УДК 354:340.133

ПАНЧЕНКО О.А., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-5649-3658.

АКТУАЛЬНІ ПИТАННЯ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРЗАГРОЗ: АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *У статті розглядаються актуальні питання оцінювання ризиків кіберзагроз. Здійснено аналіз Закону "Про основні засади забезпечення кібербезпеки України", Стратегії кібербезпеки України та інших законодавчих актів з питань забезпечення кібербезпеки. Розглядаються основні підходи до визначення оцінки кіберзагроз. Аналізуються кращі зразки зарубіжної практики оцінювання ризиків кіберзагроз, визначаються найбільш ефективні національні системи їх оцінювання. Зроблено висновок, що найбільш ефективними є багаторівневі системи оцінювання ризиків і загроз, коли аналіз проводиться як на національному, так і на регіональному або місцевому рівні.*

Ключові слова: *кіберзагроза, кібератака, кіберпростір, оцінювання ризиків, об'єкти національної системи кібербезпеки.*

Summary. *The article considers topical issues of cyber threat risk assessment. It contains an analysis of the Law "On Basic Principles for providing of Cyber Security of Ukraine", the Cyber Security Strategy of Ukraine and other legislative acts for providing on cyber security. The main approaches to determining the assessment of cyber threats are considered. The best examples of foreign practice of cyber threat risk assessment are analyzed, the most effective national systems of their assessment are revealed. It is concluded that multi-level risk and threat assessment systems are most effective when the relevant analysis is conducted at both the national and regional and/or local levels.*

Keywords*: cyber threat, cyberattack, cyberspace, risk assessment, objects of the national cyber security system.*

Аннотация. *В статье рассматриваются актуальные вопросы оценки рисков киберугроз. Осуществлен анализ Закона Украины "Об основах обеспечения кибербезопасности Украины", Стратегии кибербезопасности Украины и других законодательных актов по обеспечению кибербезопасности. Рассматриваются основные подходы к определению оценки киберугроз. Анализируются лучшие образцы зарубежной практики оценки рисков киберугроз, определяются наиболее эффективные национальные системы их оценки. Сделан вывод о том, что наиболее эффективными являются многоуровневые системы оценки рисков и угроз, когда анализ проводится как на национальном, так и на региональном или местном уровне.*

Ключевые слова: *киберугроза, кибератака, киберпространство, оценка рисков, объекты национальной системы кибербезопасности.*

Постановка проблеми. Сучасні виклики та загрози, що постали перед Україною у кіберпросторі, зумовлюють зростання ролі кібербезпеки. Нова Стратегія кібербезпеки України (далі – Стратегія), затверджена Указом Президента України від 26 серпня 2021 року № 447, містить висновок про те, що упровадження нових технологій здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків [1]. Однією з причин такого стану справ є незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки [1].

Ситуація з поширенням коронавірусної хвороби (CoVID-19) виявила низьку готовність багатьох країн світу, у т.ч. України, до реагування на загрозу масштабної пандемії, засвідчила недосконаліть національних систем оцінки ризиків кіберзагроз та вироблення заходів з кібербезпеки. Україна, як і більшість країн світу, зіштовхнулася з низкою проблемних питань у зв'язку з поширенням пандемії коронавірусу. У багатьох країнах запровадження обмежувальних протиепідемічних заходів створило додаткові ризики і загрози в інформаційній сфері. Це актуалізує питання розбудови національної стійкості, зокрема визначення ефективних механізмів комплексного реагування на кіберзагрози на всіх етапах, підвищення готовності держави і суспільства шляхом запровадження додаткових заходів з кібербезпеки, а також належної координації такої діяльності.

Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії таким загрозам [1]. Стратегічний оборонний бюлетень України до потенційних загроз в інформаційній сфері відносить, зокрема, неспроможність ефективно реагувати на зростаючу кількість та потужність кібератак [2].

Результати аналізу наукових публікацій. Система оцінювання ризиків кіберзагроз була предметом аналізу у роботах таких фахівців, як: О.Д. Довгань та Т.Ю. Ткачук [3], Р.В. Лук'янчук [4], О.М. Солодка [5], О.О. Резнікова [6], О.О. Тихомиров [7], Н. Ткачук [8] тощо. Водночас ефективне функціонування системи оцінювання ризиків кіберзагроз потребує удосконалення.

Метою статті є аналіз ризиків кіберзагроз та вироблення на підставі аналізу кращих світових практик шляхів удосконалення системи їх оцінювання.

Виклад основного матеріалу. Відповідно до ст. 1 Закону України "Про основні засади забезпечення кібербезпеки України" під кіберзагрозою розуміють наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Під індикаторами кіберзагроз слід розуміти показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози [9].

Ефективне функціонування системи оцінювання ризиків і кіберзагроз є важливим елементом стратегічного планування та забезпечення національної стійкості за напрямком кібербезпеки. Такі системи називають національними, через те що вони функціонують на рівні держави, охоплюють процеси, які стосуються забезпечення безпеки держави, суспільства та кожного громадянина, а також засновані на широкій міжвідомчій взаємодії та співпраці[5, с. 4].

Для визначення найбільш небезпечних загроз для кібербезпеки застосовуються два основні підходи. Перший передбачає оцінювання всіх можливих існуючих загроз за критеріями ймовірності й тяжкості наслідків. Як і для будь-яких експертних опитувань. Інший альтернативний підхід передбачає, що спочатку проводиться аналіз безпекового середовища у розрізі певної сфери (наприклад, інформаційної) за визначеними критеріями (індикаторами) у динаміці. Критерії відбору в кожній країні можуть бути різними. Певні країни визначають сфери національної безпеки, у яких постійний моніторинг та аналіз ризиків є обов'язковими. Це дозволяє виявити небезпечні тенденції, наближення індикаторів до критичної межі, а також звузити перелік ризиків для подальшого аналізу за критеріями ймовірності й тяжкості наслідків. При цьому рівень суб'єктивізму може бути дещо нижчим, оскільки, крім експертних оцінок, використовуються статистичні показники. Для оцінювання та порівняння ризиків і

загроз використовуються різні логарифмічні шкали і спеціальні методи досліджень. Це дає змогу визначити спектр загроз, які потребують найбільшої уваги та мають найвищу ймовірність настання і найтяжчі наслідки [5, с. 34].

Крім того, для подальшого аналізу й розробки сценарних прогнозів до отриманого переліку загроз можуть бути включені ризики, які спричиняють найбільший негативний вплив, але є малоймовірними, а також ті, що мають високу ймовірність, але незначний вплив.

Відповідно до Закону України "Про національну безпеку України" Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі [10].

За результатами експертних оцінок, стан реалізації попередньої Стратегії кібербезпеки України (затвердженої Указом Президента України від 15 березня 2016 року № 96) за визначеними показниками не перевищував 40 відсотків, а отриманий досвід надав змогу виокремити низку системних проблем [1].

Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Незадовільним був і рівень планування заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 2016 року, оскільки заплановані заходи не завжди корелювалися із визначеними нею завданнями, а реалізація зазначеної Стратегії була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення. Не були розроблені індикатори виконання Стратегії кібербезпеки України, затвердженої Указом Президента України від 2016 року, що ускладнило процес оцінки її результативності та виокремлення незавершених завдань [1]. Крім цього, участь у реалізації названої Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучалися інші державні органи, заклади освіти, наукові установи, громадськість.

Не дивлячись на таку незадовільну оцінку системи оцінювання кібезагроз, відзначимо створення умов для формування системи оцінювання кіберзагроз та певні кроки до її реалізації. Одним з важливих кроків у напрямку формування такої системи став Закон України "Про основні засади забезпечення кібербезпеки України" [9], який визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [1].

З метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку у 2016 році утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері. Утворено відповідні центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві

оборони України, Збройних Силах України [1], що свідчить про спробу координації діяльності у сфері кібербезпеки та формування системи оцінювання ризиків кіберзагроз.

Сьогодні активно розвивається співпраця у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії, Королівством Нідерланди, Японією тощо), поглиблюється співробітництво з ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій [1].

Досвід цих країн є вельми цікавим в контексті формування національної системи оцінки ризиків кіберзагроз. Як засвідчує цей досвід, найбільш ефективними є багаторівневі системи оцінювання ризиків і загроз, коли відповідний аналіз проводиться як на національному, так і на регіональному та/або місцевому рівні. Подібна практика поширена у країнах з розвиненими механізмами міжвідомчої співпраці і взаємодії на регіональному рівні та достатнім рівнем децентралізації у сфері забезпечення національної безпеки. Розглянемо таку практику у частині оцінювання кіберзагроз.

У США система оцінювання ризиків і загроз охоплює величезну кількість різноманітних об'єктів та зв'язків між ними. У роботі американських вчених "Викриття, розуміння та аналіз взаємозв'язку об'єктів критичної інфраструктури" представлена така класифікація взаємозв'язків між критичною інфраструктурою: фізична, кібернетична, географічна (топологічна) та логічна [11]. Для оптимізації досліджень застосовуються методи групування об'єктів національної системи кібербезпеки відповідно до їх взаємозалежності за секторами різного рівня з урахуванням їх важливості, зміст якої відображений в Національній стратегії з фізичного захисту об'єктів критичної інфраструктури та ключових об'єктів [12]. За результатами такої оцінки найвищий рівень захисту в ієрархії ключових об'єктів отримали об'єкти військово-промислового комплексу, системи охорони здоров'я та попередження надзвичайної ситуації. Наступне місце в ієрархії посідають об'єкти фінансового сектору. І, нарешті, найнижчий рівень складають об'єкти інформаційно-телекомунікаційного та енергетичного сектору. При цьому однією з головних умов залишається дотримання критерію "вартість – ефективність", а ключова проблема полягає в тому, щоб правильно обрати способи й засоби для організації захисту таких об'єктів [13].

Сьогодні в США функціонує збалансована система забезпечення захисту об'єктів національної системи кібербезпеки, зміст якої охоплює: визначений уповноважений орган для організації, координації заходів безпекового напрямку; методичний апарат для аналізу та прогнозування наслідків кіберзагроз; систему науково-дослідних установ, які забезпечують науково-технічне супроводження функціонування системи аналізу стану об'єктів національної системи кібербезпеки та експертизу з оцінки прогнозування наслідків впливів на стійкість таких об'єктів [15, с. 92].

Система оцінювання ризиків і загроз Великої Британії забезпечує стратегічне планування у сфері національної безпеки. Зокрема, вона надає можливість британському урядові оцінити широкий спектр ризиків і загроз національним інтересам та безпеці країни в діапазоні коротко- та довгострокових змін безпекового середовища, визначити стратегічні цілі та пріоритетні завдання щодо забезпечення національної безпеки і стійкості [5, с.7]. За результатами оцінки ризиків у сфері національної безпеки визначаються пріоритети державної політики у сфері національної безпеки та оборони, а також національної стійкості. Передусім оцінюються загрози національній безпеці Великої Британії світового масштабу – міжнародного, воєнного, геоекономічного, геополітичного, техногенного, соціального та іншого характеру, а також ті, що пов'язані із масштабними стихійними лихами, кібербезпекою, тероризмом тощо [5, с. 10].

У Стратегії національної безпеки та Огляді стратегічної оборони і безпеки Великої Британії (2015 р.) зазначено, що протягом 2015 – 2020 рр. найбільш імовірними ризиками можуть бути: тероризм, кіберзагрози, міжнародні збройні конфлікти, посилення міжнародної нестабільності, ризики здоров'ю громадян, епідемії, пандемії, природні небезпеки стихійного характеру, зростання вразливості відкритої економіки країни [5, с. 10-11].

Важливу роль в оцінюванні ризиків і загроз відіграють такі державні установи: Об'єднаний центр з питань оцінювання терористичної загрози (Joint Terrorism Assessment Centre), Центр з питань захисту інфраструктури (Centre for the Protection of National Infrastructure), Національний центр з питань кібербезпеки (National Cyber Security Centre), Агентство з питань навколишнього середовища (Environment Agency), Метеорологічне бюро (Met Office) та ін. Усі ці установи проводять ретельні дослідження щодо ризиків і загроз, які відносяться до їх компетенції, надають фахові консультації міністерствам і відомствам [5, с. 12].

Система оцінювання ризиків і загроз у Королівстві Нідерландів є важливим елементом стратегічного планування та підґрунтям для розробки Стратегії національної безпеки. Вона охоплює низку процесів, серед яких: аналіз безпекового середовища, оцінювання ризиків і загроз, визначення довгострокових тенденцій розвитку безпекової ситуації, оцінювання спроможностей [5, с. 6]. Національне оцінювання ризиків проводиться щорічно. Крім щорічного оцінювання ризиків, у Нідерландах розпочали здійснювати сканування горизонту національної безпеки, що передбачає аналіз трендів і загроз національній безпеці у довгостроковій перспективі [5, с. 17].

Нині в Нідерландах розроблений та оприлюднений лише один Національний профіль ризиків (2016 р.)

Національна система оцінювання ризиків і загроз у Королівстві Нідерландів постійно вдосконалюється, що передбачає можливість подальшої її адаптації до змін стратегічного безпекового середовища. На сьогодні вона реалізується комплексно та послідовно у єдиному алгоритмі в рамках циклу стратегічного планування у сфері національної безпеки.

Національний координатор з питань безпеки і протидії тероризму (Nationaal Coördinator Terrorismebestrijding en Veiligheid), який діє у складі Міністерства юстиції і безпеки Королівства Нідерландів (Ministerie van Justitie en Veiligheid) як ключова установа, відповідальна за процеси забезпечення національної безпеки і стійкості, визначив такі загальні пріоритети для оцінювання ризиків і загроз національній безпеці: загрози від суб'єктів, яких спонсорують інші держави; поляризація у суспільстві; пошкодження критичної інфраструктури; тероризм, екстремізм; воєнна загроза злочинності; кіберзагрози [14].

Як ми бачимо, формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті, насамперед, протягом періоду реалізації Стратегії [1].

Для формування потенціалу стримування необхідним є досягнення стратегічних цілей Стратегії, серед яких виділяється ціль С.1. "Дієва кібероборона", задля реалізація якої Україна має створити та забезпечити розвиток підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування, забезпечити ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку

спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності [1]. Одним із шляхів реалізації таких цілей є налагодження системного обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки.

Висновки.

Як видно з аналізу Стратегії [1], ефективність її реалізації визначатиметься через чітку систему індикаторів стану кібербезпеки, яка буде включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури [1], що дасть змогу комплексно оцінювати результативність та ефективність реалізації Стратегії та прогрес, якого досягли суб'єкти забезпечення кібербезпеки в її виконанні. Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу координації діяльності із забезпечення кібербезпеки, а також моніторингу виконання Стратегії у реальному часі.

Аналіз позитивного зарубіжного досвіду показує, що найбільш ефективними є багаторівневі системи оцінювання ризиків і загроз, коли відповідний аналіз проводиться як на національному, так і на регіональному або місцевому рівні з використанням сучасних веб-ресурсів (онлайн-платформ), що свідчить про прозорість вжитих заходів для суспільства і держави.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

2. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України": Указ Президент України від 06.06.16 р. № 240. URL: https://zakon.rada.gov.ua/laws/show/240/2016#Text

3. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. № 1(24)/2018. С. 89-103.

4. Лук'янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України. Серія : Державне управління*. 2016. № 3. С. 131-137.

5. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. / Резнікова О.О., Войтовський К.Є. Лепіхов А.В. ; за заг. ред. О.О. Резнікової. Київ: НІСД, 2020. 84 с.

6. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. № 3(15)/2015. С. 36-42.

7. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія; заг. ред. Р.А. Калюжний. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

8. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

10. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

11. Rinaldi S., Peerenboom J., and Kelly T. "Idenlifying, Understanding, and Analyzing Critical Infrastructure lnterdependencies". IEEE Control Systems Magazine, IEEE, December 2001, pp. 11-25.

12. Congressional Research Service Report for Congress. Critical Infrastructures. Background, Policy and Implementation. 2002. URL: https://sgp.fas.org/crs/homesec/RL30153.pdf

13. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах. URL: http://pentagonus.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnoj_stranakh_2012/19-1-0-2082

14. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США). *Інформація і право.* № 3(34)/2020. С. 88-95.

15. Priority assessment of threats and risks: which issues require extra focus. URL: https://english.nctv.nl/topics/national-security-strategy/priority-assessmentof-threats-and-risks

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~