DOI (Issue): https: //doi.org/10.36486/np.2023.1(59) Issue 1(59) 2023

УДК 004.056

Демедюк Сергій Васильович,
кандидат юридичних наук,
заступник Секретаря Ради національної
безпеки і оборони України, м. Київ, Україна
ORCID ID 0009-0008-1359-5265
Користін Олександр Євгенійович,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
головний науковий співробітник
ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0001-9056-5475

СТІЙКІСТЬ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА ЇЇ ЗАБЕЗПЕЧЕННЯ В НАТО

Статтю присвячено аналізу сутності стійкості суспільства у кіберпросторі. Методологічно зосереджується увага на усвідомленні феномена стійкості. Акцентовано увагу на питаннях, які формують чітке уявлення щодо стійкості суспільства при розбудові системи кібербезпеки. Проаналізовано еволюційний шлях становлення інституту стійкості в НАТО. Зроблено висновки щодо вітчизняної нормативно-правової бази у сфері кібербезпеки, яка за короткий час від повного ігнорування стійкості в системі кібербезпеки пройшла шлях до повноцінного формування правової бази, визначення та регулювання процесів розбудови кіберстійкості в Україні.

Ключові слова: *кібербезпека, стійкість, кіберзагроза, кіберстійкість, вразливість, спроможність, відновлення.*

У сучасному інформаційному суспільстві питання кібербезпеки займає одне з ключових місць. Розвиток суспільства та сформовані правові інструменти забезпечують реалізацію інформаційних прав і обов'язків громадян, визначають ступінь розвитку інформаційної сфери України, стан інформаційного правопорядку, рівень забезпечення правової охорони і захисту соціальних цінностей. За умови гібридизації загроз національна безпека загалом, зокрема кібербезпека, потребують формування безпекового кіберпростору та системного впровадження відповідних правових інструментів [1]. Одним із ключових сучасних світових трендів кібербезпеки є забезпечення кіберстійкості.

В умовах широкомасштабного вторгнення рф кібербезпека є одним із ключових елементів обороноздатності держави. Сьогодні кібервійна у розпалі. Російські хакери здійснюють цілеспрямовані атаки на органи влади та інфраструктурні підприємства для того, щоб знизити або паралізувати економічну активність громади, підвищити соціальну напругу через відсутність або нестабільну роботу підприємств, які забезпечують роботу критичної інфраструктури [2]. Кількість кібер-

DOI (Article): https: //doi.org/10.36486/np.2023.1(59).8

атак у 2022 році на логістику, військові об'єкти, бази даних органів влади та інформресурси нашої держави в порівнянні з 2021 роком збільшилася майже втричі; рф здійснює також системні кібератаки на транспортну, промислову та енергетичну інфраструктури України. Фіксуються численні спроби ворожих кібератак щодо наших громадян, спам-розсилання фішингу, викрадення інформації про персональні дані громадян, зокрема військовослужбовців та інших суб'єктів, які забезпечують національну безпеку та оборону [3].

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

Наразі, характеризуючи термін "стійкість", важливо зазначити, що йдеться про відповідний стан об'єкта безпеки: критичної інфраструктури, певної системи, суспільства загалом. Так, термінологічний глосарій ООН формулює визначення стійкості як здатність систем, громад та суспільства абсорбувати зовнішні впливи та швидко відновлювати характеристики (базову структуру і функції), так і адаптивні можливості, гнучкість системи в умовах значних трансформацій, впливів зовнішнього середовища [4, с. 24]. Водночас термін "стійкість" (англ., *resilience*) є достатньо вживаним в англомовних країнах та характеризується усталеними ознаками, які формують його сприйняття на рівні міжнародних нормативно-правових документів й практично їх значення формує основу сприйняття "стійкості" у стратегічних безпекових документах. Також необхідним застереженням є певна проблема інтерпретації терміну "стійкість" при перекладі з англійської на інші мови. Як зазначають Тімоті Пріор та Йонас Хагман, різноманіття смислу поняття "стійкість" призводить до проблеми його уточнення для тих, хто формує державну політику [5, с. 282].

Джонатан Джозеф з Великої Британії зазначає про "стійкість" як про неоліберальну форму державного управління, з наголосом на здатності суспільства адаптуватися до загроз [6]. Водночас Джером Каган акцентує на тому, що термін "стійкість" системно використовується у стратегічних документах, є достатньо вживаним серед політиків у Сполучених Штатах щодо питань безпеки, часто виголошується у виступах політичних діячів, а Конгресом проголошуються "місяці стійкості" [7]. Наприклад у Стратегії національної безпеки США (в редакції 2010 року) безпосереднє використання терміну "стійкість" здійснюється в контексті [8]: підвищення стійкості держави та національної економіки; дотримання послідовного політичного курсу країни на основі американських цінностей; здатності реагувати на надзвичайні ситуації; зменшення вразливості та підвищення стійкості критичної інфраструктури; протидії глобальним викликам. А у Стратегії національної безпеки Великої Британії стійкість використовується як одна з ключових частин забезпечення національної безпеки: метою державної політики у сфері нацбезпеки визначено розбудову оборони, стійкості та партнерства, а в подальшому тексті акцентовано увагу на зміцненні внутрішньої стійкості у протистоянні глобальним викликам [9].

Вітчизняні вчені також досліджують зазначені питання, зокрема Бірюков Д.С., виділяючи сутнісні ознаки, зазначає, що "стійкість" можна розглядати як суспільно-

культурний феномен, який полягає у спроможності суспільства досягати та в надзвичайних ситуаціях демонструвати високий рівень культури безпеки [10, с. 223]. Наразі приклад героїзму і рішучості українського суспільства у протистоянні російській агресії також засвідчує про відповідний рівень стійкості нашої держави, в основі якої саме соціальний феномен, рівень свідомості та культури переважної більшості українських громадян. А якщо розглядати "українські майдани", на нашу думку, саме стійкість як суспільно-культурний феномен сформувала активну громадянську позицію та об'єднала людей без підтримки держави взяти відповідальність за своє майбутнє на себе. Водночас дослідники з Великої Британії, посилаючись на американську пресу, після терактів у квітні 2003 року в Бостоні зазначали про характерні риси поведінки громадян: сміливі, швидко орієнтувалися, показували приклад щирого товариства, залишалися спокійними та дотримувалися інструкцій представників правоохоронних органів [11, с. 221].

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

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

На початковому етапі існування НАТО стійкість реалізовувалась загальним сутнісним підходом саме щодо можливості витримувати неочікувані військові удари, що закріплювалося Північноатлантичним договором та застосуванням принципу колективної оборони. Так, у ст. 3 зазначалося, що для забезпечення ефективнішої реалізації цілей Договору країни-члени, діючи окремо чи колективно, шляхом постійного та ефективного вдосконалення власних можливостей та взаємодопомоги підтримуватимуть і розвиватимуть свою індивідуальну та колективну здатність протистояти збройному нападу [14]. Але сучасні підходи прямо визначають стійкість одним із ключових напрямів.

За сучасних безпекових умов актуальність забезпечення стійкості в НАТО значно зросла та все частіше розглядається як окремий напрям діяльності Альянсу. Посилюючи цю складову, спочатку принцип колективної оборони було доповнено розбудовою спроможностей кризового менеджменту та розвитком співробітництва за напрямом безпеки [15]. Але анексія Криму рф у вересні 2014 року сформувала нові виклики в глобальному безпековому середовищі, що потребувало упровад-

DOI (Article): https: //doi.org/10.36486/np.2023.1(59).8

ження нових підходів у стратегічному та операційному плануванні і визначенні завдань. Як результат, було затверджено "План дій НАТО щодо забезпечення готовності" [16], який хоча і не реалізував ще прямо концепцію стійкості, все ж змістовно наблизив цей процес, оскільки передбачав: посилення оборонних спроможностей, підвищення мобільності та оперативності, поліпшення співпраці і координації між структурами Альянсу, відпрацювання заходів антикризового управління, посилення спроможностей отримання розвідувальної інформації тощо.

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

гарантована дієвість уряду і критично важливих урядових служб;

стійке постачання енергії;

здатність ефективно вирішувати ситуацію з неконтрольованим переміщення людей;

стійкі джерела продуктів і води;

здатність впоратися з проблемою значних людських втрат;

стійкі цивільні системи зв'язку;

стійкі транспортні системи (для потреб НАТО) [17].

На цьому ж етапі упроваджуються нові напрями та заходи розбудови стійкості у кіберпросторі [18]:

створені команди кіберреагування;

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

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

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

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

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

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

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

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

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

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

налагодження співпраці на основі взаємного доповнення з Центром ЄС з боротьби з кіберзлочинами, особливо у світлі гібридної війни та конфліктів у сірих зонах [18].

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

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

здатності витримувати неочікувані удари;

відновлення після руйнівних наслідків явищ/дій будь-якої природи до бажаної рівноваги за умови збереження безперервності процесу управління [19].

Нормативно-правове забезпечення реалізації концепту стійкості в України сформувалося лише за останні роки. Стратегія національної безпеки України 2015 року цей термін використовує лише у контексті підвищення стійкості національної економіки до негативних зовнішніх впливів [20] і понятійного визначення змісту зазначеного терміну взагалі не містить. Водночас наступна 2020 року Стратегія національної безпеки України: "БЕЗПЕКА ЛЮДИНИ – БЕЗПЕКА КРАЇНИ" ключовими засадами визначає стримування, стійкість та взаємодію [21]. А у ст. 47 прямо зазначається: "Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз...". Що буде реалізовуватися шляхом:

оцінки ризиків, своєчасної ідентифікації загроз і визначення вразливостей;

ефективного стратегічного планування і кризового менеджменту;

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

поширення необхідних знань і навичок у цій сфері;

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

У заключних положеннях зазначається, що вона є основою для розроблення галузевих стратегій, зокрема кібербезпеки України, яка і була введена в дію відповідним Указом Президента України у травні 2021 року [22]. В останньому розділі "Виміри успіху (метрики)" зазначається, що за результатами реалізації Стратегії Україна забезпечить:

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

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

розвиток кадрового потенціалу та інноваційного ринку кібербезпеки....

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

DOI (Article): https: //doi.org/10.36486/np.2023.1(59).8

Таким чином, в умовах сучасних викликів забезпечення кіберстійкості є суспільно-культурним феноменом, що реалізується через складний багатовимірний концепт, у якому ключові суб'єкти кібербезпеки одночасно є і об'єктами. Високий рівень кіберстійкості забезпечується участю усіх суб'єктів системи кібербезпеки, формуванням надійних та ефективних інституцій, структур, агенцій та місій, що сприяють кібербезпеці та реагують на кібератаки. Тобто розбудова державно-приватного партнерства та необхідної культури у суб'єктів забезпечення кібербезпеки практично формує передумови стійкості суспільства у кіберпросторі. Водночас кібербезпека не обов'язково залежить від характеру чи рівня кіберзагрози, особливо в умовах війни. Кібербезпека, що розбудовується на основі формування системи стійкості із урахуванням здатності суб'єктів кібербезпеки протистояти загрозам, навіть за умови певної уразливості, але з відповідними характеристиками спроможності національної системи забезпечення кібербезпеки, дозволяє вистояти та відновитися в умовах кібератак і кіберзлочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Користін О.Є., Веселова Л.Ю.* Ризикорієнтованість кібербезпеки. Наука і правоохорона. 2021. № 3. С. 158–167.

2. Національний саміт кібербезпеки. URL: https://www.myvin.com.ua/news/17100-u-vinnytsi-vidbuvsia-natsionalnyi-samit-kiberbezpeky (дата звернення: 04.04.2023).

3. Предтечею нової хвилі масштабної агресії рф може стати наступ у кіберпросторі – Секретар РНБОУ. URL: https://np.pl.ua/2023/02/predtecheiu-novoi-khvyli-masshtabnoi-ahresii-rf-mozhe-staty-nastup-u-kiberprostori-sekretar-rnbou/. (дата звернення: 04.04.2023).

4. *Prior T., Hagmann J.* Measuring resilience: methodological and political challenges of a trend security concept. J. Risk Research. 2014. Vol. 17. № 3. P. 281–298.

5. Terminology on Disaster Risk Reduction. Geneva: UNISDR, 2009. 30 p.

6. *Joseph J.* Resilience as embedded neoliberalism: a governmentality approach. Resilience: Int. Policies, Practices & Discourses. 2013. Vol. 1(1). P. 38–52.

7. *Kahan J.H.* Resilience Redux: Buzzword or Basis for Homeland Security. Homeland Security Affairs. 2015. Vol. 11. URL: www.hsaj.org/articles/1308 (дата звернення: 04.04.2023).

8. National Security Strategy. White House, February 2010. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (дата звернення: 05.04.2023).

9. National Security Strategy and Strategic Defence and Security Review 2015: a Secure and Prosperous United Kingdom. URL: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015 (дата звернення: 04.04.2023).

10. *Бірюков Д.С.* Поняття "стійкість" в сучасних безпекових дослідженнях. Вісник Дніпропетровського університету. 2015. № 5. С. 220–237.

11. *Brassett J., Croft S., Vaughan-Williams N.* Introduction: an Agenda for Resilience Research in Politics and International Relations. *Politics.* 2013. Vol. 33, № 4. P. 221–228.

12. Organizational Resilience – Concepts and Evaluation Method / Robert B. et al. Presses-internationales Polytechnique, 2010. 46 p.

13. *Dunn Cavelty M., Kaufmann M., Soby Kristensen K.* Resilience and (in)security: Practices, subjects, temporalities. Security Dialogue. 2015. Vol. 46. P. 3–14.

14. Північноатлантичний договір: міжнародний документ. Офіційний сайт Верховної Ради України. URL: http://zakon5.rada.gov.ua/laws/show/950_008 (дата звернення: 04.04.2023).

15. *Брежнєва Т.В.* Стійкість як ключовий елемент колективної оборони НАТО. Стратегічні пріоритети. 2017. № 3 (44). С. 13.

16. NATO's Readiness Action Plan. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_ 12/20141202_141202-facstsheet-rap-en.pdf (дата звернення: 04.04.2023).

17. NATO Defence Ministers agree to enhance collective defence and deterrence. URL: https://www.nato.int/ cps/en/natohq/news_132356.htm?selectedLocale=en (дата звернення: 05.04.2023).

DOI (Issue): https: //doi.org/10.36486/np.2023.1(59) Issue 1(59) 2023

18. *Веселова Л.Ю.* Кібернетична безпека в умовах гібридної війни: адміністративно-правові засади: монографія. Одеса: Видавничий дім "Гельветика", 2020. 488 с.

19. *Резнікова О.О.* Забезпечення стійкості держави і суспільства до терористичної загрози в Україні та світі. Стратегічні пріоритети. 2017. № 3 (44). С. 23–24.

20. Про рішення Ради національної безпеки і оборони України від 06.05.2015 "Про Стратегію національної безпеки України": Указ Президента України від 26 трав. 2015 р. № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 04.04.2023).

21. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. "Про Стратегію національної безпеки України": Указ Президента України від 14 верес. 2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 04.04.2023).

22. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26 серп. 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 04.04.2023).

REFERENCES

1. *Korystin O.Ye., Veselova L.Yu.* (2021). Ryzykoriientovanist kiberbezpeky. "Risk orientation of cyber security". Nauka i Pravookhorona. No 3. P. 158–167 [in Ukrainian].

2. Natsionalnyi samit kiberbezpeky. "National Cyber Security Summit". URL: https:// www.myvin.com.ua/news/17100-u-vinnytsi-vidbuvsia-natsionalnyi-samit-kiberbezpeky (Date of Application: 04.04.2023) [in Ukrainian].

3. Predtecheiu novoi khvyli masshtabnoi ahresii rf mozhe staty nastup u kiberprostori – Sekretar RNBOU. "The forerunner of a new wave of large-scale aggression of the Russian Federation may be an offensive in cyberspace – the Secretary of the National Defense and Security Service". URL: https://np.pl.ua/2023/02/predtecheiu-novoi-khvyli-masshtabnoi-ahresii-rf-mozhe-staty-nastup-u-kiberprostori-sekretar-rnbou/. (Date of Application: 04.04.2023) [in Ukrainian].

4. *Prior T., Hagmann J.* (2014). Measuring resilience: methodological and political challenges of a trend security concept. J. Risk Research. Vol. 17. No 3. P. 281–298 [in English].

5. Terminology on Disaster Risk Reduction. Geneva: UNISDR, 2009. 30 p. [in English].

6. *Joseph J.* (2013). Resilience as embedded neoliberalism: a governmentality approach. Resilience: Int. Policies, Practices & Discourses. Vol. 1(1). P. 38–52 [in English].

7. *Kahan J.H.* (2015). Resilience Redux: Buzzword or Basis for Homeland Security. Homeland Security Affairs. Vol. 11. URL: www.hsaj.org/articles/1308. (Date of Application: 04.04.2023) [in English].

8. National Security Strategy. White House, February 2010. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf. (Date of Application: 05.04.2023) [in English].

9. National Security Strategy and Strategic Defence and Security Review 2015: a Secure and Prosperous United Kingdom. URL: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015. (Date of Application: 04.04.2023) [in English].

10. *Biriukov D.S.* (2015). Poniattia "stiikist" v suchasnykh bezpekovykh doslidzhenniakh. "The concept of sustainability' in modern security research". Bulletin of Dnipropetrovsk University. No 5. P. 220–237 [in Ukrainian].

11. *Brassett J., Croft S., Vaughan-Williams N.* (2013). Introduction: An Agenda for Resilience Research in Politics and International Relations. Politics. Vol. 33, No 4. P. 221–228 (Date of Application: 04.04.2023) [in English].

12. Organizational Resilience – Concepts and Evaluation Method / Robert B. et al. Presses-internationales Polytechnique, 2010. 46 p. [in English].

13. *Dunn Cavelty M., Kaufmann M., Soby Kristensen K.* (2015). Resilience and (in)security: Practices, subjects, temporalities. Security Dialogue. Vol. 46. P. 3–14 [in English].

14. Pivnichnoatlantychnyi dohovir. "North Atlantic Treaty: an international document". Official website of the Verkhovna Rada of Ukraine. URL: http://zakon5.rada.gov.ua/laws/show/950_008. (Date of Application: 04.04.2023) [in Ukrainian].

DOI (Article): https: //doi.org/10.36486/np.2023.1(59).8

15. *Brezhnieva T.V.* (2017). Stiikist iak kliuchovyi element kolektyvnoi oborony NATO. "Resilience as a key element of NATO's collective defense". Strategic priorities. No 3 (44). P. 13 [in Ukrainian].
16. NATO's Readiness Action Plan. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_ 12/20141202_141202-facstsheet-rap-en.pdf. (Date of Application: 04.04.2023) [in English].
17. NATO Defence Ministers agree to enhance collective defence and deterrence. URL: https://www.nato.int/ cps/en/natohq/news_132356.htm?selectedLocale=en. (Date of Application: 05.04.2023) [in English].
18. *Veselova L.Yu.* (2020). Kibernetychna bezpeka v umovakh hibrydnoi viiny: administratyvno-pravovi zasady. "Cyber security in the conditions of hybrid warfare: administrative and legal foundations": a monograph. Odesa: "Helvetica" Publishing House. 488 p. [in Ukrainian].
19. *Reznikova O.O.* (2017). Zabezpechennia stiиkosti derzhavy i suspilstva do terorystychnoi zahrozy v Ukraini ta sviti. "Ensuring the stability of the state and society against the terrorist threat in Ukraine and the world". Strategic priorities. No 3 (44). P. 23–24 [in Ukrainian].
20. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 06.05.2015 "Pro Stratehiiu natsionalnoi bezpeky Ukrainy". "On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "The National Security Strategy of Ukraine". Decree of the President of Ukraine dated May 26 2015 No 287/2015.URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (Date of Application: 04.04.2023) [in Ukrainian].
21. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14.09.2020 "Pro Stratehiiu natsionalnoi bezpeky Ukrainy". "The decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine". Decree of the President of Ukraine dated September 14, 2020 No 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (Date of Application: 04.04.2023) [in Ukrainian].
22. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14.05.2021 "Pro Stratehiiu kiberbezpeky Ukrainy". "The decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine". Decree of the President of Ukraine dated August 26 in 2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text. (Date of Application: 04.04.2023) [in Ukrainian].

UDC 004.056

Demediuk Serhii,
Candidate of Juridical Sciences (Ph.D),
Deputy Secretary of the National Security
and Defense Council of Ukraine, Kyiv, Ukraine,
ORCID ID 0009-0008-1359-5265
Korystin Oleksandr,
Doctor of Juridical Sciences, Professor,
Honored Worker of Science and Technology of Ukraine,
Chief Researcher of the
State Research Institute MIA Ukraine,
Kyiv, Ukraine,
ORCID ID 0000-0001-9056-5475

CYBERSECURITY SYSTEM RESILIENCE AND ASSURANCE IN NATO

The article highlights the recent increased intensity of cyber attacks on logistics, military facilities, government databases and our country's information resources by

DOI (Article): https: //doi.org/10.36486/np.2023.1(59).8

the aggressor. It is noted that the intensity of cyberattacks on logistics, military facilities, government databases and information resources of our country by the aggressor has recently increased.

Methodologically, attention is focused on understanding the phenomenon of resilience. It is noted that scientists consider resilience as a socio-cultural phenomenon, which consists in the ability of society to achieve and demonstrate a high level of security culture in emergency situations. The general concept of resilience is an approach that considers the inevitability of a certain negative event, which is realized by a relevant threat and the objective need to form a resilience system based on security measures that will allow for survival and recovery.

The authors note that the term "resilience" is widely used in English-speaking countries and is characterised by well-established features, shaping its perception at the level of international legal instruments as well as its practical use in strategic security acts. In particular, the national security strategies of the United States and the United Kingdom are analyzed. The author points out the reservations regarding the interpretation of the term "resilience" when translated from English into other languages.

Attention is focused on the issues that form a clear picture of the resilience of society in the development of the cybersecurity system.

The evolutionary path of formation of the institution of resilience in NATO is analyzed. The article summarises that the national regulatory framework for cybersecurity, which in a short time has gone from completely ignoring resilience in cybersecurity to fully forming a legal framework, defining and regulating the processes of building cyber resilience in Ukraine.

Based on the analysis, the study concludes that a high level of cyber resilience is ensured by the participation of all actors in the cybersecurity system, the formation of reliable and effective institutions, structures, agencies and missions that promote cybersecurity and respond to cyber attacks.

Keywords: cybersecurity, resilience, cyber threat, cyber resilience, vulnerability, ability, recovery.

Отримано 12.04.2023