НАДУ, 2016. - 127 с.

62. Еллинек Г. Общее учение о государстве / Г. Еллинек. – СПб.: Юрид. центр Пресс, 2004. – 532 с.

63. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / [І. Є. Антіпов та ін.] ; Харків. нац. ун-т радіоелектроніки. - Харків : ХНУРЕ, 2019. - 215 с.

64. Згуровський М. З. Розвиток інформаційного суспільства в Україні: Правове регулювання у сфері інформаційних відносин / М. З. Згуровський, М. К. Родіонов, І. Б. Жиляєв ; Національний техніч. ун-т України «Київський політехнічний ін-т». – К. : НТУУ «КПІ», 2006. – 544 с.

65. Зіллер Ж. Політико-адміністративні системи країн ЄЕС. Порівняльний аналіз / Ж. Зіллер ; пер. з фр. В. Ховхуна. – К. : Основи, 1996. – 420 с.

66. Иванов Д. В. Виртуализация общества / Д. В. Иванов. – СПб. : Петербургское Востоковедение, 2000. – 96 с.

67. Иноземцев В. Л. Современное постиндустриальное общество: природа, противоречия, перспективы : учеб. пособие для студентов вузов / В. Л. Иноземцев. – М. : Логос, 2000. – 304 с.

68. Іванов В. Ф. Медіаосвіта та медіаграмотність: визначення термінів / В. Ф. Іванов, О. Я. Шкоба // Інформаційне суспільство. – 2012. – №16. – С. 41–52.

69. Інформаційно-аналітичне забезпечення органів місцевої влади : навч. посібник / [В. М. Дрешпак та ін.] ; заг. ред. В. М. Дрешпак ; Національна академія держ. управління при Президентові України ; Дніпропетр. регіон. ін-т держ. упр. – Дніпропетр. : ДРІДУ НАДУ, 2007. – 160 с.

70. Карамишев Д. В. Формування системи цінностей і переконань як чинник інститутуціональних перетворень в українському суспільстві / Д.В. Карамишев // Теорія та практика державного управління: зб.наук.пр. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2016. – Вип. 1(52). – С. 6-14.

71. Карпенко В. П. Інформаційна політика та безпека : підручник для вузів / В. П. Карпенко . – Київ : НОРА-ДРУК, 2006 . – 318 с.

72. Кастельс М. Информационная эпоха: экономика, общество, культура / М. Кастельс. – М. : ГУ ВШЭ, 2000. – 606 с.

73. Кастельс М. Інтернет-галактика. Міркування щодо Інтернету, бізнесу і суспільства / М. Кастельс ; [пер. з англ.]. – К. : Ваклер, 2007. – 304 с.

74. Кастельс М. Інформаційне суспільство та держава добробуту. Фінська модель / М. Кастельс, П. Хіманен ; пер. з англ. – К. : Ваклер, 2006. – 230 с.

75. Кастельс М. Становление общества сетевых структур / М. Кастельс // Новая постиндустриальная волна на Западе. Антология ; под ред. В. Л. Иноземцева. – М. : Academia, 1999. – 640 с.

76. Кириченко В. В. Особистість у сучасному інформаційному суспільстві : монографія / Кириченко В. В. ; Ін-т психології ім. Г. С. Костюка НАПН України, Житомир. держ. ун-т ім. Івана Франка. - Житомир : Вид-во

ЖДУ ім. І. Франка, 2020. - 244 с.

77. Кібербезпека мереж наступного покоління : навч. посіб. у галузі знань 1701 "Інформаційна безпека" за спец. 8.17010201 - Системи технічного захисту інформації, автоматизація її обробки / О. О. Вараксін [та ін.] ; за ред. чл.-кор. МАЗ В. Г. Кононовича ; Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. - О. : ОНАЗ ім. О. С. Попова, 2013. - 238 с.

78. Клименко І. В. Складові ефективності електронного врядування / І. В. Клименко // Інвестиції: практика та досвід. – 2010. – № 16. – С. 92–94.

79. Князєв В. М. Державне управління: філософські, світоглядні та методологічні проблеми / В. М. Князєв. – К. : Вид-во НАДУ – Міленіум, 2003. – 320 с.

80. Колот А. М. Соціальна згуртованість як доктрина забезпечення стійкості розвитку суспільства в умовах глобальних викликів / А. М. Колот // Україна: аспекти праці: наук.-екон. та сусп.-політ. журн. – 2009. – № 7. – С. 11–19.

81. Комаровський В. В. Мотивація посадових осіб органів публічної влади при запровадженні сервісів е-урядування / [В. В. Комаровський, В. А.Яценко, В. І. Бондарук та ін.] // Теоретичні та прикладні питання державотворення. – 2012. – № 10. – С. 1–56.

82. Конвенція про кіберзлочинність. Офіційний переклад [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575.

83. Корж І.Ф. Веб-сайти органів державної влади та органів місцевого самоврядування: механізми доступу до публічної інформації // Інформація і право. – 2018. – № 2 (25). – URL. : http://ippi.org.ua/korzh-if-veb-saiti-organiv-derzhavnoi-vladi-ta-organiv-mistsevogo-samovryaduvannya-mekhanizmi-dostup

84. Корженко В. В. Методологічні та евристичні інтенції сучасної концепції Governance [Електронний ресурс] / В. В. Корженко, В. В. Нікітін // Державне будівництво. – 2006. – № 1. – Режим доступу :

http://www.nbuv.gov.ua/e-journals/DeBu/e-book/doc/1/01.pdf.

85. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навчальний посібник для вузів / Б. А. Кормич . – Київ : Кондор, 2008 . – 382 с.

86. Корнієнко Б. Я. Безпека інформаційно-комунікаційних систем та мереж : навч. посіб. для студентів спец. 125 "Кібербезпека" / Б. Я. Корнієнко ; Нац. авіац. ун-т. - Київ : НАУ, 2018. - 225 с.

87. Котковський В. Р. Вплив інформаційних технологій на розвиток місцевих співтовариств / В. Р. Котковський // Державне управління та місцеве самоврядування: сучасні вектори розвитку : зб. тез науково-практичної конференції, Харків, 24 вересня 2014 р. [Електронний ресурс]. – Режим доступу : http://kbuapa.kharkov.ua/e-book/conf/2014-3/doc/3/02.pdf.

88. Котковський В. Р. Інформаційно-аналітичне забезпечення прийняття управлінських рішень в діяльності органів державної влади / В. Р. Котковський // Теорія та практика державного управління: зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ “Магістр”, 2015. – Вип. 4 (51). – С. 132 – 137.

89. Котух Є. Боротьба з кіберзлочинністю в країнах ЄС / Є. Котух // Матеріали 18-ї регіональної науково-практичної конференції «Актуальні проблеми європейської та євроатлантичної інтеграції України» (м. Дніпро, 13 травня 2021 р.). – Дніпро : ДРІДУ НАДУ. – С. 114-117.

90. Котух Є.В. Аудит інформаційної безпеки як необхідна складова управління в державних установах / Є.В. Котух, О.М. Кучма, Д.М. Нехороших, Г.В. Пліс, Г.З. Халімов // Державне будівництво. – 2021. – № 1. – Режим доступу: https://db.kh.ua/index.php/db/article/view/117/110.

91. Котух Є.В. Електронне урядування як нова парадигма публічного управління / Є.В. Котух // Інвестиції: практика та досвід. – 2020. – № 3, лютий. – С. 122-127.

92. Котух Є.В. Електронний уряд і кібербезпека у соціальних мережах: особливості реалізації // Вісник НУЦЗ України. Серія: Державне управління. – 2020. – № 2. – С. 564-572.

93. Котух Є.В. Кібербезпека у публічному секторі : монографія / Є.В. Котух. – Харків : Колегіум, 2021. – 272 с.

94. Котух Є.В. Кібербезпека як один з пріоритетів національної політики / В.Б. Дзюндзюк, Є.В. Котух // Державне будівництво. – 2020. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/download/90/85.

95. Котух Є.В. Кіберзагрози у сучасному світі / В.Б. Дзюндзюк, Є.В. Котух // International Scientific Integration ‘2020 (Seattle, Washington, USA, November 10, 2020). – Pp. 103-106.

96. Котух Є.В. Національні стратегії кібербезпеки: економіко-політичний аспект / Є.В. Котух // Multidisziplinare Forschung: Perspektiven, Probleme und Muster (Wien, 09.04.2021). – Pp. 49-50.

97. Котух Є.В. Національні стратегії кібербезпеки: порівняльний аналіз / Є.В. Котух // Актуальні проблеми державного управління. – 2021. – № 1. – С. 48-57.

98. Котух Є.В. Основні виклики врядування у сфері кібербезпеки / Є. Котух, В. Ободяк // Теорія та практика державного управління. – 2020. – № 4 (71). – С. 38-46.

99. Котух Є.В. Основні підходи до забезпечення кібербезпеки: досвід країн вишеградської четвірки // Інвестиції: практика та досвід. – 2021. – № 3. – С. 68-74.

100. Котух Є.В. Особливості забезпечення кібербезпеки в публічному секторі в умовах глобалізації / Є.В. Котух // Державне будівництво. – 2019. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/view/65/60.

101. Котух Є.В. Особливості національної та регіональної політики у сфері кібербезпеки / Є.В. Котух // Теорія та практика державного управління. – 2019. – № 4(67). – С. 40-47.

102. Котух Є.В. Оцінка рівня захисту кіберпростору в публічному управлінні: національний та організаційний виміри / Є.В. Котух // Теорія та

практика державного управління. – 2021. – № 1. – С. 31-39.

103. Котух Є.В. Проблема кібершахрайства та фактори стримування її вирішення органами публічного управління / Є.В. Котух. // Вісник НУЦЗ України. Серія: Державне управління. – 2021. – Випуск 1 (14). – С. 185-191.

104. Котух Є.В. Проблеми кібербезпеки в сучасному світі // Актуальні проблеми державного управління. – 2019. – №2(56). – С. 33-38.

105. Котух Є.В. Проблеми урядування у сфері кібербезпеки / В.Б. Дзюндзюк, Є.В. Котух // Abstracts of scientific papers of IV International Scientific Conference «Science and Global Studies» (Prague, November 30, 2020). – Pp. 25-28.

106. Котух Є.В. Реалізація національних стратегій кібербезпеки: силовий аспект // Наукові перспективи. – 2021. – № 2(8). – С. 125-136.

107. Котух Є.В. Реалізація стратегій кібербезпеки: економіко-політичний аспект / Є.В. Котух // Теорія та практика державного управління. – 2021. – № 2. – С. 125-136.

108. Котух Є.В. Ризики зростання відкритості публічного сектору та засоби боротьби з ними / Котух Є.В. // Збірник тез XX Міжнародного наукового конгресу «Публічне управління XXI століття: портал можливостей» (м. Харків, 23 квітня 2020 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2020. – С. 103-106.

109. Котух Є.В. Розвиток публічно-приватного партнерства у сфері кібербезпеки // Інвестиції: практика та досвід. – 2021. – № 13. – С. 76-84.

110. Котух Є.В. Сучасний стан та проблеми «цифровізації» в Україні / Є.В. Котух, А.С. Довбиш // Актуальні проблеми державного управління. – 2020. – № 2. – С. 25-31.

111. Котух Є.В. Теоретико-методологічна модель розробки національної стратегії кібербезпеки / Є.В. Котух // Наукові перспективи. – 2021. – № 6 (12). – С. 39-52.

112. Котух Є.В. Типи владних відносин у стратегії кібербезпеки / Є.В. Котух // Інвестиції: практика та досвід. – 2021. – № 11. – С. 98-102.

113. Котух Є.В. Формування систем кібербезпеки в органах публічної влади / Є.В. Котух // Державне управління: удосконалення та розвиток. – 2020. – № 3, березень. – Режим доступу: http://www.dy.nayka.com.ua/pdf/3_2020/32.pdf.

114. Котух Є.В. Щодо питання реалізації національних стратегій кібербезпеки / Котух Є.В. // Збірник тез XXI Міжнародного наукового конгресу «Публічне управління XXI століття: погляд у майбутнє» (м. Харків, 21 квітня 2021 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2021. – С. 161–165.

115. Кравець М. С. Культурологія. Розвиток культури в інформаційному вимірі : підручник / Кравець М. С. - Львів : Новий Світ-2000, 2019. - 259 с.

116. Кремлева С. О. Сетевые сообщества [Электронный ресурс] / С. О. Кремлева. – Режим доступа : http://www.follow.ru/print.php?id=116&page=1.

117. Крозье М. Современное государство – скромное государство / М. Крозье // Свободная мысль. – 2003. − № 11. – С. 56–67.

118. Крюков О. І. Публічні інформаційні ресурси та публічна інформація [Електронний ресурс] / О. І. Крюков, С. І. Петраков. – Режим доступу : https://docs.google.com/file/d/0B5PLeqrlVLsId19WN1VZODkzS1U.

119. Кудрявцев О. Ю. Електронне урядування у сучасному політико-адміністративному просторі : монографія / О. Ю. Кудрявцев ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. - Харків : ХНУМГ ім. О. М. Бекетова, 2016. - 184 с.

120. Курбан О. В. Інформаційні війни у соціальних он-лайн-мережах : [монографія] / Курбан О. В. ; Київ. ун-т ім. Бориса Грінченка. - Київ : Київ. ун-т ім. Бориса Грінченка, 2017. - 392 с.

121. Куц Ю. О. Природа та сутність державного управління / Ю. О. Куц // Теорія та практика державного управління і місцевого самоврядування [Електронне наукове фахове видання]. – 2013. – № 1. – Режим доступу :

http://nbuv.gov.ua/UJRN/Ttpdu_2013_1_24.

122. Ланде Д. В. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки : навч. посіб. / Д. В. Ланде, І. Ю. Субач, Ю. Є. Бояринова ; Ін-т спец. зв'язку та захисту інформації Нац. техн. ун-ту України "Київ. політехн. ін-т ім. Ігоря Сікорського". - Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. - 300 с.

123. Лахижа М. І. Модернізація публічної адміністрації: теоретичні та практичні аспекти : [монографія] / М. І. Лахижа. – Полтава : РВВ ПУСКУ, 2009. – 289 с.

124. Лебедев П. А. Социальные медиа: показатель развития информационного общества? / П. А. Лебедев, С. И. Петухова // Мониторинг общественного мнения. – 2010. – № 5. – С. 18–19.

125. Лещев С. В. Коммуникативное, следовательно, коммуникационное / С. В. Лещев // Вестник Российского университета дружбы народов. – 2002. – № 3. – С. 14–29.

126. Лизанчук В.В. Інформаційна безпека України: теорія і практика : підручник / В.В. Лизанчук . – Львів : Видавничий центр Львівського національного університету ім. І.Франка, 2017 . – 726 с.

127. Литвиненко О. О. Особливості сучасного етапу еволюції мультимедійного середовища / О. О. Литвиненко // Вісник Харківської державної академії культури. – 2011. – № 33. – С. 179–190.

128. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський . – Київ : КНТ, 2006 . – 279 с.

129. Лісовська Ю. П. Інформаційна безпека України : навчальний посібник / Ю. П. Лісовська . – Київ : Кондор, 2018 . – 170 с.

130. Лук’янчук Р. В. Державне управління у сфері забезпечення кібербезпеки України : автореф. дис. ... канд. наук з держ. упр. : 25.00.01 / Лук'янчук Руслан Валерійович ; Ін-т законодавства Верхов. Ради України. - Київ, 2017. - 19 с.

131. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст / Є. А. Макаренко // Актуальні проблеми міжнародних відносин. – 2011. – № 102. – С. 51–62.

132. Маклюэн М. Понимание Медиа: Внешние расширения человека / М. Маклюэн. – М. : КАНОН-пресс-Ц, 2003. – 464 с.

133. Мартиненко В. М. Нова парадигма публічного управління – об'єктивний імператив XXI століття (теоретико-методологічний аспект) / В. М. Мартиненко // Публічне управління: теорія та практика. – 2011. – № 3(7). – С. 4–16.

134. Марущак А. І. Особливості обробки та захисту персональних даних у мережі Інтернет: європейський досвід та законодавство України / А. І. Марущак, К. С. Мельник // Інформаційна безпека людини, суспільства, держави. – 2013. – № 3. – С. 19–24.

135. Марченко В. В. Електронне урядування в органах виконавчої влади : підручник / В. В. Марченко ; Харків. нац. пед. ун-т ім. Г. С. Сковороди. - Харків : Вид-во ХНАДУ, 2018. - 291 с.

136. Машкаров Ю. Г. Електронне місто – інформатизація місцевого самоурядування (на прикладі м. Харкова) / Ю. Г. Машкаров, Д. І. Палашевський // Актуальні проблеми державного управління. – 2012. – № 41. – С. 26–35.

137. Мей К. Інформаційне суспільство: Скептичний погляд / К. Мей. – пер. М. Войцицька. – К. : К.І.С., 2004. – 220 с.

138. Михеев А. Н. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности / А. Н. Михеев // Современные глобальные проблемы мировой политики : учеб. пособие для студентов вузов ; под ред. М. М. Лебедевой. – М. : Аспект Пресс, 2009. – 230 с.

139. Міжнародні стандарти з кібербезпеки та їх застосування в Україні : матеріали "круглого столу" (м. Харків, 19 квіт. 2016 р.) / Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. кримінології та кримін.-викон. права ; за ред. А. П.

Гетьмана, Б. М. Головкіна. - Харків : Право, 2016. - 87 с.

140. Міненко М. А. Трансформація системи державного управління в сучасні моделі регулювання суспільства / М. А. Міненко // Державне управління: удосконалення та розвиток [Електронне наукове фахове видання]. – К. : Академія муніципального управління, 2013. – № 6. – Режим доступу : http://www.dy.nayka.com.ua/?op=1&z=581.

141. Мэннинг Н. Реформа государственного управления. Международный опит / Н. Мэннинг, Н. Паркинсон. – М. : Весь мир. 2003. – 496 с.

142. Назаров М. М. Массовая коммуникация и общество: Введение в теорию исследования / М. М. Назаров. – М. : Книжный дом «Либроком», 2010. – 428 с.

143. Національна рада України з питань телебачення і радіомовлення [Електронний ресурс]. – Режим доступу : http://www.nrada.gov.ua.

144. Нижник Н. Р. Модернізація Української держави як передумова соціальної ефективності державного управління / Н. Р. Нижник, Л. А. Пашко // Наукові записки Інституту законодавства Верховної Ради України. – 2010. – № 1/2010. – С. 100–106.

145. Новак-Каляєва Л. М. Сучасні тенденції до конвергенції в концепціях державного управління / Л. М. Новак-Каляєва // Вісник НАДУ при Президентові України. – 2013. – № 1. – С. 29–41.

146. Носов Н. А. Манифест виртуалистики [Електронний ресурс] / Н. А. Носов. – Режим доступу : http://www.virtualistika.ru/vip_15.html

147. Огірко І. В. Оцінка якості надання адміністративних послуг / І. В. Огірко, А. Й. Серант // Ефективність державного управління. – 2015. – № 42. – С. 149–161.

148. Олійник Д. В. Ефективна держава: сутність, зміст, особливості / Д. В. Олійник // Актуальні проблеми державного управління : зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ «Магістр». – 2011. – № 2 (40). – С. 60–68.

149. Орлов О. В. Актуальні напрями державної політики України у

сфері боротьби з кіберзлочинністю / О. В. Орлов // Актуальні проблеми державного управління. – 2013. – № 3. – С. 1–6.

150. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. - Київ : Ліра-К, 2020. - 554 с.

151. Оцінка електронної готовності України Державним агентством з питань електронного урядування [Електронний ресурс]. – Режим доступу : http://www.dknii.gov.ua/sites/default/files/dodatok_5.pdf.

152. Павлютенкова М. Ю. Электронное правительство: западный опыт в российской проекции [Электронный ресурс] / М. Ю. Павлютенкова. – Режим доступа : http://conf.infosoc.ru/2006/thes/Pavlyutenkova.pdf.

153. Паркинсон С. Н. Законы Паркинсона / С. Н. Паркинсон. – М. : Прогресс, 1989. – 247 с.

154. Парсонс Т. О социальных системах / Т. Парсонс. – М. : Академический проект, 2002. – 832 с.

155. Петровський П. М. Гуманітарна парадигма в системі державного управління: [монографія] / П. М. Петровський. – Львів : ЛРІДУ НАДУ, 2008. – 251 с.

156. Політична енциклопедія / редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. – К. : Парлам. вид-во, 2011. – 808 с.

157. Попов С. А. Державно-управлінські нововведення: теорія, методологія, практика : монографія / С. А. Попов. – Одеса : ОРІДУ НАДУ, 2014. – 296 с.

158. Почепцов Г. Г. Від Facebook-у і гламуру до WikiLeaks: медіакомунікації / Г. Г. Почепцов. – К. : Спадщина-інтеграл, 2012. – 464 с.

159. Про адміністративні послуги : Закон України від 06.09.2012 р. № 5203-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/5203-17.

160. Про державну таємницю : Закон України від 21.01.1994 р. №3855-XII [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/3855-12.

161. Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади : Указ Президента України від 01.08.2002 р. № 683/2002 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/683/2002.

162. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2939-17.

163. Про електронний цифровий підпис : Закон України від 22.05.2003 р. № 852-IV [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/852-15.

164. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/851-15.

165. Про запровадження електронного сервісу для платників податків – юридичних осіб : Наказ Державної податкової адміністрації України від 11.02.2011 р. № 85 [Електронний ресурс]. – Режим доступу : http://www.tax.gov.ua/elektronna-zvitnist/platnikam-podatkiv-pro/povidomlennya-platnikam-pod/58694.html.

166. Про запровадження Національної системи індикаторів розвитку інформаційного суспільства : постанова Кабінету Міністрів України від 28.11.2012 № 1134 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1134-2012-%D0%BF.

167. Про затвердження Методики формування індикаторів розвитку інформаційного суспільства : Наказ МОН України від 06.09.2013 р. № 1271 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/z1664-13.

168. Про затвердження плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 26 вересня 2011 р. № 1014-р [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1014-2011-%D1%80.

169. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : постанова Кабінету Міністрів України від 21 жовтня 2015 р. № 835 [Електронний ресурс]. – Режим доступу : http://www.kmu.gov.ua/control/ru/cardnpd?docid=248573101.

170. Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг : постанова Кабінету Міністрів України від 3.01.2013 р. № 13 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/13-2013-%D0%BF.

171. Про затвердження Порядку ведення Реєстру адміністративних послуг : постанова Кабінету Міністрів України від 30.01.2013 р. № 57 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/57-2013-%D0%BF.

172. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

173. Про захист недоторканності приватного життя в Інтернеті : Рекомендація Комітету Міністрів Ради Європи державам-членам Ради Європи від 23.02.1999 р. № R(99)5 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_357.

174. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2297-17.

175. Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» : постанова Кабінету Міністрів України від 24.02.2003 р. № 208 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/208-2003-%D0%BF.

176. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2657-12.

177. Про Національну програму інформатизації : Закон України від

04.02.1998 р. № 74/98-ВР [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

178. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/964-15.

179. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII // ВВР України. – 2017. – № 45. – Ст. 403.

180. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.2007 р. № 537-V [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/537-16.

181. Про платіжні системи та переказ коштів в Україні : Закон України від 05.04.2001 р. № 2346-III [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2346-14.

182. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 13 грудня 2010 р. № 2250-р [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2250-2010-%D1%80.

183. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р [Електронний ресурс]. – URL. : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text.

184. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/386-2013-%D1%80.

185. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV [Електронний ресурс]. – Режим доступу :

http://zakon4.rada.gov.ua/laws/show/1280-15.

186. Проблеми суспільної безпеки в процесі розвитку соціальних мереж : [монографія] / [В. І. Попик (керівник проекту) та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. - Київ : НБУ ім. В. І. Вернадського, 2015. - 199 с.

187. Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід : монографія / Запоріз. держ. інж. акад. ; за заг. ред. Сергія Чернова [та ін.]. - Запоріжжя : ЗДІА, 2017. - 602 с.

188. Райнхард К. Реформирование государственного управления. Концепция активизирующего государства / К. Райнхард // Реформы государственного управления накануне третьего тысячелетия: сб. статей. – М. : РАГС, 1999. – С. 8–10.

189. Решота В. В. Основні концепції реформування державного управління США та Європейського Союзу / В. В. Решота В. В. Решота // Демократичне урядування. – 2010. – № 6. – С 8–17.

190. Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : автореф. дис ... канд. політ. наук: 23.00.02 / О. М. Рижук . – Чернівці, 2019 . – 20 с.

191. Рубанець О. М. Інформаційне суспільство: когнітивний креатив постнекласичних досліджень : монографія / О. М. Рубанець. – К. : Видавець ПАРАПАН, 2006. – 419 с.

192. Семенченко А. І. Механізми державного управління у сфері зв’язку та інформатизації: теоретико-методологічні засади / А. І. Семенченко // Стратегічні пріоритети. – 2015. – №4. – С. 65–73.

193. Семенченко А. І. Сучасні проблеми підвищення рівня професійної компетентності публічних службовців України щодо технологій електронного урядування / А. І. Семенченко, І. Б. Жиляєв, Т. О. Власюк // Стратегічні пріоритети. – 2016. – №1. – С. 31–42.

194. Семенченко А. І. Теоретико-методологічні основи організаційно-

правових механізмів навчання публічних службовців електронному урядуванню / А. І. Семенченко, Р. В. Власенко // Аспекти публічного управління. – 2015. – № 1–2. – С. 88–95.

195. Серенок А. О. Сервісна електронна взаємодія в системі електронного уряду / А. О. Серенок // Актуальні проблеми державного управління. – 2010. – № 1. – С. 153–161.

196. Сєров Ю. О. Соціальні комунікації в мережі Internet : навч. посіб. / Ю. С. Сєров, С. С. Федушко ; Нац. ун-т "Львів. політехніка". - Львів : Вид-во Львів. політехніки, 2017. - 235 с.

197. Сивиринов Б. С. Социальная квазиреальность или виртуальная реальность? [Электронный ресурс] / Б. С. Сивиринов. – Режим доступа : http://www.isras.ru/files/File/Socis/2003-02/Siviriniv_2.pdf.

198. Сінґер П. В. Війна лайків. Зброя в руках соціальних мереж / П. В. Сінґер, Емерсон Т. Брукінґ ; [пер. з англ. Я. Лебеденко]. - Харків : Клуб Сімейного Дозвілля, 2019. - 319 с.

199. Скородумова О. Б. Культура информационного общества / О. Б. Скородумова. – М., 2004. – С. 67–68.

200. Словник термінів з кібербезпеки / Рада нац. безпеки і оборони України, Міжвідом. н.-д. центр з пробл. орг. злочинності, Нац. акад. СБУ, Навч.-наук. ін-т інформ. безпеки ; [уклад.: Бутузов В. М. та ін. ; за заг. ред. Копана О. В., Скулиша Є. Д.]. - К. : ВБ "Аванпост-Прим", 2012. - 214 с.

201. Смирнов А. А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза : монографія / А. А. Смирнов. – М. : ЮНИТИ-ДАНА, 2011. – 150 с.

202. Сморгунов Л. В. Сетевой подход к политике и управлению / Л. В. Сморгунов // Политические исследования. – 2001. – № 3. – С. 103–112.

203. Станіславський Т. В. Механізми публічного управління забезпечення кібербезпеки в сучасних умовах : автореф. дис. ... канд. наук з держ. упр. : 25.00.02 / Станіславський Тарас Володимирович ; Ін-т підгот. кадрів держ. служби зайнятості України. - Київ, 2020. - 20 с.

204. Станкевич Л. Т. Электронное правительство: теоретические модели и реальная практика / Л. Т. Станкевич, Н. О. Новоженина // Технологии информационного общества – Интернет и современное общество: тр. VI Всерос. объединенной конф. – 2003. – С. 128–129.

205. Степанов В. Ю. Механізми формування та реалізації державної інформаційної політики в сучасних умовах / В. Ю. Степанов // Держава та регіони. – 2010. – № 2. – С. 122–126.

206. Стерледева Т. Д. Электронно-виртуальная реальность как новая ниша человеческого существования: философский прогноз / Т. Д. Стерледева // Вызовы современности и философия : материалы «Круглого стола», посвященного Дню философии ЮНЕСКО. – 2004. – С. 164–172.

207. Тенденции развития преступлений в области высоких технологий [Электронный ресурс]. – Режим доступа : http://report2014.group-ib.ru.

208. Теннис Ф. Общность и общество / Ф. Теннис. – М. : Фонд «Университет», 2002. – 456 с.

209. Теорія та історія публічного управління : навч. посібник / [Г. С. Одінцова, В. Б. Дзюндзюк, Н. М. Мельтюхова та ін.]. – К. : Професіонал, 2008. – 288 с.

210. Тоффлер Э. Революционное богатство / Э. Тоффлер. – М. : АСТ, 2008. – 569 с.

211. Тронь В. П. Комп’ютерна підтримка прийняття рішень на різних рівнях державного управління : метод. реком. та зб. завдань / В. П. Тронь. – К. : Вид-во УАДУ, 1998. – 55 с.

212. Турен А. Возвращение человека действующего. Очерк социологии / А. Турен. – М. : Научный мир, 1998. – 204 с.

213. Туронок С. Г. Субкультура Интернет-сообществ / С. Г. Туронок // Культура России как ее стратегический ресурс. Тетради Международного университета (в Москве) : сб. научных трудов. – 2004. – № 2. – С. 209–214.

214. Уилби П. Концепции публичной политики, связей с общественностью и публичной коммуникации / П. Уилби. – [Электронный

ресурс]. – Режим доступа : http://www.nscs.ru/docs/Peter_Wilby.doc.

215. Федосеева Н. Н. Демократия в информационном обществе / Н. Н. Федосеева // Журнал российского права. – 2007. – № 6. – С. 27–32.

216. Фионова Л. Р. Оценка готовности государственных служащих к работе в электронном правительстве / Л. Р. Фионова // Теория и практика общественного развития. – 2014. – № 1. – С. 73–77.

217. Харченко Л.С. Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов ; За заг. ред. Р. А. Калюжний . – Київ : Текст, 2004 . – 135 с.

218. Хомяков В. І. Формування людського капіталу: результати і тенденції / В. І. Хомяков // Збірник наукових праць Черкаського державного технологічного університету. – 2014. – № 36. – С. 5–19.

219. Храмцовская Н. А. Открытое правительство США: основные идеи и практическая реализация [Электронный ресурс] / Н. А. Храмцовская. – Режим доступа : http://ojs.ifmo.ru/index.php/IMS/article/viewFile/126/126.

220. Хэмит Ф. Виртуальная реальность (дайджест книги) / Ф. Хэмит [Электронный ресурс]. – Режим доступа : http://www.aquarun.ru/aquarius/hemit.html.

221. Чиж І. С. Конституційно-правові засади забезпечення права на поширення інформації в процесі формування інформаційного та громадянського суспільства / І. С. Чиж // Держава і право. Юридичні і політичні науки. – 2013. – № 59. – С. 529–534.

222. Чиж І. С. Україна: шлях до інформаційного суспільства / І. С. Чиж. – К. : Либідь, 2004. – 288 с.

223. Член правления Ericsson, Sony и GlobalLogic – о потенциале Украины в IT [Электронный ресурс]. – Режим доступа : http://ain.ua/2015/10/02/607251.

224. Чукут С. А. Смарт-сіті чи електронне місто: сучасні підходи до розуміння впровадження е-урядування на місцевому рівні / С. А. Чукут, В. І. Дмитренко // Інвестиції: практика та досвід. – 2016. – № 13. – С. 89–93.

225. Чукут С. Сутність електронного уряду та принципи його організації / С. Чукут // Вісн. УАДУ. – 2003. – № 2. – С. 429–433.

226. Шамрай В. В. Модерне суспільство: від ліберальної і тоталітарної утопій до мережної соціальності : [монографія] / В. В. Шамрай ; НАН України, Ін-т філософії ім. Г. С. Сковороди. - Київ : НАН України, 2015. - 305 с.

227. Штомпка П. Социология. Анализ современного общества / П. Штомпка. – М. : Логос, 2005. – 664 с.

228. Щорічна доповідь Державного агентства з питань електронного урядування [Електронний ресурс]. – Режим доступу : http://www.dknii.gov.ua/sites/default/files/dodatok_1_0.docx.

229. Юдін О. К. Інформаційна безпека держави : Навч. посібник для вузів /О. К. Юдін, В. М. Богуш . – Харків : Консум, 2005 . – 576 с.

230. Accenture (2002), “E-government Leadership - Realizing the Vision”. April 2002. Available at: www.accenture.com/xd/xd.asp?it=enWeb &xd=industries%5 Cgovernment%5Cgove_welcome.xml.

231. Adelmann B., “Cispa is big brother‘s friend,” 2012.

232. AG (2009) Cyber Security Strategy, Office of the Attorney General, Australia, available at http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity#h2strategy.

233. Alexander S., “Rise of outsourcing poses new cybersecurity problems,” 2011.

234. Anderson, R. H., & Anthony, H. (1996). An exploration of cyberspace security R&D investment strategies for DARPA: “The day after... in cyberspace II”.

235. APCOForum.com. (2013, Jun.) The cyber security challenge: The risk of inaction. [Online]. Available: www.apcoforum.com

236. Asllani, A., White, C. S., & Ettkin, L. (2012). Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. Allied

Academies International Conference: Proceedings Of The Academy Of Legal, Ethical & Regulatory Issues (ALERI), 16(1), 1-2.

237. Axelrod, Robert/Keohane, Robert O. (1993): “Achieving Cooperation Under Anarchy: Strategies and Institutions”, in: David A. Baldwin (Ed.): Neorealism and Neoliberalism: The Contemporary Debate, New York: Columbia University Press, 85-115.

238. Baker, Stewart/Waterman, Shaun/Ivanov, George (2019): In the Crossfire: Critical Infrastructure in the Age of Cyberwar, Santa Clara, CA: McAfee, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure- cyber-war.pdf.

239. Barlow, J. P. 1996. "A Declaration of the Independence of Cyberspace". Accessed January 11, 2018. https://projects.eff.org/~barlow/Declaration-Final.html.

240. Barnett, Michael, and Raymond Duvall (2005), ‘Power in International Politics’, *International Organization*, Vol.59, No.1, pp.39-75.

241. Barzilay M.. (2013, May) A simple definition of cybersecurity. [Online]. Available: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

242. Bauer, Johannes M., and Michel J.G. van Eeten (2009), ‘Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options’, *Telecommunications Policy*, Vol.33, Nos.10-11, pp.706-719.

243. Bendiek A (2012) European cybersecurity policy. SWP website www. swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf.

244. Bhatnagar, S.C. (2001), “Philippine Customs Reform.” World Bank. Washington, DC. Available at: <http://www1.worldbank.org/publicsector/ egov/philippinecustomscs.htm>

245. Billo, Charles/Chang, Welton (2020): Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States, Institute for Security Technology Studies at Dartmouth College, Hanover, NH.

246. Black. (1971). Black, J., Concurring Opinion, Supreme Court of the

United States 403 U.S. 713 New York Times Co. v. United States Certiorari to the United States Court of Appeals for the Second Circuit No. 1873. Argued: June 26, 1971; decided: June 30, 1971.

247. Blair, Admiral D. (2011). “Cybersecurity Address.” U.S. Naval Academy Foreign Affairs Conference (April 15).

248. Blakemore, M., and Lloyd, P. (2007). “Trust and transparency: Pre-requisites for effective eGovernment,” Citizen-Centric eGovernment Think Paper, 2007: 10.

249. BMI (2011b) Cyber Security Strategy for Germany, Federal Ministry of the Interior (Bundesministerium des Innern), Berlin, Germany, available at http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Sicherheit/css_engl_download.pdf?__blob=publicationFile.

250. Booz Allen Hamilton. (2009). “Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce,” Partnership for Public Service, July 2009: http://www.ourpublicservice.org.

251. Borg S (2005) Economically complex cyberattacks. Secur Priv 3(6):64-67

252. Bovaird, T and Loffler, E. 2003. Public Management and Governance. London: Routledge.

253. Bovens, M., and Loos, E. (2002). “The digital constitutional state: Democracy and law in the information society,” Information Policy, Vol. 7, No. 4, 2002, pp. 16, 185-197.

254. Brechbuhl, Hans, Robert Bruce, Scott Dynes, and M. Eric Johnson (2010), ‘Protecting Critical Information Infrastructure: Developing Cybersecurity Policy’, *Information Technology for Development*, Vol.16, No.1, pp.83-91.

255. Broad, W. J. et al. (2011). “Israeli Test on Worm Called Crucial in Iran Nuclear Delay.” New York Times (January 15), p. 1A.

256. Brown, David (2005), “Electronic government and public administration”. International Review of Administrative Sciences. Vol. 71 (2): 241-254, London, Thousand Oaks, CA and New Delhi: Sage Publications

257. Brown, Douglas (1999), “Information Systems for Improved Performance Management: Development Approaches in U.S. Public Agencies. In Reinventing Government in the Information Age, edited by Richard Heeks, 113-34. London and New York: Routledge.

258. BSA (Business Software Alliance). 2010. BSA Global Cybersecurity Framework. Washington, DC, USA: Business Software Alliance (BSA).

259. Bundesministerium des Innern, (2011) "Cyber-Sicherheitsstrategie fur Deutschland" [online] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OEDVerwaltung/Informationsgesellschaft/cyber.pdf ? blob=publicationFile.

260. Burg, D. (2015). Top findings: Escalating concern over cyber threats has CEOs warming to government collaboration. Retrieved from http://www.pwc.com/us/en/ceo-survey- 2015/secure-assets.html.

261. Burgerlink (2006). Workbook e-Citizen Charter,” Version 2.2; http://www.burgerlink.ml/Documenten/burgerlink-1.0/live/binaries/burgerlink/pdf/citizen-charter/workbook-e-citizen-charter-english.pdf.

262. Butrimas, V. (2015). National security and international policy challenges in a post Stuxnet world. Lithuanian Annual Strategic Review. Lithuania: Ministry of Internal Affairs.

263. Buzan, B., Waver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Boulder: Lynne Rienner.

264. C. M., “Arm yourself for cyber war - are you next?” in Sibos Conference Panel 2012, 2012.

265. Cabinet Office (2009a), *The National Security Strategy of the United Kingdom: Update 2009: Security for the Next Generation*, Cm. 7590, June 2009 (Norwich: The Stationery Office); available at http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf. accessed 6 May 2010.

266. Cabinet Office (2009c), *HMG Security Policy Framework: Making*

Government Work Better, Version 3.0, October 2009 (London: Cabinet Office); available at http://www.cabinetoffice.gov.uk/ media/207318/hmg security policy.pdf, accessed 16 May 2010.

267. Campbell, S. (2013). Who Should Drive Cybersecurity Policy: Government or Private Industry? Retrieved from http://www.threattracksecurity.com/blogs/cso/best-cybersecurity-policy-driver-government-private-industry/

268. Capgemini, IDC, Rand Europe, Sogeti, and DTI. (2010). "Digitizing Public Services in Europe: Putting ambition into action—Ninth Benchmark Measurement," for the European Commission, Directorate General for Information Society and Media, December 2010.

269. Caralli R. A., J. H. Allen, and D. W. White, CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience. Addison-Wesley Professional, 2010.

270. Carr, Jeffrey (2018): Inside Cyber Warfare, Sebastopol, CA: O'Reilly.

271. Carr, M. (2016). Public Private Partnerships in National Security Strategies. International Affairs, 43-62.

272. CCDCOE (Cooperative Cyber Defence Centre of Excellence). 2018. "Cyber Definitions." Resources 2017. Accessed February 1. https://ccdcoe.org/cyber-definitions.html.

273. Chabinsky, Steven R. (2010), 'Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line', *Journal of National Security Law & Policy*, Vol.4, No.1, pp.27-39.

274. Chadwick, A. 2006. Internet politics: States, citizens and new communication technologies. Oxford: Oxford University Press

275. CIO Council's Guidelines for Secure Use of Social Media by Federal Departments and Agencies: http://www.cio.gov/documents_details. cfm/uid/1F4378B4-2170-9AD7-F2A2B098D3F954EE/structure/Information%20Technology/category/IT%20Security-Privacy.

276. Cisco. 2010. Annual Security Report.

277. Clarke, Michael (2009), 'Cyber Security as an Aspect of National Security', *Cyber Security: A Public- Private Partnership,* Royal United Services Institute, 21-22 October 2009.

278. Clarke, Richard A., Knake, Robert K. (2010): Cyberwar: The Next Threat to National Security and What to Do about it, New York: Harper/Collins.

279. CO (2009) Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, Cabinet Office, London, UK, available at http://www.official- documents.gov.uk/document/cm76/7642/7642.pdf.

280. CO (2011) The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, Cabinet Office, London, UK, available at https://update.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy- final.pdf.

281. Commonwealth. 2014. Commonwealth Cybergovernance Model. London: Commonwealth ICT Ministers Forum 2014.

282. Conroy S. (2011), Joint Media Release. Cyber White Paper. Available at www.minister.dbcde.gov.au/media/media_releases/2011/198.

283. Council of Europe (2001): Convention on Cybercrime, Budapest, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

284. Council of Europe (2011), "Cybercrime strategies". Discussion paper prepared by the Global Project on Cybercrime. Available at www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/ Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf

285. Council of Europe, (2001) "Convention on Cyber Crime", [Online] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

286. Crenshaw, Kimberle. "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics." University of Chicago Legal Forum, 1989.

287. CSEC 620: Human Aspects in Cybersecurity: Ethics, Legal Issues, and Psychology (2158). Cybercrime: Law Enforcement and E-Government

Transnational Issues. Video posted in University of Maryland University College NSCI 170 6981 online classroom, archived at: https://learn.umuc.edu.

288. CTO (Commonwealth Telecommunications Organisation). 2015. Commonwealth Approach for Developing National Cybersecurity Strategies: A Guide to Creating a Cohesive and Inclusive Approach to Delivering a Safe, Secure and Resilient Cyberspace. 2015th ed. London, UK: Commonwealth Telecommunications Organisation (CTO).

289. Davenport, Tara. "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis." Catholic University Journal of Law and Technology 24 (2015) Accessed Accessed January 4, 2016.

290. Deane, Arsala (2003), "Increasing Voice and Transparency Using ICT Tools: (E-Government, E-Governance)". World Bank. March 2003.

291. Deibert, R. J. (2002). Dark guests and great firewalls: The Internet and Chinese security policy. Journal of Social Issues, 58, 143-159. https://doi.org/10.1111/1540-4560.00253.

292. Deibert, R., & Crete-Nishihata, M. (2011). Blurred boundaries: Probing the ethics of cyberspace research. Review of Policy Research, 28, 531-537. https://doi.org/10.1111/j.1541-1338.2011. 00521.x.

293. Deibert, Ronald J., and Rafal Rohozinski (2010), 'Risking Security: Policies and Paradoxes of Cyberspace Security', *International Political Sociology*, Vol.4, No.1, pp.15-32.

294. Demchak, Chris, and Peter Dombrowski. "Rise of a Cybered Westphalian Age." Strategic Studies Quarterly, March 2011. Accessed January 28, 2013

295. Derrick, L. (2011) Available at http://lafiga.firedoglake.com/2011/06/03/finally-an-intelligent-use-for-cupcakes-hacking-terrorist-sites.

296. Dickey, et al. (2010). "The Shadow of War." Newsweek (December 20), 156:25 (cover story).

297. Digital Agenda website:

http://ec.europa.eu/information_society/newsroom/ cf/pillar.cfm?pillar_id=45.

298. DIT (2011) Discussion Draft of National Cyber Security Policy Version April 6, 2011, Department of Information Technology, Ministry of Communications and Information Technology, New Delhi, India, available at http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf.

299. Drapeau, M. (2010). What does Government 2.0 look like? O'Reilly Radar. Retrieved from http://radar.oreilly.com/2010/05/what-does-government-20-look-l.html.

300. DSS (2010) Draft Cyber Security Policy of South Africa, in Annex to Government Gazette/Staatskoerant, Vol. 536, No. 32963, Department of State Security, Republic of South Africa/Republiek van Suid-Afrika, Pretoria, South Africa, available at http://www.info.gov.za/view/DownloadFileAction?id=118895.

301. Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review, https://doi.org/10.1111/ misr.12023.

302. Dunn, M. (2005). "A Comparative Analysis of Cybersecurity Initiatives Worldwide." Background Paper, WSIS Thematic Meeting on Cybersecurity, Document: CYB/05, June 10, 2005.

303. Dunn-Cavelty, M. (2009) Manuel Suter, Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, International Journal of Critical Infrastructure Protection, Volume 2, Issue 4, December 2009, Pages 179-187, ISSN 1874-5482, http://doi.org/10.1016/j.ijcip.2009.08.006.

304. Dupont B (2012) L'environnement de la cybersecurite a l'horizon tendances, moteurs et implications.Note de recherche 14 Centre International de Criminology Compare. Universite de Montreal, Montreal

305. Dziundziuk V. Change of Functions of Public Administration in an Information Society / Viacheslav Dziundziuk // In Global, Continental, National and Regional Conditions of Local Development ; Eds. T. Michalski and A. Radchenko. – Gdańsk ; Kharkiv : Publishing House "ADNDU", 2012. – P. 55–

58.

306. Dziundziuk V. Possibilities and Threats Caused by the Development of Information Society / Viacheslav Dziundziuk // Research papers of Kaunas University of Technology “Public Policy and Administration”. – 2010. – Nr. 33. – P. 9–22.

307. Dziundziuk V. Stopping Cyberterror / Viacheslav Dziundziuk // Per Concordiam. Journal of European Security and Defense Issues. – 2011. – Vol. 2. – Issue 2. – P. 17–21.

308. EC (2008) Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, European Commission, Brussels, Belgium, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (accessed on May 5, 2012).

309. EC (2010) A Digital Agenda for Europe - COM(2010)245 Final/2, European Commission, Brussels, Belgium, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT.

310. EC (European Commission). 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels: European Commission (EC). doi:10.4271/2010-01-1021.

311. Economist Intelligence Unit. 2009. E-readiness rankings 2009: The usage imperative.

312. ENISA (2011c), “Cyber security: future challenges and opportunities”. Available at www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities.

313. ENISA (2012), “National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace”. Available at www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.

314. ENISA (European Union Agency for Network and Information Security). 2012b. National Cyber Security Strategies: Practical Guide on Development and Execution. Heraklion, Greece: European Network and Information Security Agency (ENISA). doi:10.2824/3903.

315. ENISA. (2013, May) European network and information security agency glossary. [Online]. Available: www.enisa.europa.eu/act/res/files/glossary

316. Eriksson, Johan, and Giampiero Giacomello. International Relations and Security in the Digital Age. London: Routledge, 2007.

317. Eriksson, Johan. Threat Politics: New Perspectives on Security, Risk, and Crisis Management. Aldershot, Hants, England: Ashgate, 2001.

318. Etzioni, A. (2014). The private sector: A reluctant partner in cybersecurity. Georgetown Journal of International Affairs, 69-78. Retrieved from https://search.proquest.com/docview/1832800641?accountid=28902.

319. European Transparency Initiative, IDABC European eGovernment News Roundup. November 2, 2005, No. 116.

320. European Union (2012), "Neelie Kroes. A European Strategy for Internet Security. High Level Public-Private Security Roundtable. Brussels, 21st March 2012". Available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204.

321. European Union Agency for Network and Information Security (ENISA). (2012). Cyber Europe 2012, key findings report, European Union Agency for Network and Information Security.

322. Falliere, Nicolas/O'Murchu, Liam/Chien, Eric (2011): W32.Stuxnet Dossier, Symantec, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

323. Federal Communications Commission: http://www.fcc.gov/pshs/services/911 -services/enhanced911/.

324. FEMA (2011) Critical infrastructure. Strategic foresight initiative. June 2011. http://www.fema.gov/pdf/about/programs/oppa/

critical_infrastructure_paper.pdf.

325. Fetzer, P. (2014, May 2). A Compilation of Enforcement and Non-Enforcement Actions - 30 April 2014. Mondaq Business Briefing. Retrieved from http://bi.galegroup.com.ezproxy.umuc.edu/essentials/article/GALE%7CA366740594/da1cb a907f837d6534b75f26925c2f8c?u=umd_umuc

326. Fitzgerald, Ben. "The Theory Of Intersectionality Can Make Cybersecurity Collaboration Real." TechCrunch. May 17, 2015.. http://techcrunch.com/2015/02/17/the- theory-of-intersectionality-can-make-cybersecurity-collaboration-real/. Accessed January 10, 2016

327. Floridi, L. (2014). The fourth revolution, how the infosphere is reshaping human reality. Oxford: Oxford University Press.

328. Floridi, L. (2016). Mature information societies—a matter of expectations. Philosophy & Technology, 29(1), 1-4. https://doi.org/10.1007/s13347-016-0214-6.

329. Foreign Policy (2019): “The FP Survey: The Internet”, Septembre/October 2019, 90.

330. French Network and Information Security Agency, (2011) "Information Systems Defense and Security France's Strategy" [online] http://www.ssi.gouv.fr/IMG/pdf/2011-02-15.

331. Friedman, N. (2010). “Virus Season.” Proceedings: United States Naval Institute (November), 136:11, 88-89.

332. GCSCC (Global Cyber Security Capacity Centre). 2014. Cyber Security Capability Maturity Model (CMM). Version 1. Oxford: Global Cyber Security Capacity Centre (GCSCC), University of Oxford.

333. GdE (2011b) Spanish Security Strategy: Everyone’s Responsibility, Gobierno de Espana, Madrid, Spain, available at http://www.cidob.org/en/content/download/27940/337722/file/EES_eng.pdf.

334. Georgia Tech Information Security Center. Emerging Cyber Threats Report, 2019.

335. GGDL (2011) Strategie Nationale en Matiere de cyber Securite, Le

Gouvernement du Grand-Duche de Luxembourg, Luxembourg, Luxembourg, available at http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf.

336. Givens, A N. B. (2013). Realizing the promise of public private partnerships in U.S. critical infrastructure protection. International Journal of Critical Infrastructure Protection, 39-50.

337. Gjelten, Tom (2010a): "Shadow Wars: Debating 'Cyber 'Disarmament'", World Affairs Online, November/December 2010, http://www.worldaffairsjournal.org/articles/2010-NovDec/full-Gjelten-ND-2010.html.

338. Gorman S, Bernes JE (2011) Cyber combat: act of war. Wall Str J. 31 May 2011

339. Gourley B., "Open source software and cyber defense," 2009.

340. Greiman, V. (2015). Public private partnerships in cyberspace: Building a sustainable collaboration. Paper presented at the 118-X. Retrieved from https://search.proquest.com/docview/1781336082?accountid=28902.

341. Grier, P. (2010). "WikiLeaks Chief Julian Assange: 'Terrorist' or Journalist?" Christian Science Monitor (December 20), p. 1-3.

342. Guardian newspaper. June 15, 2007. guardian.co.uk. Online crime maps crash under weight of 18 million hits an hour by A. Travis and H. Mulholland: http://www.guardian.co.uk/uk/2011/feb/01/online-crime-maps-power-hands-people.

343. Hansard Society. (2008). "Digital Dialogues 3": http://www.hansardsociety. org.uk.

344. Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security and the Copenhagen School (2009). International Studies Quarterly, 53, 1155-1175. Available at SSRN: https://ssrn.com/ abstract=2567410.

345. Hare, Forrest. "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?" In The Virtual Battlefield: Perspectives on Cyber Warfare, 88-105. Vol. 3. Cryptology and Information Security Series. IOS Press,

2009 DOI: 10.3233/978-1-60750-060-5-88. Accessed March 21, 2013.

346. Harknett, R., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. Journal of Homeland Security and Emergency Manage¬ment. Berlin/New York: De Gruyter.

347. Harris, Shane (2009): "The Cyber Defense Perimeter", National Journal, 02.05.2009, http://www.nationaljournal.com/njmagazine/id_20090502_5834.php.

348. Hausken, K. (2007) Information sharing among firms and cyber attacks, Journal of Accounting and Public Policy, Volume 26, Issue 6, November-December 2007, Pages 639-688.

349. Heal, G., and H. Kunruther. "Self-protection and Insurance with Interdependencies." Journal of Risk and Uncertainty 36 (2008): 101-23. Accessed January 4, 2016.

350. Healey J, (2012) "Lessons From Our Cyber Past: The First Military Cyber Units" [Online Transcript], (Washington DC: Atlantic Council) http://www.acus.org/event/lessons-our-cyber-past-first-military-cyber-units/transcripts.

351. Heeks, R. (ed.) (2001), "Re-inventing Government in the Information Age - International practice in IT-enabled public sector reform." London and New York: Routledge.

352. Henderson, Scott (2017): The Dark Visitor: Inside the World of Chinese Hackers, N.N.

353. Henry, N. 1975. Paradigms in Public Administration. Public Administration Review, Volume 35 (4) pp 378-386

354. Henry, Nicholas (1995), "Public Administration and Public Affairs". (6th edition), USA: Prentice-Hall, Inc.

355. Hesseldahl, A. (2010). "How Bad Guys Worm Their Way into Factories." Business Week.com (October 15).

356. Hollis, David M. (2010), 'USCYBERCOM: The Need for a Combatant

Command Versus a Subunified Command', *Joint Force Quarterly*, Vol.8, No.7, pp.48-53.

357. Hopkins, Curt (2011a): "'PakCyberArmy' Attacks Dozens of Indian Sites", Read Write Web, http://www.readwriteweb.com/archives/pakcyberarmy_attacks_dozens_of_indian_ site s.php.

358. Hopkins, Curt (2011b): "Iran's 'Cyber Army' Hacks Voice of America", Read Write Web, http://www.readwriteweb.com/archives/irans_cyber_army_hacks_voice_of_americ a.p hp.

359. Hughes, Rex (2010), 'A Treaty for Cyberspace', *International Affairs*, Vol.86, No.2, pp. 523-541.

360. Human Capital Institute and Saba, "Social Networking in Government: Opportunities and Challenges," January 2010.

361. ICS-CERT. (2013, Jun.) ICS-CERT monitor report between April-June 2013 of department of homeland security. [Online]. Available: http://icscert.uscert.gov/sites/default/files/IC-CERT_Monitor_AprilJune2013_3.pdf

362. Intelligence and Security Committee (ISC) (2010b), *Annual Report 2009-2010*, Cm.7844, March 2010 (Norwich: The Stationery Office); available at http://www.cabinetoffice.gov.uk/media/348175/isc-annualreport0910.pdf.

363. Ionology, Local Government and Social Media: http://www.ionology.com/ blog/is-local-government-ready-for-social-media/.

364. ISACA (Information Systems Audit and Control Association). 2013. Cybersecurity Nexus: Transforming Cybersecurity. Illinois, USA: Information Systems Audit and Control Association (ISACA).

365. ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2012. ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity. Geneva: ISO/IEC.

366. ISPC (2009) Information Security Strategy for Protecting the Nation, Information Security Policy Council, Tokyo, Japan, available at http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

367. ITU (2007): ITU Cyber security Work Programme to Assist Developing Countries 2007 - 2009, Genf, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work- programme-developing-countries.pdf.

368. ITU (International Telecommunication Union). 2012. ITU National Cybersecurity Strategy Guide. Geneva: International Telecommunication Union (ITU).

369. ITU (International Telecommunication Union). 2017a. "National Strategies. ITU-D Cybersecurity." Accessed August 17, 2017. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.

370. ITU. April 2009. Understanding Cybercrime: A Guide for Developing Countries. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

371. ITU. February 2010. Toolkit for Cybercrime Legislation. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

372. ITU. ITU called to play a key role in WSIS implementation of Action Line C5. http://www.itu.int/osg/csd/cybersecurity/WSIS/index.phtml.

373. ITU. January 2008. Botnet Mitigation Toolkit: Background Information. http:// www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

374. ITU. July 11, 2007. Evolving threats in cybersecurity. http://www.itu.int/osg/spu/newslog/Evolving+Threats+In+Cybersecurity.aspx.

375. ITU. September 2010. National Cybersecurity Strategy Guide. http://www. itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf.

376. ITU: Committed to connecting the world. https://www.itu.int.

377. Jain Palvia, S. C.and Sharma, S.S. 2007. E-government and e-governance: Definitions/ Domain framework and status around the world Accessible on http:// www.iceg.net/2007/books/1Z1_369.pdf . Accessed on 1/1/2013

378. Jervis, Robert (2003): “Realism, Neoliberalism, and Cooperation: Understanding the Debate”, in: Colin Elman, Miriam F. Elman (Eds.): Progress in International Relations Theory: Appraising the Field, Cambridge, MA: The MIT Press, 277-309.

379. Karabacak B. and S. OZKAN, “Critical infrastructure protection status and action items of turkey,” 2009.

380. Kaspersky Labratuaries. (2013, Jun.) Red October an advanced cyber espionage campaign targeting diplomatic and government institutions worldwide. [Online]. Available: http://www.kaspersky.com/about/news/virus/2013/

381. Keohane, Robert O. (1984): After Hegemony: Cooperation and Discord in the World Political Economy, Princeton, NJ: Princeton University Press.

382. Kissel R., Glossary of key information security terms. DIANE Publishing, 2011.

383. Klimburg, A. and Healey, J. (2012) "Strategic Goals & Stakeholders" in Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Talinn.

384. Klimburg, A., ed. 2012. National Cyber Security Framework Manual. Tallin: NATO Cooperative Cyber Defence Centre of Excellence. doi:9789949921119.

385. Klimburg A., Ed., National cyber security framework manual. NATO CCD COE Publications, 2012.

386. Kotukh, Y. V. Cybercrime and subculture of cybercriminals / Y. V. Kotukh, D. V. Kislov, T. S. Yarovoi, R. O. Kotsiuba, O. H. Bondarenko // Linguistics and Culture Review. –2021 – 5(S4). – Pp. 858-869.

387. Kotukh Ye. Encryption scheme based on the automorphism group of the Ree function field / Gennady Khalimov, Yevgeniy Kotukh, Svitlana

Khalimova // 7th International Conference on Internet of Things: Systems, Management and Security (Paris, France. December 14-16, 2020). – Pp. 1-8.

388. Kotukh Ye.V. Public value management and new public governance as modern approaches to the development of public administration / Oleksandr O. Bryhinets, Ivo Svoboda, Oksana R. Shevchuk, Yevgen V. Kotukh, Valentyna Yu. Radich // Revista San Gregorio (Web of Science Core Collection). – Núm. 42 (2020). Pp. 205-213. http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1568/20-OLAKSANDR

389. Kotukh Ye.V. Spread of virtual communities as a potential threat to national security / Viacheslav B. Dziundziuk, Oleksandr A. Kotukov, Dmytro V. Hryn, Eugene V. Kotukh // Rivista Di Studi Sulla Sostenibilita (Scopus). – 2020. – Issue 2. – Pp. 7-18.

390. Kotukh Y.V. State Information Security Policy (Comparative Legal Aspect) / Y. V. Kotukh, V. B. Dziundziuk, O. M. Krutii, V. P. Solovykh, O. A. Kotukov // Cuestiones Políticas. – 2021. – 39(71). – Pp. 166-186.

391. Lawson, Sean (2010), 'General Alexander's Confirmation and the Failure of Cyberwar Transparency', *The Firewall*, 13 May 2010 [online]; available at http://blogs.forbes.com/firewall/2010/05/13/general-alexanders-confirmation-and-the-failure-of-cyberwar-transparency/.

392. Lessig, Lawrence (2006): Code: Version 2.0, New York, NY: Basic Books.

393. Lewis AJ, Neuneck G (2013) The Cyber Index. International security trends and realities. New York and Geneva, United Nations Institute for Disarmament Research

394. Lewis, D. E. (2015). Cyber Threat Information Sharing - Recommendations for Congress and the Administration. Washington, DC: Center for Strategic and International Studies .

395. Liberthal K, Singer PW (2012) Cybersecurity and US-China relations. Brookings Institution. February 2012

396. Libicki, Martin C. (2007): Conquest in Cyberspace: National Security and Information Warfare, Cambridge: Cambridge University Press.

397. Libicki, Martin C. (2009): Cyberdeterrence and Cyberwar, Santa Monica, CA: RAND.

398. Linder, Stephen H. (1999), 'Coming to Terms with the Public-Private Partnership: A Grammar of Multiple Meanings', *American Behavioural Scientist*, Vol.43, No.1, pp.35-51.

399. Lobato, C. L., & Kenkel K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. Revista Brasileira de Politica International, 58(2), 23-43. Available at http:// www.scielo.br/pdf/rbpi/v58n2/0034-7329-rbpi-58-02-00023.pdf.

400. Lord, Kristin M./Sharp, Travis (2018): America's Cyber Future: Security and Prosperity in the Information Age: Volume I, Washington, DC: Center for a New American Security.

401. Luiijf, H.A.M. (2008) 'Cyberterrorisme', in Muller, E.R., Rosenthal, U. and De Wijk, R., (Eds.): Terrorisme: Studies Over Terrorisme en Terrorismebestrijding, Kluwer, Deventer, Netherlands, pp.149-168.

402. Luiijif, E. and Healey, J. (2012) "Organizational Structures & Considerations" in Alexander Klimburg (Ed.), National Cyber Security Framework Manual, Talinn, NATO CCD COE Publication.

403. Markoff, John/Kramer, Andrew E. (2009): "U.S. and Russia Differ on a Treaty for Cyberspace", The New York Times, 28.06.2009, http://www.nytimes.com/2009/06/28/world/28cyber.html (22.11.2010).

404. Maserumule, M.H. 2004. E-Government, e-Governance, and e-Democracy: a conceptual perspective. Service Delivery Review, Volume 3 (2): 76-78

405. Maserumule, M.H. 2011. Good governance in the new partnership for Africa's development (NEPAD): a public administration perspective. D. Litt et Phil. Thesis. University of South Africa

406. Masters, G. (2010). "Raids from Afar." SC Magazine (November)

21:11, 30-32.

407. Mathiason, John (2009): Internet Governance: The new Frontier of Global Institutions, London/New York: Routledge.

408. Matrosov A., E. Rodionov, D. Harley, and J. Malcho, “Stuxnet under the microscope,” ESET LLC (September 2010), 2010.

409. McAfee. 2010. Threats Report: Fourth Quarter.

410. McKinsey. (2009). E-government 2.0, number 4, summer 2009 edition of McKinsey on Government, retrieved December 8, 2009, from: http:// www.mckinseyquarterly.com/Public_Sector/E-government_20_2408.

411. Mearsheimer, John J. The Tragedy of Great Power Politics. New York: Norton, 2001.

412. Melissen, J. (2007) "The New Public Diplomacy: Soft Power in International Relations", New York, Palgrave Macmillan.

413. Microsoft. 2013. Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation. Redmon: Microsoft.

414. Minogue, M., Polidano, C. and Hulme, D. 1999. Beyond the New Public

415. MinV&J (2011b) The National Cyber Security Strategy (NCSS): Success Through Cooperation, Netherlands Ministry of Security and Justice, The Hague, Netherlands, available at http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

416. Misuraca, G.C. 2007. E-Governance in Africa: From theory to action. New Jersey: World Press

417. MoED (2011) New Zealand’s Cyber Security Strategy, Ministry of Economic Development, New Zealand, available at http://www.med.govt.nz/upload/New%20Zealands%20Cyber%20Security%20Strategy%20Ju ne%202011.pdf.

418. MoICT (2011) National Information Security Strategy, Ministry of Information and Communication Technology, Republic of Uganda, available at http://www.ict.go.ug/index.php?option=com_docman&task=doc_download&gid=

49&Itemid= 61.

419. Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (pp. 3-23). Washington, D.C.: National Academy of Sciences.

420. Morse, A. (2013) "The UK Cyber Security Strategy: Landscape Review", National Audit Office, London Oxford University Press.

421. MSCI (2011) Strategia de Securitate Cibernetica a Romaniei, 23 May 2011, Bratislava, Romania, available at http://www.mcsi.ro/Transparenta-decizionala/21/Strategie_Cyber_23052011.

422. Muhammad, M. I. and Abu Momtaz, S. A. 2007. Understanding e-governance: A theoretical approach. Journal of Asian Affairs, Volume 29 (4) pp29-46

423. NATO.(2013, Jun.) Nato web site. [Online]. Available: http://www.nato.int, June,2013

424. Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1(3), 9-19. Excelsior College, Albany.

425. Nicander, Lars (2010), 'Shielding the Net – Understanding the Issue of Vulnerability and Threat to the Information Society', *Policy Studies,* Vol.31, No.3, pp.283-300.

426. NIST (National Institute of Standards and Technology). 2014. Framework for Improving Critical Infrastructure Cybersecurity. Version 1. New York: National Institute of Standards and Technology (NIST).

427. Nye, Joseph S., Jr. (2010), *Cyber Power,* May 2010 (Cambridge, MA: Belfer Center for Science and International Affairs); available at http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

428. OAS (Organization of American States). 2004. "A Comprehensive Inter-American Cybersecurity Strategy: Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity." In Inter-Americaan Committee

Against Terrorism, A1-A8 (Appendix 1). Montevideo, Uruguay: Organization of American States (OAS).

429. Obama, B. (2009). Transcript: President Obama's Town Hall Meeting with Students in Shanghi (November 16). http://www.cbsnews.com/stories/2009/11/16/politics/main5670903.shtml (accessed March 27, 2011).

430. OECD (2005), The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, Paris. Available at www.oecd.org/dataoecd/16/27/35884541.pdf

431. OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, Paris. Available at www.oecd.org/dataoecd/U13/40825404.pdf.

432. OECD (2009), Computer Viruses and Other Malicious Software: A Threat to the Internet Economy, OECD Publishing. doi: 10.1787/9789264056510-en.

433. OECD (2011), National Strategies and Policies for Digital Identity Management in OECD Countries, OECD Digital Economy Papers, No. 177, OECD Publishing. http://dx.doi.org/10.1787/5kgdzvn5rfs2-en.

434. OECD (2012) Cybersecurity policy making at a turning point: analysing new generation of national cybersecurity strategies for the internet economy. OECD digital economy papers 21. OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

435. OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy", [online] OECD Digital Economy Papers, No. 211, OECD Publishing http://www.oecd.org/sti/ieconomv/cvbersecuritv%20policv%20making.pdf.

436. OECD (2012a), "Proactive Policy Measures by Internet Service Providers against Botnets", OECD Digital Economy Papers, No. 199, OECD Publishing. http://dx.doi.org/10.1787/5k98tq42t18w-en.

437. OECD (Organisation for Economic Co-operation and Development). 2012. Cybersecurity Policy Making at a Turning Point: Analysing a New

Generation of National Cybersecurity Strategies for the Internet Economy. 211 vols, No.322. OECD Publishing. doi:10.1787/5k8zq92vdgtl-en.

438. OECD. 2008. Measuring Security and Trust in the Online Environment. A View Using Official Data.

439. Offe, Claus (2008): "Governance - 'Empty Signifier' oder sozialwissenschaftliches Forschungsprogramm", in: Schuppert, Gunnar F./Zurn, Michael (Eds.) (2008): Governance in einer sich wandelnden Welt, Wiesbaden: VS Verlag, 61-76.

440. Olson, Mancur (1965): The Logic of Collective Action: Public Goods and the Theory of Groups, Cambridge: Harvard University Press.

441. Olson, Parmy (2011): "Egypt's Internet Blackout Cost More than OECD Estimates", in: Forbes, http://blogs.forbes.com/parmyolson/2011/02/03/how-much-did- five-days-of-no-internet-cost-egypt/.

442. Oxford Dictionaries, [Online] http://www.oxforddictionaries.com/definition/english/cvbercrime?a=cvber+crime.

443. Oxford dictionaries. [Online]. Available: http://oxforddictionaries.com/

444. Pabru, C.S. 2004. E-governance: Concepts and Case Studies. New Delhi: PHI Learning Pty Ltd

445. Pacific Council on International Policy (PCIP) (2002), "Roadmap for E- government in the Developing World". The Working Group on E-Government in the Developing World. Los Angeles. April 2002. Available At <http:// www.pacificcouncil.org/pdfs/e-gov.paper.f.pdf>.

446. Pepper, David (2010), 'The Business of SIGINT: The Role of Modem Management in the Transformation of GCHQ', *Public Policy & Administration*, Vol.25, No.1, pp.85-97.

447. Pew Internet and American Life Project. April 2010. Government Online: The Internet gives citizens new paths to government services and information. http://www.pewinternet.org/Reports/2010/Government-Online/ Summary-of-Findings.aspx.

448. Ponemon Institute (2012) 2012 Cost of Cyber Crime Study: United States. http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

449. Ponemon Institute LLC. (2019). 'Cybersecurity in Operational Technology: 7 Insights You Need to Know, March 2019'. Ponemon Institute LLC. https://lookbook.tenable.com/ee2b2c72-e552- 43f6-843e-3a63a29d895c.

450. Ponemon Institute. 2016. Cyber Security Mega Trends: Study of IT leaders in the U.S. federal government.

451. PSC (2010a) Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, Public Safety Canada/Securite publique Canada, Ottawa, Canada, available at http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

452. Rauscher, K.F. and Yashenko, V. (Eds.) (2011) Critical Technology Foundations, EastWest Institute, London, available at http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf.

453. Riley, Thomas B. and Riley, Cathia Gilbert (2003), "E-governance to E- democracy - Examining the Evolution". International Tracking Survey Report, 2003. Number Five. Commonwealth Centre for E-Governance, Canada: Riley Information Services.

454. Rosenzweig, P. (2011). Cybersecurity and Public Goods: the Public/Private Partnership. In P. Berkowitz (Series Ed.), Emerging Threats in National Security and Law (pp. 2-35). Retrieved from Board of Trustees of the Leland Stanford Junior University website: http://www.emergingthreatsessays.com.

455. Saco, D. (1999). Colonizing cyberspace: "National security" and the Internet. In J. Weldes, M. Laffey, H. Gusterson, & R. Duvall (Eds.), Cultures ofinsecurity: States, communities, and the production ofdanger. Minneapolis: University of Minnesota Press.

456. Saljic, E., & Bordevic, Z. (2011). Modern forms of terroism [!]

environmental terrorism. Retrieved from https://dk.um.si/IzpisGradiva.php?lang=eng&id=30223.

457. Samuelson, Paul A. (1954): “The Pure Theory of Public Expenditures”, Review of Economics and Statistics, 36 (4), 387-389.

458. Schjolberg, S. 2007. The Report of the Chairman of High-Level Experts Group (HLEG) on the ITU Global Cybersecurity Agenda (GCA). Geneva, Switzerland: International Telecommunication Union (ITU).

459. Schneider, F. B., Elain, S. M., & Deirdre, M. K. (2016). Public cybersecurity and rationalizing information sharing. Lausanne: Opinion Piece for the International Risk Governance Center (IRGC). http:// www.irgc.org.

460. Security task force: Public-private information sharing, 2012.

461. Seddigh N., P. Pieda, A. Matrawy, B. Nandy, I. Lambadaris, and A. Hatfield, “Current trends and advances in information assurance metrics.” in PST, 2004, pp. 197-205.

462. SGDN (2008) Defense et Securite nationale: Le Livre Blanc, Secretariat general de la defense et de la securite nationale, Paris, France, available at http://www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/livre_blanc_tome1_partie1.pdf.

463. SGDN (2011b) Information Systems Defence and Security: France’s Strategy, Secretariat general de la defense et de la securite nationale, Paris, France, available at http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_- _France_s_strategy.pdf.

464. Sklerov, Matthew J. (2010): “Responding to International Cyber Attacks as Acts of War”, in: Jeffrey Carr (Ed.): Inside Cyber Warfare, Sabastopol, CA: O’Reilly Media.

465. Smith, J. (2012, February 9). Groups Warn Of Privacy Concerns In Cybersecurity Bills. National Journal Daily. Retrieved from http://bi.galegroup.com.ezproxy.umuc.edu/essentials/article/GALE%7CA296609515/1bdddd15100244706117f040a6f0096a?u=umd_umuc

466. Social Media Today: http://socialmediatoday.com/kanter/271724/lessons-red -cross-twitter-mistakes-and-how-handle-them.

467. Sofaer, Abraham D./Clark, David/Diffie, Whitfield (2010): „Cyber Security and International Agreements“, in: National Research Council (Ed.): Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Washington, DC: The National Academies Press, 179-206.

468. Somekh, B. and Lewin, C. 2005. Research methods in Social Sciences. London: Sage Publications

469. Sosa, Gilbert C. (2009): “Country Report on Cybercrime: The Phillipines”, in: United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) (Eds.): Work Product of the 104th International Training Course ‘The Crminal Justice Response to Cybercrime’, Tokio, 80-86, http://www.unafei.or.jp/english/pdf/RS_No79/No79_12PA_Sosa.pdf.

470. Stein, Arthur (1993): “Coordination and Collaboration: Regimes in an Anarchic World”, in: David A. Baldwin (Ed.): Neorealism and Neoliberalism: The Contemporary Debate, New York: Columbia University Press, 29-59.

471. Stevens, Tim (2010a), ‘Breaching Protocol: The Threat of Cyberespionage’, *Jane’s Intelligence Review,* Vol.22, No.3, pp.8-13.

472. Stevens, Tim (2010c), ‘Web of Intelligence Gets More Complex’, *The Guardian,* 27 March 2010 [online]; available at http://www.guardian.co.uk/commentisfree/cifamerica/2010/mar/27/web-intelligence-online-jihadists.

473. Sugrue, M. (2010). “Virus May Be Targeting Iran’s Nuclear Program.” Arms Control Today (November) 40:9, 7.

474. Swiatkowska, J., et al. (2012). V4 cooperation in ensuring cyber security - Analysis and recommendations. Krakow: Koscluszko Institute.

475. Symantec. 2010. State of Enterprise Security.

476. Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556(7701), 296-298. https://doi.org/10.1038/d41586-018-04602-6.

477. TechAmerica. (2010). “Tranparency and transformation through technology.” Twentieth Annual Survey of Federal Chief Information Officers, March 2010.

478. TechAmerica. 2017. Twenty-seventh Annual Survey of Federal Chief Information Officers (CIO), April 2017.

479. Technavio. (2018). Global artificial intelligence-based cybersecurity market 2018-2022. Technavio. 2018. https://www.technavio.com/report/global-artificial-intelligence-based-cyber-security-marke t-analysis-share-2018.

480. Techrepublic. (2013, May) Cybersecurity challenges in 2013. [Online]. Available: http://www.techrepublic.com/blog/security/cybersecurity-challenges-in-2013/9038

481. The Dutch Ministry of Security and Justice (2011) "The National Cyber Security Strategy", The Hague. [online] https://www.enisa.europa.eu/media/news-items/dutch-cvber-securitv-strategv-2011.

482. The Economist. (2010). “Yet to Turn” (December 18), 397:8713.

483. The Guardian (2013) "Ex-hackers could be recruited to UK cyberdefence force", [online] http://www.theguardian.com/technologv/2013/oct/22/uk-cvber-defence-force-ex-hackers-gcha.

484. The New York Times (2013) "Universities Face a Rising Barrage of Cyber attacks" New York.

485. The UK Cabinet Office (2011) "The UK Cyber Security Strategy Protecting and promoting the UK in a digital world", [Online] https://www.gov.uk/government/uploads/system/uploads/attachmentdata/file/60961/uk-cyber-security-strategy- final.pdf.

486. The Vulnerability of Data: http://socialmediaclub.org/blogs/social-media-observer/vulnerability-data.

487. The White House (2011b): Joint Statement by Cyber security Coordinator Schmidt and Deputy Secretary Klimashin, Washington, DC, http://www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber _joint_statement.pdf.

488. The White House (May 2010) "National Security Strategy" Washington, http://www.whitehouse.gov/sites/default/files/rssviewer/nationalsecuritystrategy.pdf.

489. The White House, (July 2011) "International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World" Washington, http://www.whitehouse.gov/sites/default/files/rss viewer/international strategy for cyberspace.pdf.

490. Thielmann, G., and Crail, P. (2010). “Chief Obstacle to Iran’s Nuclear Effort: Its Own Bad Technology.” Christian Science Monitor (December 8).

491. Thornhill, C. 2006. The domain of Public Administration. Journal of Public Administration, Volume 41(1) pp. 793-806

492. Thorson, Stuart and Ragland, Jennifer (2002), “E-governance in the Americas and Europe”. A paper prepared as a part of the final report to the Electronic Governance Research Institute of the University of Seoul.

493. Traynor, Ian (2007): “Russia Accused of Unleashing Cyberwar to Disable Estonia”, The Guardian, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

494. Turkish Ministry of Transport (2013), Maritime Affairs and Communication, "National Cyber Security Strategy and Action Plan 2013-2014" Ankara [Online] http://www.ccdcoe.org/strategies/TUR CyberSecurity.pdf.

495. TWH (2011) International Strategy for Cyberspace, The White House, Washington DC, USA, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspac e.pdf.

496. UK Cabinet Office (2008) Data handling procedures in government:

final report. June 2008. http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/65948/dhr080625.pdf.

497. UK Cabinet Office (2011a), “The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world”. Available at www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy.

498. UNIDIR. (2013). The cyber index, International security trends and realities. Geneva: UNIDIR, United Nations Institute for Disarmament Research.

499. United Nations Development Programme. Millennium Development Goal 8: A global partnership for development. http://www.undp.org/mdg/goal8.shtml.

500. United Nations. 2003. World Public Sector Report: E-Government at the Crossroads.

501. United Nations. September 18, 2000. United Nations Millennium Declaration. http://www.un.org/millennium/declaration/ares552e.pdf.

502. United States Cyber Challenge; available at https://www.uscyberchallenge.org/

503. US Department of Defense, Department of Defense Strategy for Operating in Cyberspace, July 2011, Washington http://www.defense.eov/news/d20110714cyber.pdf.

504. US White House (2011a), “International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World”. Available at www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

505. Valeriano B, Maness R (2011) Cyberwar and rivalry: the dynamics of cyber conflict between antagonists. University of Illinois, Chicago World Economic Forum (2012) Risk and responsibility in a hyperconnected world. Pathways to global cyber resilience. June 2012

506. Vatis, Michael V. (2003): “International Cyber-Security Cooperation: Informal Bilateral Models”, in James A. Lewis (Ed.): Cyber Security: Turning

National Solutions into International Cooperation, Washington, DC: CSIS Press, 1-12.

507. von Solms R. and J. van Niekerk, “From information security to cyber security,” Computers & Security, 2013.

508. von Solms, B., and R. von Solms. 2018. "Cybersecurity and Information Security - What Goes Where?" Information and Computer Security 26: 2-9. doi:10.1108/ICS-01-2015-0001.

509. Waltz, Kenneth N. (2003): “The Anarchic Structure of World Politics”, in: Robert J. Art, Robert Jervis (Eds.): International Politics: Enduring Concepts and Contemporary Issues, New York: Longman, 47-67.

510. Waltz, Kenneth N. Theory of International Politics. Reading, MA: Addison-Wesley Pub., 1979.

511. Warfield, D. (2013). Critical infrastructures: IT Security and Threats from Private Sector Ownership. Information Security Journal: A Global Perspective, 21(3), 2012, 127-136. doi10.1080/19393555.2011.652289.

512. Warrick, J. (2011). “WikiLeaks Damage Will Last for Years, Says Clinton.” Sydney Morning Herald (January 11), p. A1. http://www.smh.com.au/technology/technology-news/wikileaks-damage-will-last-for-years-says-clinton-20110110-19l8f.html (accessed March 27, 2011).

513. Waxler, C. CIOs Struggle with Social Media’s Security Risks, Public CIO, February 11, 2011.

514. Weber, S. (2017). Coercion in cybersecurity: What public health models reveal. Journal of Cybersecurity, 3(3), 173-183. https://doi.org/10.1093/cybsec/tyx005.

515. WEF (World Economic Forum). 2012a. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. Geneva, Switzerland: World Economic Forum (WEF). doi:270912.

516. WEF (World Economic Forum). 2012b. Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines. Geneva, Switzerland: World Economic Forum (WEF).

517. WEF (World Economic Forum). 2014. Risk and Responsibility in a Hyperconnected World: Implications for Enterprises. Geneva, Switzerland: World Economic Forum (WEF).

518. WEF (World Economic Forum). 2015. Global Risks 2015: Insight Report. 10th ed. Cologny/Geneva, Switzerland: World Economic Forum (WEF).

519. Wendt, Alexander. Social Theory of International Politics. Cambridge: University Press, 1999.

520. West, Darrel M. (2004), "E-government and the Transformation of Service Delivery and Citizen Attitudes." Public Administration Review 64 (1) January/February 2004.

521. Wever, Ole. Concepts of Security. K0benhavn: Institute of Political Science, University of Copenhagen, 1997.

522. Wiater, P. (2015). On the Notion of "Partnership" in Critical Infrastructure Protection. Symposium on Critical Infrastructures, 255-262.

523. WikiLeaks. https://wikileaks.org/About.html.

524. Wikipedia (2012) available at http://en.wikipedia.org/wiki/Strategy.

525. Williamson, Charles W. (2008): "Carpet Bombing in Cyberspace: Why America Needs a Military Botnet", Armed Forces Journal, http://www.armedforcesjournal.com/2008/05/3375884.

526. Wilson, Clay (2009): "Cyber Crime", in: Franklin D. Kramer/Stuart H.Starr/Larry K. Wentz (Eds.) (2009): Cyberpower and National Security, Washington, DC: National Defense University Press, 415-436.

527. Woolf, Katie (2010), *'Information Matters:* Government's Strategy to Build Capability in Managing its Knowledge and Information Assets', *Legal Information Management,* Vol.10, No.1, pp.47-50.

528. Wriston, Walter B. September/October 1997. Bits, bytes, and diplomacy. Foreign Affairs 76(5): 174–175.

529. Zetter, Kim (2010): "Countries Should be Held Responsible for Cyber Attacks", Wired, http://www.wired.co.uk/news/archive/2010-07/30/cyber-attack-countries.

530. Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal ‘Act of Force." PC, March 25, 2013.Wired. March 25th, 2013: http://www.wired.com/2013/03/stuxnet-act-of-force/ Accessed October 4, 2014.

531. Zrahia, A. (2014). A Multidisciplinary Analysis of Cyber Information Sharing. Military and Strategic Affairs, Vol 6 No. 3, 59-77

Додаток А
Довідки про впровадження результатів дисертаційного дослідження

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
(Мінфін)

вул. М. Грушевського 12/2 м. Київ 01008 тел. (044) 206-59-47, факс 425-90-26
e-mail: infomf@minfin.gov.ua, код ЄДРПОУ 00013480

від _____ 20___ р. № _____ На № _____ від _____ 20___ р.

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Котуха Євгена Володимировича
за темою «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі»

У дисертаційній роботі визначено особливості запобігання та протидії кіберзагрозам у публічному секторі України. Виходячи з цього автор пропонує комплекс взаємопов'язаних заходів, а саме: заходи фінансового характеру, які передбачають обов'язкове фінансування в державному та місцевому бюджетах коштів на кіберзахист, інвестування в кібераналітику і хмарні технології; кадрові заходи, що включають регулярне підвищення кваліфікації всіх державних службовців і посадових осіб органів місцевого самоврядуванн з питань захисту організаційної та персональної інформації, електронного документообігу, он-лайн комунікацій тощо; заходи матеріально-технічного характеру, метою яких є постійне оновлення комп'ютерного обладнання та його програмного забезпечення.

Впровадження цих заходів дає можливість суттєво підвищити рівень кібербезпеки, більш активно протистояти кібезагрозам, відтак забезпечити більш стабільну діяльність як окремих органів влади, так і системи публічного управління в цілому.

Враховуючи значну практичну цінність запропонованих заходів їх було впроваджено в практичній роботі

Директор Департаменту з
питань цифрового розвитку,
цифрових трансформацій і цифровізації **Микола МАТЮШЕНКО**

ДОКУМЕНТ СЕД Мінфін АСКОД
Сертифікат 58E2D9E7F900307B040000007F9228009A208800
Підписувач Матюшенко Микола В'ячеславович
Дійсний з 11.09.2020 17:47:34 по 11.09.2022 17:47:34

Міністерство фінансів України
20040-03-73/26056 від 20.08.2021

МІНІСТЕРСТВО МОЛОДІ ТА СПОРТУ УКРАЇНИ

(Мінмолодьспорт)

вул. Еспланадна, 42, м. Київ, 01601, тел./факс: (044) 289-12-94, тел. (044) 289-03-66, 289-12-64

E-mail: correspond@msms.gov.ua, web-site: http://dsmsu.gov.ua код згідно з ЄДРПОУ 38649881

від _____ 20__ р. № _____ На № _____ від _____ 20__ р.

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Котуха Євгена Володимировича

за темою «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі»

У дисертаційному дослідженні автором було визначено основні виклики для публічного сектора у контексті забезпечення кібербезпеки, до яких віднесено такі: велика ступінь оперативної незалежності та «ізольованості» між різними частинами публічного сектора, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного; важливі загальнодоступні дані створюються, зберігаються та застосовуються відповідними суб'єктами поза органами публічної влади; працівники організацій публічного сектора далеко не завжди демонструють безпечну поведінку у кібепросторі, хоча саме поведінка людини є стрижнем кібербезпеки; зворотна залежність між використанням інформаційно-комунікаційних технологій і кібербезпекою; відсутність або неефективність публічно-приватного партнерства щодо забезпечення кібербезпеки.

Виходячи з цього, автором було запропоновано механізм протидії даним викликам, що містить конкретні заходи і дає можливість підвищити кібербезпеку органів публічної влади.

Враховуючи значну практичну цінність даного механізму його було прийнято для впровадження в практичній роботі цифровізації сфери спорту.

Заступник міністра з питань цифрового розвитку, цифрових трансформацій і цифровізації Віталій ЛАВРОВ

ДЕРЖАВНА АУДИТОРСЬКА СЛУЖБА УКРАЇНИ

04070, м. Київ, вул. П.Сагайдачного, 4, тел. 425-09-24, факс 425-35-58
E-mail: post@dasu.gov.ua Код ЄДРПОУ № 40165856

_____ № _____ На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження

Котуха Євгена Володимировича

за темою «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі»

У дисертаційній роботі Євгена Котуха визначено, що в умовах активного розвитку кіберпростору органи публічної влади мають можливість взаємодіяти з громадянами через використання соціальних медіа, що сприяє переходу до технологій Gov 2.0 у взаємодії з громадськістю.

Виходячи з цього, автор запропонував методологічний підхід до забезпечення кібербезпеки у середовищі Gov 2.0 і визначив, що вона має ґрунтуватись на реалізації таких заходів: модерування контенту публічних акаунтів; запобігання несанкціонованому використанню і передачі конфіденційної інформації; використання браузерів з обмеженими привілеями; впровадження систем виявлення/запобігання вторгнень; використання сервісів Web-репутації; фільтрація на рівні доменних імен (DNS), універсального локатора ресурсів (URL) та протоколів Інтернету; фільтрація шкідливих програм по периметру мережі; використання інструментів попереднього перегляду скорочення URL тощо.

Через значну практичну цінність цього методологічного підходу його було прийнято для впровадження в практичній роботі під час подальшої розробки внутрішніх політик (регламентів) і прийняття управлінських рішень.

Заступник Голови Державної аудиторської служби
України з питань цифрового розвитку,
цифрових трансформацій і цифровізації **Дмитро ШЕВЧУК**

ДОКУМЕНТ СЕД Держаудитслужба АСКОД
Сертифікат 58E2D9E7F900307B0400000077353200E7579500
Підписувач Шевчук Дмитро Павлович
Дійсний з 03.06.2021 0:00:00 по 03.06.2023 0:00:00

Державна аудиторська служба України
001400-16/8764-2021 від 13.07.2021