УДК 351.862.4:340.13+338.583
DOI https://doi.org/10.32782/2408-9257-2024-1-63

Сокіран М. В.,
кандидат юридичних наук, докторант
Науково-дослідного інституту публічного права

МІЖНАРОДНІ СТАНДАРТИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

INTERNATIONAL STANDARDS IN THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

У статті проаналізовано міжнародні та європейські документи, що встановлюють стандарти щодо захисту та стійкості критичної інфраструктури загалом та інформаційної – зокрема. Визначено, що кібербезпека – це важлива складова всієї системи забезпечення безпеки країни і є стабілізуючим елементом стійкості суспільства. Тому країни світу почали розробляти правові стандарти та політики у сфері забезпечення безпеки критичної інформаційної інфраструктури. З'ясовано, що термін «інформаційна безпека» є частиною загального поняття безпека і формує тип безпеки, для якого, як і для самої безпеки, існує багато визначень. Однак існує відносний консенсус у безпековій спільноті щодо основних характеристик терміну інформаційна безпека. Зазначено, що термін «інформаційна безпека» є ширшим, тоді як термін «кібербезпека» означає захист інформації в «кіберпросторі», який широко розуміється як Інтернет, однак для цілей цієї статті ці два терміни розглянуто як еквівалентні.

Досліджено Міжнародний стандарт з інформаційної безпеки (ISO 27001) та зроблено висновок про необхідність інтеграції управлінських і технічних компетенцій у системи управління інформаційною безпекою. Підкреслено, що ефективне управління нею має враховувати та включати технічні, кадрові та організаційні аспекти. Аналіз юридичної літератури дозволив підтвердити висновок про необхідність інтеграційного підходу до забезпечення захисту критичної інформаційної інфраструктури. Оскільки контрзаходи безпеки часто приймають форму складних процедур, а в деяких випадках відсутність знань про прийнятті правила безпеки та відповідну поведінку не є основною причиною недотримання процедур безпеки. Скоріше це результат недостатньої організаційної культури безпеки, яка може наражати організацію на небезпеку в наслідок потенційної вразливості людини.

Ключові слова: *критична інформаційна інфраструктура, міжнародні стандарти, безпека, захист, інформаційна безпека, кібербезпека, система управління безпекою.*

The article analyzes international and European documents that set standards for the protection and stability of critical infrastructure in general and information infrastructure in particular. It was determined that cyber security is an important component of the entire system of ensuring the security of the country and is a stabilizing element of the stability of the world society, the countries of the world began to develop legal standards and policies in the field of ensuring the security of critical information infrastructure. It was found that the term "information security" is part of the general concept of security and forms a type of security for which, like security itself, there are many definitions. However, there is a relative consensus in the security community regarding the basic characteristics of the term information security. It is noted that the term "information security" is broader, while the term "cybersecurity" refers to the protection of information in "cyberspace", which is broadly understood as the Internet, but for the purposes of this article, the two terms are considered equivalent.

The International Standard for Information Security (ISO 27001) was studied, and a conclusion was drawn about the need to integrate managerial and technical competencies into information security management systems, and it was emphasized that its effective management should take into account and include technical, personnel and organizational aspects. The analysis of legal literature allowed to confirm the conclusion about the need for an integration approach to ensure the protection of critical information infrastructure. Since security countermeasures often take the form of complex procedures, and in some cases, lack of knowledge about the adoption of security rules and appropriate behavior is not the main reason for non-compliance with security procedures. Rather, it is the result of an insufficient organizational security culture, which can expose the organization to danger as a result of potential human vulnerability.

Key words: *critical information infrastructure, international standards, security, protection, information security, cybersecurity, security management system.*

Постановка проблеми. Під час «холодної» війни глобальний баланс у ядерній гонці підтримувався за допомогою «гарантій взаємного знищення». У сучасний період цю ж саму роль почала відігравати кіберзброя. Адже її відносно низька вартість істотно розширила список країн, які мають доступ до сучасних засобів для кібератак і це може в будь-який момент призвести до глобальної дестабілізації. Тому розуміючи, що кібербезпека – це важлива складова всієї системи забезпечення безпеки країни і є стабілізуючим елементом стійкості світового суспільства, країни світу почали розробляти правові стандарти та політики у сфері забезпечення безпеки критичної інформаційної інфраструктури.

Аналіз останніх досліджень і публікацій у сфері забезпечення безпеки і стійкості критичної інформаційної інфраструктури показав недостатню увагу з боку науковців до цієї сфери. В більшості випадків фахівці аналізували міжнародні стандарти забезпечення захисту щодо критичної інфраструктури, залишаючи поза уваги її інформаційну складову. Як приклад, можна навести наступні роботи: В. В. Крикун «Адміністративно-правовий механізм захисту об'єктів критичної інфраструктури» (2021 р.), С. А. Теленик «Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України (2021 р.), І. І. Осипчук «Адміністративно-правові засади діяльності Служби безпеки України як суб'єкта забезпечення критичної інфраструктури» (2021 р.), В. В. Косинський «Адміністративно-правове забезпечення безпеки критичної інфраструктури в Україні (2021 р.).

Мета статті – на основі аналізу міжнародних стандартів, а також результатів загальнотеоретичних та галузевих досліджень виокремити необхідні підходи щодо удосконалення забезпечення безпеки і стійкості критичної інформаційної інфраструктури України.

Виклад основного матеріалу. Побудову інформаційного суспільства як глобальне завдання у новому тисячолітті, проголосила Декларація принципів 12 грудня 2003 року, яка була прийнята на Всесвітній зустрічі на найвищому рівні в Женеві [1]. У Декларації наголошено, що, будуючи інформаційне суспільство, необхідно забезпечити, взаємодію між зацікавленими сторонами на принципах довіри, а також необхідний рівень безпеки при використанні інформаційних технологій – все означене і є ключовим при побудові відкритого інформаційного суспільства.

У жовтні 2004 року Генеральна Асамблея Організації Об'єднаних Націй прийняла резолюцію про створення глобальної культури кібербезпеки та захисту критичних інформаційних інфраструктур, яка рекомендувала 11 елементів для захисту. Одними із яких є: створення мереж для термінового попередження про фактори вразливості, погроз та інцидентів в кібернетичному просторі; підтримка державно-приватного партнерства з обміну та аналізу щодо критичної інформаційної інфраструктури; прийняття адекватних матеріальних та процесуальних законів, які дозволять державам розслідувати та переслідувати напади на критичну інформаційну інфраструктуру та координувати такі розслідування з іншими державами, коли це необхідно [2].

Усвідомлення зростання терористичних загроз в Європі призвело до того, що Європейська Комісія у листопаді 2005 р. випустила Зелену книгу щодо Європейської програми захисту критичної інфраструктури [3], а згодом, у 2006 р., коли завершився етап консультацій між членами ЄС, була запущена в дію Європейська програма захисту критичної інфраструктури [4]. Особливості підходу ЄС, як об'єднання суверенних держав, у подальшому знайшли своє відображення у документі Європейської Комісії «Захист критичної енергетичної та транспортної інфраструктури Європи» (лютий 2007 р.) [5], а також у спеціальній директиві щодо визначення об'єктів критичної інфраструктури та оцінку потреб у підвищенні рівня їхнього захисту (грудень 2008 р.) [6]. Захист критичної інфраструктури енергопостачання Декларацією Чиказького саміту (20 травня 2012 р.) [7] було віднесено до числа пріоритетних напрямів забезпечення енергетичної безпеки для держав-членів НАТО та самого Альянсу [8].

Пізніше, ЄС оприлюднив свою позицію стосовно захисту критичних інфраструктур на міжнародному рівні. Вона полягає в тому, що замість того, щоб створювати нові міжнародно-правові інструменти з питань кіберзлочинност-

ті, він закликає всі країни розробити відповідне національне законодавство та співпрацювати в рамках існуючої міжнародної структури. Наприклад, Кіберстратегія 2017 року також підтверджує позицію ЄС, згідно з якою міжнародне право, зокрема Статут ООН, застосовується в кіберпросторі. Як доповнення до обов'язкового міжнародного права, ЄС схвалює добровільні необов'язкові норми, правила та принципи відповідальної поведінки держав-членів ООН [9].

Вище зазначені документи зрозуміло не охоплюють увесь масив міжнародних та європейських документів, які направлені на вирішення питань належного захисту та стійкості критичної інформаційної інфраструктури. Дійсно у часи, коли даними та інформацією торгують як товарами, їх захист має важливе значення. Один із способів зробити це – запровадити управління інформаційною безпекою на основі стандартів інформаційної безпеки серії ISO/IEC 2700x. Це міжнародне сімейство стандартів IT-безпеки та інформаційної безпеки в приватних, державних або некомерційних організаціях. На основі ISO 27001 може бути запроваджена система управління інформаційною безпекою (СУІБ), яку організації та органи державної влади можуть створювати, експлуатувати та сертифікувати для власного захисту [10].

Загальне поняття безпеки є дуже широким і включає багато аспектів і багато значень, отже, є багато різних визначень терміну безпеки і існує багато типів безпеки. З іншого боку, концепція безпеки дуже близька кожній людині, внутрішня, яку ми інтуїтивно розуміємо. Вона навіть формує одну з основних людських потреб, а бажання її віднайти є одним із фундаментальних інстинктів не лише людей, а й інших організмів. Забезпечення безпеки було однією з головних рушійних сил в організації людського суспільства від початку цивілізації. В свою чергу, термін «інформаційна безпека» є частиною загального поняття безпека і формує тип безпеки, для якого, як і для самої безпеки, існує багато визначень. Однак існує відносний консенсус у безпековій спільноті щодо основних характеристик терміну інформаційна безпека.

Відповідно до Міжнародного стандарту з інформаційної безпеки (ISO 27001), який розроблений спільно Міжнародною організацією зі стандартизації та Міжнародною електротехнічною комісією, інформаційна безпека визначається як: «збереження конфіденційності, цілісності та доступності інформації» [11]. Де конфіденційність визначається як інформація яка не надається або не розкривається неавторизованим особам, організаціям або процесам; а доступність – як: властивість бути доступним і використовуватися на вимогу уповноваженої особи, а цілісність визначається як: «точність та повнота» [11].

Управління інформаційною та кібербезпекою має ключове значення в контексті розвитку сучасного інформаційного суспільства. Перед тим як розкрити зазначене управління необхідно відмітити наступне: терміни «управління інформаційною безпекою» та «управління кібербезпекою» тісно пов'язані між собою та мають однакову мету – забезпечення безпеки інформації. І хоча термін «інформаційна безпека» є ширшим (зокрема термін «кібербезпека» означає захист інформації в «кіберпросторі», який широко розуміється як Інтернет), для цілей цієї статті ми розглядатимемо ці два терміни як еквівалентні.

Стандарт ISO 27001 [11] описує систему управління інформаційною безпекою (СУІБ) наступним чином: вона складається із сукупності політик, процедур, методів, інструкцій і пов'язаних ресурсів, якими керує організація з метою захисту своїх інформаційних активів. СУІБ – це системний підхід до встановлення, впровадження, експлуатації, моніторингу, перегляду, підтримки та покращення інформаційної безпеки організації у досягненні бізнесцілей. Він базується на оцінці ризику та рівні прийнятності ризиків організації, що призначені для ефективного лікування та управління ризиками.

Загрози та ризики для інформаційної безпеки мають дуже складну природу, так як є не лише одновимірною технічними, але багатовимірними, соціально-технічними проблемами для безпеки. Тому система управління потребує врахування різних, а не лише технологічних аспектів забезпечення кібербезпеки. Ця вимога також часто обговорюється в науковій літературі. Є статті та дослідження, які показують необхідність комплексного (цілісного) під-

ходу до управління інформаційною безпекою [12; 13].

У літературі [14; 15; 16] також сформовано необхідність інтеграції управлінських і технічних компетенцій у системи управління інформаційною безпекою та підкреслено, що ефективне управління нею має враховувати та включати технічні, кадрові та організаційні аспекти.

Так, наприклад, автори дослідження «Підвищення обізнаності співробітників про інформаційну безпеку в приватних і державних організаціях: систематичний огляд літератури» [15] стверджують, що значна кількість інцидентів, що посягали на інформаційну безпеку пов'язана з людським фактором, який прямо та/або опосередковано викликає більшість інцидентів безпеки. Добре обізнані та навчені співробітники зводять до мінімуму випадкові та ненавмисні дії, що визначають порушення правил кібербезпеки, і відіграють значну роль у мінімізації ризиків інформаційної безпеки та захисті критично важливих активів організації та цінної інтелектуальної власності. Таким чином, обізнаність працівників щодо сфери інформаційної безпеки стає одним із критичних аспектів захисту від небажаної поведінки у цій сфері.

Останній серйозний інцидент у сфері кібербезпеки, а саме хакерська атака на найбільшого мобільного оператора України – Київстар, також показав вразливість систем захисту. Однією із версій є те, що така атака могла відбутися з середини Київстар [17].

Інші автори, підкреслюють, що незалежно від того, наскільки технологія буде незалежною від людини, зрештою люди будуть взаємодіяти з нею в різні моменти часу (наприклад, працівники можуть бути в курсі під час встановлення, налаштування та обслуговування технології). Дійсно, визнається, що проблема кібербезпеки залежить від високої складності, взаємозв'язку та нових якостей соціально-технічних систем і що люди можуть бути «частиною рішення», а не «частиною проблеми». Таким чином, автори стверджують, що люди залишаються життєво важливим і невід'ємним елементом кіберзахисту організацій, оскільки вони є критичними чинниками успіху чи невдачі управління критичною інформаційною інфраструктурою в організаціях [16].

Дійсно, контрзаходи безпеки часто приймають форму складних процедур, а в деяких випадках відсутність знань про прийнятті правила безпеки та відповідну поведінку не є основною причиною недотримання процедур безпеки. Скоріше це результат недостатньої організаційної культури безпеки, яка може наражати організацію на небезпеку в наслідок потенційної вразливості людини.

Висновки і пропозиції. Проведений аналіз юридичної літератури, а також міжнародних та європейських документів дозволив підтвердити висновок про необхідність інтеграційного підходу до забезпечення захисту критичної інформаційної інфраструктури. Інтеграційний підхід побудований на сукупності управлінських і технічних компетенцій у системи управління інформаційною безпекою. В свою чергу ефективне управління нею має враховувати та включати технічні, кадрові та організаційні аспекти. Все означене потребує нових підходів у забезпеченні безпеки і стійкості критичної інформаційної інфраструктури України.

ЛІТЕРАТУРА:

1. Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Document WSIS-03/GENEVA/DOC/4-E. 12 December 2003. URL: https://www.itu.int/net/wsis/docs/geneva/official/dop.html

2. Creation of a global culture of cybersecurity and the protection of critical information infrastructures : resolution / adopted by the General Assembly. UN. General Assembly (58th sess. : 2003-2004). URL: https://digitallibrary.un.org/record/509571?ln=en

3. Green Paper on a European Programme for Critical Infrastructure Protection. European Union, 2005. URL: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

4. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, URL: http://eurlex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

5. A Communication on Protecting Europe's Critical Energy and Transport Infrastructure (цей документ містить чутливу інформацію, і тому не підлягає публікації).

6. Council Directive 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

7. Chicago Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. URL: https://www.nato.int/cps/uk/natohq/official_texts_87593.htm?selectedLocale=en

8. Зелена книга з питань захисту критичної інфраструктури в Україні (друга версія проекту документа) Національний інститут стратегічних досліджень, 2014. URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf С.3

9. Heinl, Caitríona. An overview of the European Union's current strategies, policies and concepts on Cyber security and stability in cyberspace – may 07, 2019. URL: https://incyber.org/en/an-overview-of-the-european-unions-current-strategies-policies-and-concepts-on-cyber/

10. Крюгер Г. Стандарти інформаційної безпеки – огляд. DQS Holding GmbH, 2023. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/standarti-informacijnoyi-bezpeki-oglyad

11. ISO/IEC 27000. Information technology – Security techniques – Information security management systems – Overview and vocabulary, Geneva: ISO (the International Organization for Standardization), 2018.

12. Soomoro, Z; Shah, M. and Ahmed, J. (2016) Information security management needs more holistic approach: A literature review. *International Journal of Information Management*. No 36 (2), 215–225. URL: https://pure.coventry.ac.uk/ws/portalfiles/portal/11711640/litreviewcomb.pdf

13. Červený, Vlastimil, Martin Hromada, Roman Jašek. Cybersecurity Management System of the Czech Republic. Research Article, 2023. https://doi.org/10.21203/rs.3.rs-3274570/v1

14. Kosutic, Dejan. The Impact of Cybersecurity on Competitive Advantage. Researchgate, 2021. URL: https://www.researchgate.net/publication/357826918_The_Impact_of_Cybersecurity_on_Competitive_Advantage

15. Khando, Khando, Shang Gao, Sirajul M. Islam, Ali Salman. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security, 2021. Volume 106. URL: https://www.sciencedirect.com/science/article/pii/S0167404821000912

16. Pollini, Alessandro, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi & Davide Guerri. Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 2022. Volume 24, pages 371–390. URL: https://link.springer.com/article/10.1007/s10111-021-00683-y

17. Капнік О. У «Київстарі» не виключають, що масштабна атака була зсередини мережі. ТСН, 2023. URL: https://tsn.ua/ukrayina/u-kiyivstari-ne-viklyuchayut-scho-masshtabna-ataka-bula-zseredini-merezhi-2470534.html