УДК 351.862.4:340.13
DOI https://doi.org/10.32782/pyuv.v5.2023.14

М. В. Сокіран
orcid.org/0000-0002-1682-2012
кандидат юридичних наук,докторант
Науково-дослідного інституту публічного права

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Актуальність дослідження кращих практик щодо захисту критичної інформаційної інфраструктури ще раз довела найбільша хакерська атака на національного мобільного оператора України – Київстар, яка відбулася 12 грудня 2023 року. Щоб зменшити масштаб знищених даних, компанія фізично вимкнула зв'язок, а це в свою чергу вплинило на роботу інших критичних інфраструктур. І це при тому, що Київстар має потужну команду кіберфахівців, власний Security Operations Center та постійно інвестує у власну кібербезпеку. Однак, як вірно зазначають фахівці, немає в світі компаній або організацій, здатних попередити усі кібератаки. Їх зазнають усі: від маленьких онлайн-магазинів до великих операторів зв'язку і навіть суб'єктів прийняття рішень з кібербезпеки [1].

Тому сьогодні все більше країн розуміють необхідність захисту не тільки своїх критично важливих інфраструктур, таких як залізничні мережі, електростанції, аеропорти, газопроводи та системи водопостачання тощо, а й критичні інформаційні інфраструктури, такі як телекомунікаційні мережі та мережі передачі даних, фінансові системи та системи управління процесами. Це означає, що сьогодні всі критично важливі інфраструктури залежать від безпеки одна одної, оскільки найслабша ланка може бути вразливою для багатьох інших. Тому для всіх питання забезпечення безпеки і стійкості критичної інформаційної інфраструктури стає дедалі важливішими.

На початку цього дослідження необхідно коротко схарактеризувати, що таке критична інформаційна інфраструктура, адже в Україні питанням її захисту приділяється увага досить недавно. А саме з прийняттям 27 січня 2016 року «Стратегії кібербезпеки України». Ця стратегія була розроблена після кібератаки вірусу Black Energy [2] на критичну інфраструктуру України. Згідно з цим документом, захист критичної інфраструктури від кіберзагроз, у тому числі, повинен полягати у визначенні критеріїв класифікації інформаційних (автоматизованих) телекомунікаційних, інформаційно-телекомунікаційних систем як критичної інформаційної інфраструктури [3].

І як в наведеному вище прикладі хакерської атаки на Київстар, державні структури України, на жаль не працюють на випередження, а починають розробляти системи захисту, вносити зміни у законодавство вже постфактум. І це є проблемою не тільки для України. Зокрема в Європейських країнах теж не завжди грають на випередження. Так, наприклад, ще у грудні 1993 року була підготовлена доповідь Бангеманна: Європа та глобальне інформаційне суспільство [4], а тільки у 2001 році була прийнята Конвенція про кіберзлочинність (Convention on Cybercrime) [5].

Необхідно відмітити, що питання стійкості та захисту критичної інфраструктури взагалі та інформаційної – зокрема не є проблемою виключно держави. Що стосується потреб бізнес-спільноти, «тривале нехтування критичною інфраструктурою та її потребами в розвитку» посідає четверте місце серед головних проблем для ринків і економік, що розвиваються, для стимулювання бізнесу, економічної інтеграції та ефективності торгівлі [6]. Перші три проблеми пов'язані з фінансовою кризою та кризою ліквідності. На жаль, згідно з висновками Міжнародного економічного форуму (WEF), за останні 10 років було досягнуто незначного прогресу в усуненні ризику збоїв у роботі критичної інфраструктури.

Зазначимо, що у міжнародних практиках критична інформаційна інфраструктура визначається як: «сукупність всіх взаємопов'язаних інформаційних та комунікаційних інфраструктур, які необхідні для підтримання життєво важливих суспільних функцій (здоров'я, безпека, безпека, економічний або соціальний добробут людей), порушення або знищення яких призвело б до серйозних наслідків» [7]. У вітчизняному законодавстві надається інше визначення критичної інформаційної інфраструктури, а саме, що це: «сукупність об'єктів критичної інформаційної інфраструктури» [8]. Водночас, під «об'єктом критичної інформаційної інфраструктури» розуміють: «комунікаційну або технологічну систему об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури» [8].

Тобто в першому визначенні акцент надається саме на тому, що критична інформаційна інфра-

структура, це не проста сукупність об'єктів, а це сукупність, яка необхідна для підтримання життєво важливих суспільних функцій. Крім того, зазначена сукупність не тільки стосується власне діяльності критичного об'єкта, а є взаємопов'язаною із іншими об'єктами. У цьому варіанті можна зрозуміти, чому такий об'єкт є критично важливим. У другому варіанті, незрозуміло чому атака на такий об'єкт буде критичною і навіщо його потрібно посилено захищати. Втім загально прийнято, що інфраструктури, які є національно значимими, є критичними.

Для того щоб певний об'єкт чи елемент об'єкту був віднесений до критичної інформаційної інфраструктури необхідно щоб він відповідав наступним встановленим критеріям:

– об'єкт інформаційної інфраструктури є необхідним як для стійкого та безперервного функціонування об'єкта критичної інфраструктури, так і для надання ним основних послуг;

– кібератака, кіберінцидент, інцидент з інформаційної безпеки на об'єкті інформаційної інфраструктури істотно вплине на безперервність та стійкість надання об'єктом критичної інфраструктури основних послуг;

– у разі порушення безперервності та стійкості надання основних послуг об'єктом інформаційної інфраструктури відсутній альтернативний об'єкт (спосіб) для їх надання [9].

Тобто, коли об'єкт буде відповідати усім цим трьом ознакам, тоді його віднесуть до переліку критичної інформаційної інфраструктури, а потім – у Реєстр об'єктів критичної інфраструктури. До речі, сьогодні в Україні зазначений реєстр тільки створений, але ще не наповнений. Подати інформацію про необхідність внесення у Реєстр той чи інший об'єкт можуть і представники бізнесу, що є досить суттєвою інновацією для захисту критичних інформаційних структур, які є у володінні приватних структур. Адже сьогодні відбувається певна диспропорція щодо права власності на об'єкти критичної інформаційної інфраструктури, які в своєї більшості перебувають у приватній власності.

Більшість країн будували свою систему захисту об'єктів критичної інфраструктури протягом п'яти-семи років в умовах мирного часу. Україні ж доводиться робити це у більш стислі терміни та у значно складніших умовах, коли російські війська прицільно знищують саме критичну інфраструктуру: енергетичні об'єкти, логістику, зв'язок тощо. Тож синергія усіх учасників процесу в розбудові надійної системи захисту критичної інфраструктури є надзвичайно важливою [10]. Відповідно до затвердженого «Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» [11] для об'єктів критичної інфраструктури передбачені періодичні перевірки раз на три роки із залученням секторальних та функціональних органів щодо дотримання правил захисту. Перші такі перевірки відбудуться не раніше 2026 року. Важливо: відповідальність за безпеку об'єкта лежить саме на його операторі, держава може бути партнером у її забезпеченні, але не може втручатися у роботу бізнесу [11].

Зазначені вище критирії критичності об'єкта є важливими, але вони містять якісні характеристики і не містять чітких кількісних показників. Наприклад, в Нідерландах з квітня 2015 року [12] встановлено критерії для поділення об'єктів критичної інфраструктури на дві категорії відповідно кількісних характеристик.

Категорія А: принаймні вплив на одну з наступних чотирьох секторів: 1) економічний вплив: > 50 000 мільйонів євро витрат і збитків, або 5,0% зниження реального доходу; 2) фізичний вплив: > 10 000 смертей, тяжко поранених або хронічно хворих; 3) соціально-психологічний вплив: > 1 мільйон людей емоційно вражені або відчувають серйозні соціальні проблеми виживання (страх, гнів, хвилювання); 4) каскадний вплив: це порушення спричиняє збій мінімум двох інших (критичних) секторів. Категорія В: принаймні вплив на одну з наступних трьох секторів: 1) економічний вплив: > 5 000 мільйонів євро витрат і збитків, або 1,0% зниження реального доходу; 2) фізичний вплив: > 1000 смертей, тяжко поранених або хронічно хворих; 3) соціально-психологічний вплив: > 100 000 осіб емоційно вражені або відчувають серйозні соціальні проблеми з виживанням [12].

Отже, включення кількісних параметрів до критеріїв критичності дозволяє більш точно оцінювати та класифікувати об'єкти критичної інфраструктури, тим самим забезпечуючи більш зрозумілі стандарти визначення їх важливості.

У статті 19 Загальної декларації прав людини зазначено, що: «кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів» [13]. Отже, спілкування є фундаментальним соціальним процесом, основною людською потребою та основою будь-якої соціальної організації і це є центральним місцем в інформаційному суспільстві. Адже, кожен і всюди повинен мати можливість брати участь у спілкуванні і ніхто не повинен бути виключений із переваг, які пропонує інформаційне суспільство. Але сучасний світ показав свою залежність від рівня безпеки та стійкості критичної інформаційної інфраструктури. І ця залежність найбільше себе проявила з початком пандемії COVID-19 та посилилась із повномасштабною війною в Україні.

Висновки. Для вирішення виявлених у цьому дослідженні проблем усі зацікавлені сторони повинні працювати разом, щоб: покращити доступ до інформаційної та комунікаційної інфраструктури та технологій, а також до інформації та знань; нарощувати потенціал; підвищити стійкість та безпеку у використанні інформаційно-комунікаційних технологій; створити сприятливе середовище на всіх рівнях; розвивати та розширювати програми інформаційно-комунікаційних технологій та заохочувати міжнародну та регіональну співпрацю. Це ключові принципи побудови інклюзивного інформаційного суспільства.

Література

1. Експерт детально прокоментував випадок з Київстаром. UAZMI – Агрегатор українських ЗМІ, 2023. URL: https://uazmi.org/news/post/d4a2c3c771567efb6f7ee1995a0afb8d
2. Cherepanov A. BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. WeLiveSecurity.com., 2016. URL: https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96/2016. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
4. Bangemann report: Europe and the global information society. CORDIS services EC, 2022. URL: https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the-global-information-society
5. Convention on Cybercrime. Budapest, 23.XI.2001. European Treaty Series – No. 185. Council of Europe. URL: https://rm.coe.int/1680081561
6. WEF (World Economic Forum). 2015. "Global Risks 2015, 10th Edition." Geneva: World Economic Forum. URL: https://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf
7. GFCE Global Good Practices. Critical Information Infrastructure Protection (CIIP). Global Conference Cyberspace, 2017. URL: https://thegfce.org/wp-content/uploads/CriticalInformationInfrastructureProtectionCIIP-1.pdf
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
9. Деякі питання об'єктів критичної інформаційної інфраструктури: постанова Кабінету Міністрів України від 09.10.2020 р. № 943. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text
10. Бізнес може долучитися до наповнення Реєстру об'єктів критичної інфраструктури. Європейська Бізнес Асоціація, 2023. URL: https://eba.com.ua/biznes-mozhe-doluchytysya-do-napovnennya-reyestru-ob-yektiv-krytychnoyi-infrastruktury/
11. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 22.07.2022 р. № 821. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#n8
12. Tweede Kamer der Staten-Generaal. Nationale Veiligheid. Den Haag, 12 mei 2015. URL: https://archief.rijksbegroting.nl/binaries/pdfs/2/0/8/kst208663.pdf
13. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III). Генеральної Асамблеї ООН від 10 грудня 1948 року. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text

Анотація

Сокіран М. В. **Актуальні питання захисту критичної інформаційної інфраструктури.** – Стаття.

У статті досліджено взаємозалежність суспільства від стійкості та безпеки критичних інформаційних інфраструктур. Констатовано, що сучасне суспільство не може розвиватися та працювати без критично важливих інфраструктур, більшість з яких стали залежними від підключення до Інтернету для різноманітних функцій управління інформацією, зв'язку та контролю. У багатьох випадках інформаційні та комунікаційні технології стали всеохоплюючими, з'єднуючи інші інфраструктури, які називають критичною інформаційною інфраструктурою. Визначено, що сучасний світ показав свою залежність від рівня безпеки та стійкості критичної інформаційної інфраструктури. І ця залежність найбільше себе проявила з початком пандемії COVID-19 та посилилась із повномасштабною війною в Україні. На підставі аналізу хакерської атаки на національного оператора України «Київстар», зроблено висновок про посилення взаємозалежності суспільства від критичної інформаційної інфраструктури, яка сьогодні є особливо вразливою до стихійних лих, технічних проблем, кібератак і тероризму. Доведено, що тема захисту критичної інформаційної інфраструктури є предметом посиленої уваги і поступово вважається невід'ємною частиною національних стратегій сталого розвитку, а також те, що питання стійкості та захисту критичної інфраструктури взагалі та інформаційної – зокрема не є проблемою виключно держави. Приватний бізнес не менш зацікавлений в стійкості та безпеці критичної інформаційної інфраструктури. З'ясовано, що адаптація досвіду Нідерландів щодо додавання кількісних параметрів до критеріїв критичності дозволить більш точно оцінювати та класифікувати об'єкти критичної інфраструктури, тим самим забезпечуючи більш зрозумілі стандарти визначення їх важливості.

Ключові слова: критична інформаційна інфраструктура, об'єкт, хакери, кібербезпека, інформаційна безпека, захист, безпека, стійкість, Київстар.

Summary

Sokiran M. V. **Actual issues of protection of critical information infrastructure.** – Article.

The article examines the interdependence of society on the stability and security of critical information infrastructures. It has been established that modern society cannot develop and function without critical infrastructures, most of which have become dependent on Internet connectivity for a variety of information management, communication, and control functions. In many cases, information and communication technologies have become pervasive, connecting other infrastructures called critical information infrastructure. It was determined that the modern world has shown its dependence on the level of security

and stability of critical information infrastructure. This dependence manifested itself most with the beginning of the COVID-19 pandemic and intensified with the full-scale war in Ukraine.

Based on the analysis of the hacker attack on the national operator of Ukraine – Kyivstar, a conclusion was made about the strengthening of the interdependence of society on critical information infrastructure, which today is especially vulnerable to natural disasters, technical problems, cyber attacks, and terrorism. It has been proven that the topic of critical information infrastructure protection is attracting more and more attention and is gradually being considered an integral part of national sustainable development strategies. Also, the fact that the issue of stability and protection of critical infrastructure in general, and information in particular, is not a problem of the state alone. Private business is no less interested in the stability and security of critical information infrastructure. The given example of the Netherlands regarding the addition of quantitative parameters to the criticality criteria allows for a more accurate assessment and classification of critical infrastructure objects, thereby providing clearer standards for determining their importance.

Key words: critical information infrastructure, object, hackers, cybersecurity, information security, protection, security, sustainability, Kyivstar.