DOI: *https://doi.org/10.37405/2221-1187.2024.242-248*
УДК 007:004

В. С. Дяченко, *к.е.н., доц.*
ORCID 0000-0002-0055-9256
e-mail: dyachenko.v@ukr.net,
Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія»

ОСОБЛИВОСТІ ФОРМУВАННЯ КІБЕРБЕЗПЕКИ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Актуальність проблеми. Інформаційна сфера життєдіяльності людей, знаходячись під впливом динамічного розвитку інформаційних технологій, набуває нових, зокрема, віртуальних, середовищ різноманітних просторів, які здійснюють інтенсивний вплив на суспільну діяльність та набувають все більшої значущості у міжнародних і міждержавних відносинах, в екзогенній та ендогенній діяльності підприємств, установ та організацій, у спілкуванні громадян.

Аналіз останніх досліджень і публікацій. Дослідженню проблеми формування кібербезпеки з урахуванням ризиків, загроз та небезпек присвятили відомі вітчизняні науковці, зокрема особливості проявів ризиків при формуванні кібернетичної безпеки в умовах пандемії ідентифікували М. Василенко, В. Новіков, В. Рачук та В. Слатвінська [1, с. 30-39]. Генезу ризиків та їх інформаційної складової деталізували М. Василенко та О. Козін [2, с. 43-51]. Кіберризики та особливості формування кібербезпеки при роботі з великими обсягами даних дослідили у своїй роботі F. Cremer, B. Sheehan та M. Fortmann [3].

Метою дослідження є ідентифікація особливостей формування кібербезпеки з урахуванням ризиків в умовах сучасних викликів.

Виклад основного матеріалу дослідження. Розвиток інформаційних технологій, інтенсифікуючи процеси отримання, обробки та зберігання інформації, обумовив потребу забезпечення захисту інформації, приватної, комерційної, державної.

Інформація, як потужна сила в суспільному середовищі, має потенціал для дестабілізації суспільства, а відтак, може бути джерелом політичних і соціальних загроз.

На сьогодні стан інформаційної безпеки характеризується зростанням використання окремими державами та міжнародними організаціями інформаційних технологій у воєнній сфері та міжнародними організаціями інформаційних технологій у воєнно-політичних цілях, зокрема для здійснення дій, що суперечать міжнародному праву, спрямованих на підрив суверенітету політичної та соціальної стабільності, територіальної цілісності та створюють загрозу миру, глобальній та регіональній безпеці.

Держави почали нарощувати потенціал у кіберпросторі, оскільки це – базовий чинник стабільного економічного державного розвитку.

Формування економічної та інформаційної безпеки є базовими функціями держави, та, як зазначено у Конституції України (стаття 17) [4] – справою всього Українського народу, адже, загрози національній безпеці в інформаційній сфері, особливо в аспекті протидії руйнівному інформаційному впливу в умовах новітніх технологій гібридної війни, викликів глобалізації та вільного обігу інформації актуалізують потребу інноваційних підходів до формування системи захисту та розвитку інформаційного простору.

Інформаційна безпека, як невід'ємна складова кожної зі сфер національної безпеки, є запорукою сталого розвитку та економічного зростання. Стратегією інформаційної безпеки [5], затвердженої 21.12.2021 р. передбачено формування передумов щодо забезпечення інформаційної безпеки держави, її інформаційного простору з метою захисту державного суверенітету.

Оперативний доступ до відкритої оперативної достовірної є неймовірно актуальним, особливо в умовах правового режиму воєнного стану в Україні. Адже саме наявність такої інформації формує суспільну думку, віру й впевненість громадян у перемогу, суспільну довіру до органів державної влади.

Інформація – стратегічний ресурс, саме тому питанню захисту інформації в умовах правового режиму воєнного стану приділяється так багато уваги, зокрема:

– Указом Президента України від 24.02.2022 р. передбачено ряд обмежень щодо доступу до публічної інформації [6];

– Законом України від 24.03.2024 р. [7] зокрема передбачено кримінальну відповідальність за поширення інформації щодо переміщення чи розміщення Збройних Сил України.

Формування інформаційної безпеки в умовах воєнного стану є комплексною політико-правовою та практичною діяльністю

суб'єктів владних повноважень, спрямованою на захист держави, суспільства і людини.

Відстоювання територіальної цілісності та захист інтересів національної безпеки є базовими функціями держави. Наразі перед органами публічної влади в Україні постали завдання формування безпечних умов функціонування підприємств, установ та організацій в сучасних умовах воєнного стану, та забезпечення населенню безпечних умов життєдіяльності.

У сучасних умовах інформаційного суспільства доступ до публічної інформації є нагальною потребою кожного.

Конституцією України (стаття 40), Конвенцією Ради Європи (ратифіковано із заявами Законом України від 20.05.2020 р. № 631-IX) про доступ до офіційних документів [8] та Законом України «Про доступ до публічної інформації» від 13,01.2011 р. № 2939-VI гарантовано право громадян на звернення до суб'єктів владних повноважень й отримання відповіді та передбачено, що в умовах воєнного стану, з метою захисту інтересів національної безпеки, доступ до публічної інформації може бути обмежений.

На період дії правового режиму воєнного стану можуть обмежуватися конституційні права та свободи, передбачені рядом статей Конституції України.

За таких умов певні органи публічної влади, призупинивши надання відповідей на запити та звернення громадян щодо деяких аспектів суспільного життя, що обумовлено, зокрема й тим, що вони, відповідно Закону України «Про правовий режим воєнного стану» від 12.05.2015 р. № 389-VIII, у першу чергу здійснюють заходи, спрямовані на формування національної безпеки, водночас оперативно оновлюють поточну суспільно важливу інформацію на сайтах, у ЗМІ та соціальних мережах, зокрема про стан довкілля та надзвичайні події, які стались чи можуть статись та загрожують безпеці життєдіяльності громадян.

В умовах воєнного стану реалізація громадянами прав на доступ до публічної інформації може ускладнитись у зв'язку урахуванням ризиків:

– запровадження комендантської години;

– здійснення контрою за змістом та легітимністю надання інформації;

– охорони об'єктів державного значення та впровадженням особливого режиму;

– призупинення оновлення баз даних та державних реєстрів тощо.

У той же час здійснюється системний парламентський контроль щодо дотримання прав громадян на доступ до публічної інформації, зокрема в Рекомендаціях Уповноваженого Верховної Ради України з прав людини з питань додержання конституційного права людини і громадянина на доступ до інформації [10], деталізовано загальні особливості таких обмежень.

Потреба ж громадян в оперативній та достовірній інформації в умовах воєнного стану стає надзвичайно необхідною, особливо про гуманітарну допомогу, надання безоплатних послуг, консультацій чи потребу у волонтерах.

З урахуванням умов воєнного часу, за яких суб'єкти владних повноважень, приділяючи максимум уваги та часу організації та впровадженню заходів щодо формування національної безпеки, збереження життя та майна населення, підтримання безперебійного функціонування життєво необхідної інфраструктури, пропонують з запитуваною інформацією ознайомитись у відкритих джерелах, якщо вона оприлюднена, чи надіслати відповіді на запити та звернення громадян щодо деяких аспектів суспільного життя не в друкованому, а в електронному вигляді, використовуючи можливості сучасних інформаційних технологій, що значно економить час та ресурси.

Сучасні інформаційні технології (*англ.* the information technologies), як сукупність засобів, методів та прийомів створення, накопичення, зберігання, оприлюднення, подання та передавання повідомлень, сприяючи розширенню сфери знань, інтенсифікації комунікаційних процесів, забезпеченню ефективності організації суспільної діяльності окреслюють потребу нейтралізації загроз, серед яких: доступ сторонніх осіб до конфіденційної/секретної інформації, порушення/припинення роботи комп'ютерної інформаційної системи, спотворення/знищення даних тощо. А відтак, кібербезпека є необхідною передумовою розвитку інформаційного суспільства [11].

Забезпечення кібербезпеки – системи засобів, стратегій, принципів, гарантій, технологій та підходів до управління ризиками, відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 р. № 447/2021 [12] є одним із пріоритетів у системі національної безпеки, адже передбачає протидію кіберзагрозам у сучасному безпековому середовищі.

Посеред основних загроз для користувачів у процесі використання комп'ютерних мереж виділять ряд ризиків, які за ступенем припустимості розподіляють на:

– знехтуваний характеризується незначними та допустимими відхиленнями;

– прийнятний в межах характеристик наявної техніки;

– гранично допустимий не повинен перевищуватись ні при яких обставинах;

– надмірний здебільшого, призводить до негативних наслідків.

Серед базових загроз у процесі використання ІТ виокремлюють:

– комунікаційні ризики, серед яких булінг;

– контентні ризики (матеріали шкідливого характеру);

– споживчі ризики, що пов'язані з порушенням прав споживачів;

– технічні ризики (шкідливі програми тощо).

Актуальним наразі є питання виявлення, ідентифікації, оцінки ризиків та загроз в ІТ-проєктах. Усуненню чи нейтралізації їх сприяє науково обґрунтоване поєднання методів прогнозування з інструментами управління ризиками.

Висновки та перспективи подальших досліджень. В умовах правового режиму воєнного стану в Україні фахівці фіксують збільшення кіберінцидентів та кібератак на державні інформаційні системи, об'єкти критичної інфраструктури.

Процес формування засад інформаційної та кібернетичної безпеки з урахуванням ризиків сьогодення необхідно здійснювати системно з урахуванням необхідності здійснення системного моніторингу екзогенного й ендогенного інформаційного простору.

Література

1. Василенко М. Д., Новіков В.П., Рачук, В. О., Слатвінська В. М. Кібербезпека в проявах ризиків у період пандемії: стан та генеза. *Вісник Черкаського державного технологічного університету*. 2020. № 3. С. 30-39. DOI: https://doi.org/10.24025/2306-4412.3.2020.214774.

2. Василенко М. Д., Козін О. Б. Право в теорії ризиків: від генеза ризиків від правової до інформаційної складових (інституційний підхід). *Юридичний вісник*. 2019. № 4. С. 43-51.

3. Cremer F., Sheehan B., Fortmann M. et al. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice*. 2022. Vol. 47(3). P. 698-736. DOI: https://doi.org/10.1057/s41288-022-00266-6.

4. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

5. Стратегія інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text.

6. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 р. № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text.

7. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24.03.2022 р. № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2227-19#Text.

8. Конвенція Ради Європи про доступ до офіційних документів. URL: https://zakon.rada.gov.ua/laws/show/994_001-09#Text.

9. Про правовий режим воєнного стану: Закон України від 12.05.2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/ laws/show/389-19#Text.

10. Рекомендації Уповноваженого Верховної Ради з прав людини з питань додержання конституційного права людини й громадянина на доступ до інформації. URL: https://rm.coe.int/recomendations-final-10-02-21/1680a165f7.

11. Дяченко В. С., Дяченко Н. П., Кочегаров В. С., Безверхий В. А. Державна політика у сфері інформаційної безпеки. *Розумовскі зустрічі*: зб. наук. пр. 2023. Вип. 10. С. 31-41. DOI: https://doi.org/10.5281/zenodo.8281186.

12. Стратегія кібербезпеки в Україні: Указ Президента України від 24.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

References

1. Vasylenko. M. D., Novikov. V. P., Rachuk, V. O., Slatvinska. V. M (2020). Kiberbezpeka v proiavakh ryzykiv u period pandemii: stan ta heneza [Cybersecurity in the manifestations of risks during the pandemic: status and genesis]. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu – Bulletin of Cherkasy State Technological University*, 3, pp. 30-39. DOI: https://doi.org/10.24025/2306-4412.3.2020.214774 [in Ukrainian].

2. Vasylenko, M. D., Kozin, O. B. (2019). Pravo v teorii ryzykiv: vid heneza ryzykiv vid pravovoi do informatsiinoi skladovykh (instytutsiinyi pidkhid) [Law in risk theory: from the genesis of risks from legal to informational components (institutional approach)]. *Yurydychnyi visnyk – Legal Bulletin*, 4, pp. 43-51. DOI: https://doi.org/10.32837/yuv.v0i4.945 [in Ukrainian].

3. Cremer F., Sheehan B., Fortmann M., et al. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice*, vol. 47(3), pp. 698-736. DOI: https://doi.org/10.1057/s41288-022-00266-6.

4. Konstytutsiia Ukrainy [Constitution of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/254% D0%BA/96-%D0%B2%D1%80#Text [in Ukrainian].

5. Stratehiia informatsiinoi bezpeky [Information security strategy] .(2021). Retrieved from https://zakon.rada.gov.ua/laws/show/n0080525-21#Text [in Ukrainian].

6. Pro vvedennia voiennoho stanu v Ukraini: Ukaz Prezydenta Ukrainy vid 24.02.2022 r. № 64/2022 [On the introduction of martial law in Ukraine: Decree of the President of Ukraine dated February 24, 2022 No. 64/2022]. Retrieved from https://zakon.rada.gov.ua/laws/show/64/2022#Text [in Ukrainian].

7. Pro vnesennia zmin do Kryminalnoho ta Kryminalnoho protsesualnoho kodeksiv Ukrainy shchodo zabezpechennia protydii nesanktsionovanomu poshyrenniu informatsii pro napravlennia, peremishchennia zbroi, ozbroiennia ta boiovykh prypasiv v

Ukrainu, rukh, peremishchennia abo rozmishchennia Zbroinykh Syl Ukrainy chy inshykh utvorenykh vidpovidno do zakoniv Ukrainy viiskovykh formuvan, vchynenomu v umovakh voiennoho abo nadzvychainoho stanu: Zakon Ukrainy vid 24.03.2022 r. № 2160-IX [On Amendments to the Criminal and Criminal Procedural Codes of Ukraine to Ensure Counteraction to the Unauthorized Dissemination of Information on the Sending, Transfer of Weapons, Armaments and Ammunition to Ukraine, the Movement, Relocation or Deployment of the Armed Forces of Ukraine or Other Military Formations Formed in Accordance with the Laws of Ukraine, Committed in Conditions of Martial Law or a State of Emergency: Law of Ukraine No. 2160-IX of March 24, 2022]. Retrieved from https://zakon.rada.gov.ua/laws/show/2227-19#Text [in Ukrainian].

8. Konventsiia Rady Yevropy pro dostup do ofitsiinykh dokumentiv [Council of Europe Convention on Access to Official Documents]. Retrieved from https://zakon.rada.gov.ua/laws/show/994_001-09#Text [in Ukrainian].

9. Pro pravovyi rezhym voiennoho stanu: Zakon Ukrainy vid 12.05.2015 r. № 389-VIII [On the legal regime of martial law: Law of Ukraine dated 12.05.2015 No. 389-VIII]. Retrieved from https://zakon.rada.gov.ua/laws/show/389-19#Text [in Ukrainian].

10. Rekomendatsii Upovnovazhenoho Verkhovnoi Rady z prav liudyny z pytan doderzhannia konstytutsiinoho prava liudyny y hromadianyna na dostup do informatsii [Recommendations of the Verkhovna Rada Commissioner for Human Rights on compliance with the constitutional right of a person and a citizen to access information]. Retrieved from https://rm.coe.int/recomendations-final-10-02-21/1680a165f7 [in Ukrainian].

11. Diachenko, V. S., Diachenko, N. P., Kocheharov, V. S., Bezverkhyi, V. A. (2023). Derzhavna polityka u sferi informatsiinoi bezpeky [State policy in the sphere of information security]. *Rozumovski zustrichi – Rozumovski meetings*, Vol. 10, pp. 31-41. DOI: https://doi.org/10.5281/zenodo.8281186 [in Ukrainian].

12. Stratehiia kiberbezpeky v Ukraini: Ukaz Prezydenta Ukrainy vid 24.08.2021 r. № 447/2021 [Cybersecurity Strategy in Ukraine: Decree of the President of Ukraine dated August 24, 2021 No. 447/2021]. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

Надійшла до редакції: 11.11.2024 р.
Рецензовано: 29.11.2024 р.