УДК 303.62:004:056
DOI https://doi.org/10.32782/msd/2025.1/03

ЗМІСТ ТА ОСОБЛИВОСТІ ЕКСПЕРТНОЇ ВИБІРКИ В ОЦІНЮВАННІ КІБЕРРИЗИКІВ

Демедюк С. В.
кандидат юридичних наук, заступник Секретаря
Ради національної безпеки і оборони України
ORCID ID: 0009-0008-1359-5265

Анотація. *У статті досліджено сучасні підходи до забезпечення кібербезпеки, зокрема концепцію кіберстійкості, яка включає не лише захист від атак, але й здатність організацій швидко відновлюватися після інцидентів. Проаналізовано міжнародні та національні нормативні документи, що регулюють сферу кібербезпеки. Визначено ключові загрози в кіберпросторі та необхідність упровадження ризик-орієнтованого підходу для оцінки й мінімізації потенційних небезпек. Значну увагу приділено аналітичним методам оцінки кіберризиків, які базуються на зборі даних, їх обробці та класифікації. Важливою складовою кібербезпеки є міждисциплінарний підхід, що поєднує кримінологічні, соціологічні та математичні методи для ефективного управління загрозами.*

Дослідження проводилось на основі експертного опитування представників державного сектору, правоохоронних органів, військових адміністрацій, наукових установ та підприємств критичної інфраструктури. Виявлено значну варіативність оцінки кіберзагроз залежно від досвіду фахівців, що підкреслює важливість залучення широкого експертного середовища для формування стратегічних рішень у сфері кібербезпеки.

У статті обґрунтовано необхідність розробки ефективних механізмів протидії кіберзлочинності на основі комплексного аналізу загроз та впровадження інструментів кіберстійкості. Запропоновано основні напрями розвитку національної системи кібербезпеки України, зокрема вдосконалення законодавчої бази, впровадження інноваційних технологій аналізу великих даних та розширення програм підготовки фахівців у цій сфері.

Отримані результати можуть бути використані для вдосконалення державної політики у сфері кібербезпеки, розробки нормативних документів, спрямованих на зниження кіберризиків, та створення ефективних методик оцінювання загроз. Подальші дослідження мають зосередитися на глибшому аналізі ризиків з урахуванням міжнародного досвіду та технологічних інновацій, що дозволить підвищити рівень кіберзахисту державних установ, підприємств та громадянського суспільства.

Ключові слова: *кібербезпека, кіберзагроза, кіберстійкість, ризик, оцінка ризиків, експертна вибірка.*

Demediuk S. V. CONTENT AND FEATURES OF EXPERT SAMPLING IN CYBER RISK ASSESSMENT

Abstract. *The article examines modern approaches to cybersecurity, in particular the concept of cyber resilience, which includes not only protection against attacks but also the ability of organizations to quickly recover from incidents. International and national regulatory documents governing cybersecurity are analyzed. The key threats in cyberspace and the need to implement a risk-based approach to assess and minimize potential dangers are identified. Considerable attention is paid to analytical methods of cyber risk assessment based on data collection, processing and classification. An important component of cybersecurity is an interdisciplinary approach that combines criminological, sociological, and mathematical methods for effective threat management.*

The study was conducted on the basis of an expert survey of representatives of the public sector, law enforcement agencies, military administrations, scientific institutions, and critical infrastructure enterprises. The study reveals significant variability in the assessment of cyber threats depending on the experience of specialists, which emphasizes the importance of involving a wide range of experts in the formation of strategic decisions in the field of cybersecurity.

The article substantiates the need to develop effective mechanisms for countering cybercrime based on a comprehensive threat analysis and implementation of cyber resilience tools. The author proposes the main directions of development of the national cybersecurity system of Ukraine, in particular, improvement of the legislative framework, introduction of innovative technologies for big data analysis and expansion of training programs for specialists in this area.

The results obtained can be used to improve the state policy in the field of cybersecurity, develop regulations aimed at reducing cyber risks, and create effective threat assessment methods. Further research should focus on a deeper analysis of risks, taking into account international experience and technological innovations, which will increase the level of cyber defense of government agencies, enterprises and civil society.

Key words: *cybersecurity, cyber threat, cyber resilience, risk, risk assessment, expert sample.*

Постановка проблеми. Зростаюча залежність від цифрових технологій і на цій основі постійно зростаючі загрози в кіберпросторі потребують розвитку сучасних підходів до формування безпекового кіберпростору. Багато країн прийняли відповідні закони та регламенти, що зобов'язують організації забезпечувати належний рівень кібербезпеки та захисту даних. Але ключовим інструментом кібербезпеки у теперішній час є так звана система «кіберстійкості», яка набуває все більшої актуальності в сучасному світі [1–4].

Кіберстійкість включає не лише захист від атак, але й здатність організації швидко відновлюватися після інциденту та продовжувати функціонувати. Це вимагає комплексного підходу, включаючи технологічні рішення, процеси управління ризиками та підвищення обізнаності персоналу [5–7]. У свою чергу, управління ризиками розпочинається з відповідного аналітичного процесу – оцінювання ризиків, що також передбачає вирішення додаткових задач: збір даних, їх групування, обробка тощо [8–10].

Безпосередній аналітичний процес, що базується на сучасному глибокому статистичному аналізі, вирішує низку питань щодо надійності даних та репрезентативності статистичних висновків. Використовуючи експертне середовище, важливо враховувати думку різних експертних груп, яка може бути певним чином відмінною у залежності від регіону, сфери поширення загроз, а також фахового рівня експертів тощо. Зазначене надзвичайно важливо враховувати при розробленні стратегій та концепцій, тобто при здійсненні стратегічного аналізу, що формує певну особливу експертну думку, яку необхідно враховувати та розробляти на її основі специфічні завдання кіберзахисту.

Метою статті є розвідки у сфері кібербезпеки з акцентуванням уваги на досліджені особливостей аналізу та напрацюванні системи знань щодо кіберзлочинності. Усвідомлення сучасних трендів та реального пізнання ключових кіберзагроз, на основі оцінювання ризиків їх поширення, із врахуванням особливостей експертної вибірки, дасть можливість охарактеризувати напрями для формування реально дієвих механізмів ризик-орієнтованого підходу [11-13] щодо забезпечення кібербезпеки сучасного українського суспільства, що, у свою чергу, сформує достатній масив знань для формування обґрунтованих пропозицій щодо протидії кіберзлочинності.

В останні роки, у дослідженнях багатьох відомих вітчизняних дослідників, значна увага приділяється різним проблемам, пов'язаним з розробкою напрямів щодо кібербезпеки, зокрема протидії кіберзлочинності: Баранова О.А. [14], Бєлякова К.І. [15], Бірюкова Д.С., Бутузова В.М., Гнатюка С.О. [16], Горбуліна В., Довганя О.Д. [17], Дубова Д.В., Кормича Б.А., Корченка О.Г. [18], Лісовської Ю.П., Марущака А.І. [19], Пилипчука В.Г., Тихомирова О.О., Хахановського В.Г., Цимбалюка В.С., Швеця М.Я. та інших. Разом з тим, розуміння реального стану та упровадження адекватної державної політики у цій сфері потребує компетентного розвідувального аналітичного процесу, усвідомлення сучасних трендів й реального пізнання ключових кіберзагроз й на цій основі формування стратегії кіберстійкості. Важливе місце у цій системі займає оцінювання ризиків поширення кіберзагроз. При цьому важливо враховувати думки різноманітних груп експертів, формуючи при цьому реально дієвий механізм ризик-орієнтованого підходу щодо забезпечення кібербезпеки [20].

Виклад основного матеріалу. Високі новітні технології окрім технологічного розвитку цивілізації несуть також і загрози глобального характеру, що характеризуються значним руйнівним потенціалом та можуть призвести до складних наслідків для життєдіяльності будь-якого суспільства. Врахування таких змін, моніторинг загальних тенденцій є невід'ємним елементом сучасного світового розвитку, зокрема і щодо впровадження механізмів забезпечення кібербезпеки [21].

Сфера кібербезпеки, характеризується новаціями як загальнонаукового, так і спеціального змісту, що формує відповідну систему знань для прогнозування розвитку подій та поширення кіберзагроз, і ключовим інструментом у цій системі є саме управління ризиками. Свого часу, Резолюція генеральної асамблеї ООН, започаткувала у межах розвитку глобальної культури кібербезпеки,

упровадження механізмів управління ризиками – *учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації і її захисту* [22].

Україна також активно розвивається в цьому напрямі, реалізуючи державну політику із врахуванням міжнародних стандартів, у Стратегії національної безпеки України, введеної в дію Указом Президента України від 14 вересня 2020 року № 392/2020 [23], зазначено, що Україна *запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей, а також поширення необхідних знань і навичок у цій сфері*. Про ризик-орієнтований підхід щодо забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021–2025 років [24], а у Плані реалізації Стратегії кібербезпеки [25] (далі *План реалізації Стратегії*) чітко визначено завдання: *«Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки ... розробити методики ідентифікації та оцінки кіберризиків ..., забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик».*

Вочевидь, упровадження сучасних методологій потребує відповідного наукового супроводження, більше того, аналіз стратегічного характеру, що базується на емпіричній базі, сформованій широкою експертною думкою, реалізується безпосередньо в межах не лише кримінології, а й соціології, статистики та науки про дані (*Data Science*), що вимагає дотримання методологічних вимог. Саме тому, на нашу думку, є усі підстави стверджувати, що такі завдання вирішуються переважно в межах прикладного наукового дослідження, із врахуванням дослідницького досвіду та напрацюванням відповідної методології й інструментарію обробки та аналізу великих даних (Big Data).

У межах підготовки пропозицій до розроблення нової Стратегії кібербезпеки, у 2024 році було започатковано дослідницький проект «Система кіберстійкості в Україні» та визначено наступні завдання:

– ідентифікація кіберзагроз та оцінювання ризиків поширення їх в Україні;

– визначення індикаторів, що характеризують інституційну спроможність кіберсистеми та кіберстійкість в Україні;

– побудова прогнозної моделі на основі регресійного аналізу.

Для проведення дослідження обрано ризик-орієнтований підхід у якості базового, який, на нашу думку, став основою для дослідження за обраним напрямом. Базовими засадами для реалізації визначених завдань оцінювання ризиків є міжнародний стандарт, імплементований до вітчизняного законодавства, так як у 2018 році прийнятий як національний стандарт, – ДСТУ ISO 31000:2018 [26].

На цій основі розроблено відповідний опитувальник, відповіді на запитання якого були конфіденційними і не потребували розкриття особистих даних експертів. Опитування проводилось в режимі ON-LINE шляхом заповнення анкет, в яких кожен індикатор оцінювався за двома характеристиками: «Ймовірність (Рівень оцінювання)» та «Можливі наслідки (Вплив)» за 3-4-5–бальною шкалою.

Для забезпечення комплексності аналізу, системного бачення проблем, врахування специфіки поширення кіберзагроз важливим вбачалося відображення специфіки регіону мешкання, власного досвіду та обізнаності респондентів щодо сфери кібербезпеки України тощо.

За суб'єктом, який представляє експерт (табл. 1) найбільшу частку склали представники обласних військових адміністрацій (20,1%), районних військових адміністрацій (8,5%), які сукупно сформували майже третину генеральної експертної сукупності.

Значною експертною вибіркою характеризуються групи представників об'єктів критичної інфраструктури (15,8%), правоохоронних органів (15,5%), Державної служби спецзв'язку та захисту інформації України (далі ДСТЗІ) (13,3%) та центральних органів виконавчої влади (далі ЦОВВ) (13,0%).

Таблиця 1

Розподіл експертів за суб'єктом (органом)

Суб'єкт (орган)	%
Національний координаційний центр кібербезпеки (РНБО)	0,6
Кабінет міністрів України	0,2
міністерство або інший центральний орган виконавчої влади	13,0
Державна служба спецзв'язку та захисту інформації України	13,3
обласна військова адміністрація	20,1
районна військова адміністрація	8,5
правоохоронний орган	15,5
розвідувальний орган	0,8
контррозвідувальний орган	0,2
постачальник ІКТ послуг	0,5
критична інфраструктура	15,8
громадська організація	0,6
освітня (наукова) установа	10,6

Водночас, недостатньо охопленими виявились експертні групи з представників розвідувальних та контррозвідувальних органів (0,8% та 0,2% – відповідно), підприємств-постачальників ІКТ послуг (0.5%) та фахового спрямування громадських організацій (0,6%).

Опитуванням було охоплено усі регіони України (табл. 2), серед яких майже третину даних сформовано експертною думкою столичного регіону (Київ – 31,9%).

Загалом представники усіх регіонів прийняли участь в опитуванні але з певною перевагою з Донецької (тимчасово переміщених) (14,3%), Київської (6,6%), Івано-Франківської (6,3%), Херсонської (5,4%) та Чернівецької (5,1%) областей.

Опитуванням охоплено і експертів, які представляють різні галузі та сфери (табл. 3).

Найбільша експертна вибірка представляє державне управління (40,1%), телекомунікаційні (30,5%) та цифрові (17,2%) послуги. Значно меншою, але все ж наявною є думка експертів оборонно-промислового (4,8%) та енергетичного (3,3%) комплексів, а також інфраструктура (транспорт) (2,2%) та фінансова система (1,8%).

Окремий інтерес викликає аналіз експертної вибірки за досвідом діяльності у сфері кібербезпеки (табл. 4).

Найбільшою групою експертів у генеральній експертній сукупності виявились фахівці

Таблиця 2

Регіональний розподіл експертного середовища

Регіон	%
Вінницька обл.	1,7
Волинська обл.	0,9
Донецька обл.	14,3
Дніпропетровська обл.	1,7
Житомирська обл.	0,5
Закарпатська обл.	1,4
Запорізька обл.	1,9
Івано-Франківська обл.	6,3
м.Київ	31,9
Київська обл.	6,6
Кіровоградська обл.	1,3
Луганська обл.	0,8
Львівська обл.	3,2
Миколаївська обл.	0,7
Одеська обл.	1,8
Полтавська обл.	1,6
Рівненська обл.	1,0
Сумська обл.	3,8
Тернопільська обл.	0,9
Харківська обл.	2,3
Херсонська обл.	5,4
Хмельницька обл.	1,4
Черкаська обл.	1,1
Чернівецька обл.	5,1
Чернігівська обл.	2,7

Таблиця 3

Галузевий розподіл експертного середовища

Галузь діяльності	%
державне управління	40,1
енергетичний комплекс	3,3
фінанси/банки/страхування	1,8
інфраструктура/транспортна система	2,2
телекомунікаційні послуги	30,5
цифрові послуги	17,2
оборонно-промисловий комплекс	4,8

Таблиця 4

Експертна вибірка за досвідом діяльності у сфері кібербезпеки

Досвід діяльності за фахом кібербезпеки	%
до 1 року	37,3
1–3 роки	27,6
3–10 років	23,3
10–20 років	8,2
понад 20 років	3,7

з досвідом до 1-го року (37,3%) та в інтервалі 1–3 років (27,6%). Достатньо помітною у відносному значенні також є група експертів з досвідом 3–10 років (23,3%). Водночас, найменш вираженою експертна вибірка з досвідом 10–20 років (8,2%) та понад 20 років (3,7%). Такий розподіл, на нашу думку, є закономірним, так як відображає переважно експертне середовище державного сектору суб'єктів представлених у дослідженні (орієнтовно близько 80% за даними табл. 1).

Одним з результатів стало те, що було оцінено ризики поширення кіберзагроз та визначено ті з них, що характеризуються найвищим рівнем (рис. 1). Водночас, в межах дослідницького інтересу, варто, перш за все, звернути увагу на варіативність оцінювання кіберзагроз за середнім значенням генеральної експертної сукупності та вибірки на основі виділення експертних груп за досвідом фахової діяльності у сфері кібербезпеки.

За середнім значенням, в межах генеральної експертної сукупності, оцінювання ризиків поширення кіберзагроз є достатньо варіативним і певним чином формує базові засади виявлення найзначніших загроз та визначення пріоритетних напрямів у формуванні стратегічного бачення в системі кібербезпеки.

Водночас, використовуючи додаткові дані, що характеризують ризики сформовані на основі експертної вибірки за ознакою досвіду фахової діяльності у сфері кібербезпеки, достатньо помітними є певні розбіжності в оцінюванні рівня ризику за окремими кіберзагрозами (рис. 2).

Як бачимо, певною варіативністю характеризується і оцінювання ризиків поширення

Рис. 1. Варіативність оцінювання кіберзагроз за середнім значенням генеральної експертної сукупності

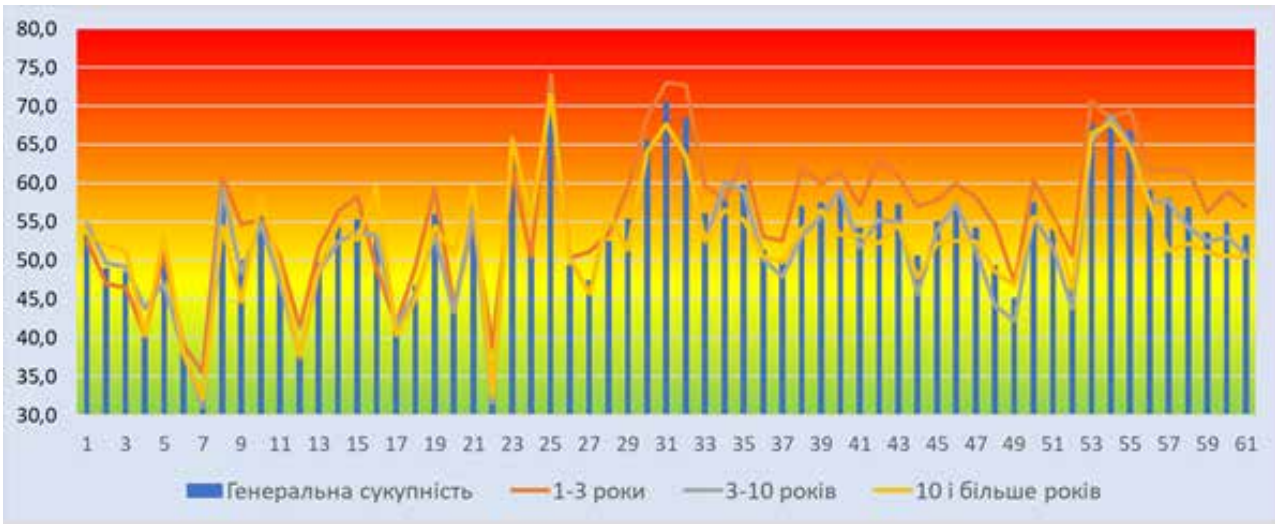

Рис. 2. Варіативність оцінювання кіберзагроз за експертною вибіркою щодо досвіду фахової діяльності у сфері кібербезпеки

кіберзагроз між різними групами експертів, які розподіляються за фаховим рівнем у сфері кібербезпеки.

Зазначений підхід вказує на необхідність у подальшому більш глибокого аналізу кіберзагроз із врахуванням особливостей експертної вибірки. Саме такий підхід дає можливості більш глибоко досліджувати тенденції поширення кіберзагроз на основі ризик-орієнтованого підходу, і як наслідок більш обґрунтовано підходити до формування стратегічних напрямів у сфері кібербезпеки та враховувати специфіку й певну особливість думок експертного середовища.

Висновки. Сучасна кібербезпека потребує комплексного підходу, що включає розвиток кіберстійкості, управління ризиками та стратегічний аналіз загроз. Головним інструментом є ризик-орієнтований підхід, що базується на зборі та обробці аналітичних даних. Україна активно розвиває державну політику у сфері кібербезпеки, імплементуючи міжнародні стандарти. Дослідження показують, що оцінка кіберзагроз варіюється залежно від досвіду та спеціалізації експертів. Важливим є врахування регіональних та галузевих особливостей, що дозволяє формувати ефективні механізми захисту. Створення прогнозних моделей, заснованих на статистичному та регресійному аналізі, є ключовим етапом у боротьбі з кіберзлочинністю. Розвиток наукового супроводу, використання технологій аналізу великих даних та залучення широкого кола експертів сприятимуть посиленню кіберстійкості держави та суспільства.

Література:

1. Holling C.S. Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*. 1973. vol. 4(1), p. 1–23.

2. Woods D.D. Essential characteristics of resilience. Pp. 21–34 in Hollnagel, E., Woods, D.D., Leveson, N. & (eds.). 2006. Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Press,.

3. Rose A., Liao S. Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. *Journal of Regional Science*. 2005. vol. 45(1), p.75–112.

4. Westrum R. A typology of resilience situations. Pp. 49–60 in Hollnagel E, Woods, D.D., Leveson, N. & (eds.) (2006). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Press.

5. Hollnagel E., Woods D.D., Leveson N. (eds.) Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Press. 2006.

6. Waller M.A. Resilience in ecosystemic context: evolution of the concept. *American Journal of Orthopsychiatry*. 2001.vol. 71, p. 290–297.

7. Software Engineering Institute (SEI). CERT Resiliency Engineering Framework, Preview version, v0.95R, 2008. URL: http://www.cert.org/resiliency engineering

8. Haimes Y.Y. On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis*. 2006. vol. 26(2), p. 293–296.

9. Haimes Y.Y. On the Definition of Resilience in Systems. *Risk Analysis*. 2009. vol. 29, no. 4. p. 498–501. DOI: 10.1111/j.1539-6924.2009.01216.x.

10. Haimes Y.Y. Risk Modeling, Assessment, and Management, 3rd ed. New York: Wiley. 2009.

11. Roger Hurwitz. Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. *Georgetown Journal of International Affairs: Georgetown University.* 2014.

12. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30 грудня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

13. Користін О.Є., Свиридюк Н.П. Методологічні засади оцінювання ризиків в правоохоронній діяльності. *Наука і правоохоронна*. № 3. 2020. С. 191–197.

14. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. Київ: Видавничий дім «СофтПрес», 2005. 316 с.

15. Бєляков К.І. Інформація в праві: теорія і практика: монографія. Київ: Видавництво «КВІЦ», 2006. 116 с.

16. Гнатюк С.О. Методологія формування та забезпечення державної системи кібербезпеки в галузі цивільної авіації. Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доп. III міжнар. наук.-практ. конф., 22–25 лютого 2017 р. Київ, 2017. С. 65–67.

17. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: Видавничий дім «АртЕк», 2017. 107 с.

18. Корченко О., Казмірчук С., Ахметов Б. Прикладні системи оцінювання ризиків інформаційної безпеки: монографія, Київ: ЦП Компринт, 2017. 435 с.

19. Марущак А.І. Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика*. 2009. № 1(21). С. 65–71.

20. Користін О.Є., Веселова Л.Ю. Ризикорієнтованість кібербезпеки. *Наука і правоохоронна*. 2021. № 3. С. 16–23.

21. Директива Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA

22. Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement

23. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

24. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

25. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 01 лютого 2022 року №37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text

26. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf

References:

1. Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4(1), 1–23.

2. Woods, D. D. (2006). Essential characteristics of resilience. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience Engineering: Concepts and Precepts* (pp. 21–34). Aldershot, UK: Ashgate Press.

3. Rose, A., & Liao, S. (2005). Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. *Journal of Regional Science*, 45(1), 75–112.

4. Westrum, R. (2006). A typology of resilience situations. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience Engineering: Concepts and Precepts* (pp. 49–60). Aldershot, UK: Ashgate Press.

5. Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate Press.

6. Waller, M. A. (2001). Resilience in ecosystemic context: Evolution of the concept. *American Journal of Orthopsychiatry*, 71, 290–297.

7. Software Engineering Institute (SEI). (2008). CERT Resiliency Engineering Framework, Preview version, v0.95R. Retrieved from http://www.cert.org/resiliencyengineering

8. Haimes, Y. Y. (2006). On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis*, 26(2), 293–296.

9. Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis*, 29(4), 498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

10. Haimes, Y. Y. (2009). Risk Modeling, Assessment, and Management (3rd ed.). New York: Wiley.

11. Hurwitz, R. (2014). Keeping cool: Steps for avoiding conflict and escalation in cyberspace. *Georgetown Journal of International Affairs*. Georgetown University.

12. Verkhovna Rada Ukrainy. (2021). Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy [On the Plan for Implementing the Cybersecurity Strategy of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

13. Korystin, O. Ye., & Svyrydyuk, N. P. (2020). Metodolohichni zasady otsiniuvannia ryzykiv v pravookhoronnii diialnosti [Methodological principles of risk assessment in law enforcement activities]. *Nauka i pravoohoronna*, 3, 191–197. [in Ukrainian].

14. Baranov, O. A. (2005). Informatsiine pravo Ukrainy: stan, problemy, perspektyvy [Information law of Ukraine: Status, problems, prospects]. Kyiv: SofPress. [in Ukrainian].

15. Belyakov, K. I. (2006). Informatsiia v pravi: teoriia i praktyka [Information in law: Theory and practice]. Kyiv: KVITS. [in Ukrainian].

16. Hnatyuk, S. O. (2017). Metodolohiia formuvannia ta zabezpechennia derzhavnoi systemy kiberbezpeky v haluzi tsyvilnoi aviatsii [Methodology of formation and implementation of the state cybersecurity system in civil aviation]. Aktualni pytannia zabezpechennia kiberbezpeky ta zakhystu informatsii: Proceedings of the III International Scientific and Practical Conference (pp. 65–67). Kyiv. [in Ukrainian].

17. Dovhan, O. D., & Doronin, I. M. (2017). Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu [Escalation of cyber threats to national interests of Ukraine and legal aspects of cybersecurity]. Kyiv: Artek. [in Ukrainian].

18. Korchenko, O., Kazmirchuk, S., & Akhmetov, B. (2017). Prykladni systemy otsiniuvannia ryzykiv informatsiinoi bezpeky [Applied risk assessment systems for information security]. Kyiv: CP Komprint. [in Ukrainian].

19. Marushchak, A. I. (2009). Informatsiini resursy derzhavy: zmist ta problema zakhystu [Information resources of the state: Content and protection issues]. *Pravova informatyka*, 1(21), 65–71. [in Ukrainian].

20. Korystin, O. Ye., & Veselova, L. Yu. (2021). Ryzykorientovanist kiberbezpeky [Risk orientation of cybersecurity]. *Nauka i pravoohoronna*, 3, 16–23. [in Ukrainian].

21. European Parliament and Council. (2016). Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems across the Union. Retrieved from https://zakon.rada.gov.ua/laws/show/984_013-16

22. United Nations General Assembly. (2002). Resolution 57/329. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement

23. Verkhovna Rada Ukrainy. (2020). Pro Stratehiiu natsionalnoi bezpeky Ukrainy [On the National Security Strategy of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/392/2020#Text

24. Verkhovna Rada Ukrainy. (2021). Pro Stratehiiu kiberbezpeky Ukrainy [On the Cybersecurity Strategy of Ukraine]. Retrieved from https://www.president.gov.ua/documents/4472021-40013

25. Verkhovna Rada Ukrainy. (2022). Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy [On the Plan for Implementing the Cybersecurity Strategy of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/37/2022#Text

26. Ukrainian Standardization Institute. (2018). DSTU ISO 31000:2018 Menedzhment ryzykiv. Printsypy ta nastanovy [Risk Management. Principles and Guidelines] (ISO 31000:2018, IDT). Retrieved from https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf