**Міністерство освіти і науки України**

**Національний університет**
**«Полтавська політехніка імені Юрія Кондратюка»**

**Навчально-науковий інститут фінансів, економіки,**
**управління та права**
**Кафедра фінансів, банківського бізнесу та оподаткування**


# ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

**Матеріали Міжнародної**
**науково-практичної Інтернет-конференції**

**29 вересня 2022 р.**

**Полтава**
**2022**

**Міністерство освіти і науки України**

**Національний університет**
**«Полтавська політехніка імені Юрія Кондратюка»**
**Навчально-науковий інститут фінансів, економіки, управління та права**
**Кафедра фінансів, банківського бізнесу та оподаткування**

**Білостоцький технологічний університет (Польща)**

**Університет Північ (Хорватія)**

**Університет ISMA (Латвія)**

**Міжнародний науково-освітній та навчальний центр (Естонія)**

**Київський національний університет імені Тараса Шевченка**
**Кафедра фінансів**

**Національний університет «Чернігівська політехніка»**

**ЗБІРНИК МАТЕРІАЛІВ**
**Міжнародної науково-практичної Інтернет-конференції**

# «ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО»

**29 вересня 2022 р.**

**Полтава**
**2022**

**УДК 330.336**
**Е45**



**Е45 Економічна безпека: держава, регіон, підприємство:** Матеріали Міжнародної науково-практичної Інтернет-конференції, 29 вересня 2022 р. – Полтава: Національний університет імені Ю.Кондратюка, 2022. – 215 с.

**ISBN 978-966-616-152-2**

У збірнику матеріалів Міжнародної науково-практичної Інтернет-конференції представлено результати розвитку теорії економічної безпекології, теоретичні та методологічні аспекти системотворення економічної безпеки держави, регіону та підприємства, забезпечення економічної безпеки держави, регіону, підприємства (концепції, напрями дій, способи та алгоритми), оцінювання економічної безпеки держави, регіону, підприємства.

Участь у конференції взяли представники закладів вищої освіти, наукових, фінансових установ, державних органів управління та бізнес-середовища з України, Польщі, Грузії, Естонії, Азербайджану, Хорватії.

Призначений для фахівців з економічної безпеки, науковців, викладачів, аспірантів, докторантів та студентів.

*Тези надано в авторській редакції. За виклад, зміст, достовірність та відсутність плагіату у тезах відповідають автори.*

**УДК 330.336**
**Е45**

ISBN 978-966-616-152-2

2. Оцінка інфляції. Серпень 2022 року. Національний банк України: веб-сайт. URL: https://bank.gov.ua/admin_uploads/article/CPI_2022-08.pdf?v=4.

3. Данилишин Б. Інфляційні процеси в Україні і світі та їх перспективи. URL: https://lb.ua/blog/bogdan_danylysyn/513069_inflyatsiyni_protsesi_ukraini_i_sviti.html.

**УДК 338.2**

***Маслій Олександра Анатоліївна,***
*кандидат економічних наук, доцент*
***Максименко Андрій Петрович,***
*здобувач третього (наукового) рівня вищої освіти*
*Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)*

## ЗАГРОЗИ КРИТИЧНІЙ ЦИФРОВІЙ ІНФРАСТРУКТУРІ В УМОВАХ ВІЙНИ

Технічний і технологічний розвиток останніх десятиліть, проникнення технологічних рішень на ринок, домінування ринку цифрових послуг у розвинених країнах – призвели до відповідного виникнення цифрової інфраструктури, здатної забезпечити всі потреби і переваги зумовлені таким зростанням. Але окрім економічного і наукового розвитку, прискорення фінансових операцій і стимулювання розвитку людського потенціалу – цифровізація прямо і опосередковано сприяла створенню нових методів і технологій для знищення реальної та цифрової інфраструктури [1], технологічного шпигунства, втручанню у вибори, розповсюдженню деструктивних ідей і «Fake-News».

Також унаслідок глобалізації цифрових економік у одну – не лише виросла ціна війни, а й якісно змінилася їхня

сутність: економічного, цифрового та інформаційного превалювання над суперником; виникли нові інструменти впливу на економіку та політичне середовище [2], окрім того атаки стали безпечнішими для агресора.

Найбільшим прикладом можливого застосування цифрових технологій для враження критичної інфраструктури є інцидент «Stuxnet» у 2011 році, коли група хакерів проникла у закриту і, на перший погляд, надійно захищену цифрову систему керування іранською атомною електростанцією у місті Бушер на березі Персидської затоки [3].

Катастрофа, котра могла бути викликана цілеспрямованим хакерським втручанням чи помилкою при проникненні, могла би спричинити значну техногенну загрозу для країн Перської затоки, світовому забезпеченню нафтою, а також викликати гуманітарну, інфраструктурну, цифрову, електричну, виробничу, екологічну та політичну кризу для Ірану. Групу, що стояла за атакою не було знайдено, як і не відомий рівень проникнення ворогуючих держав у інфраструктуру один одного.

Варто відзначити, що конфліктуючі країни мають значну кількість об’єктів критичної інфраструктури: гребель, електростанцій, у тому числі атомних, аеропортів тощо, а їх критичне враження рівноцінне ракетним атакам чи застосуванню ядерної зброї (табл. 1).

Таблиця 1

Кількість об’єктів критичної інфраструктури по країнам

| **Країна** | **Не атомних електростанцій** | **Атомних реакторів** | **Греблі** | **Крупні трубопроводи** | **Разом** |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| Україна | 57 | 15 | 21 | 3 | 96 |
| США | 1227 | 92 | 9265 | 160 | 10744 |
| Китай | 1273 | 54 | 4688 | 98 | 6113 |
| Росія | 249 | 37 | 91 | 61 | 438 |
| Японія | 91 | 33 | 1121 | 4 | 1249 |

Продовження табл. 1

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| Південна Корея | 23 | 24 | 1205 | 4 | 1256 |
| Індія | 346 | 23 | 4636 | 10 | 5015 |
| Пакистан | 10 | 6 | 71 | 1 | 88 |
| Тайвань | 20 | 1 | - | - | 21 |
| Іран | 92 | 1 | 135 | 1 | 229 |

*Складено авторами за джерелами [4-5]*

Одночасне враження навіть частини цих об'єктів інфраструктури буде мати руйнуючий вплив на економіку держави і майже не матиме наслідків для сил, що нанесли цю атаку, якщо вони не будуть встановлені.

Кібертероризм, у тому числі і міждержавний – ефективний сучасний інструмент ведення війн та відстоювання геополітичних інтересів. Іншими вразливими ланками є банківська та адміністративна система, котрі, під потужною DDoS-атакою, можуть перестати виконувати свої функції, чим сповільнити оборот ресурсів, товарів, деякі інституції можуть перестати виконувати свої функції і тим паралізувати всю фінансову чи державну систему [6, 7].

Росія, починаючи з 2007 року, активно вкладалася в ці засоби враження, починаючи із кібератаки на Естонію, у 2008 році ці атаки передували масштабному вторгненню в Грузію, і мали періодичний характер з 2014 року проти України.

Прикладом реальної цілеспрямованої атаки на інфраструктуру є цільове влучення по по трубопроводу «Баку-Тбілісі-Джейхан», стратегічному об'єкту для економіки Грузії та конкуруючому для Росії, оскільки через нього планувалося постачати нафту у Європу в обхід. Відповідальність за цю атаку взяла на себе Робітнича Партія Курдистану, проте існують непрямі докази, що це була перша у світі комп'ютерна атака на об'єкт критичної інфраструктури однією державою проти іншої у період війни [8].

Іншим прикладом є атака на «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго» з дистанційним відключенням підсистем, викраденням та видаленням даних, блокуванням дистанційного доступу. Хакери змогли проникнути до систем керування через внутрішню мережу, після чого мали можливість створювати інструменти для подальших атак. На заваді повного знищення підстанцій були політичні причини та можливість ручного режиму керування підстанціями [9].

Отже, враховуючи те, що немає реального покарання і навіть доступу до злочинців, яких патронують держави у своїх інтересах та яких прямо працюють на неї. А також постійне зростання критичного будівництва: електростанцій, аеропортів, дамб, гребель, що сприяє економічному зростанню, поліпшує якість життя і виробничі потужності, проте створює мережу із вразливих ланок, доступ до яких, при певному рівні проникнення, можуть мати як злочинні терористичні харкерські групи, так і розвідувальні агентства чи спецслужби різних держав. Тому потрібно поруч із створенням цифрової інфраструктури забезпечувати її захист, зокрема створювати альтернативні шляхи доступу до керування, якщо цифрові – будуть втрачені. Україні під час повномасштабного вторгнення і подій, що їм передували допомагали західні розвідки і кібервійська союзників, а проте відтепер кожна держава має забезпечувати захист не тільки реальних, а й цифрових активів і систем.

**Література**

1. Онищенко С.В., Глушко А.Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. *Соціальна економіка*. Х.: ХНУ, 2020. Вип. 59. С. 14-24.

2. Onyshchenko S., Hlushko A., Maslii O. Threats to information security of Ukraine in the conditions of digitalization.

The world of science and innovation : Proceedings of the 12th International scientific and practical conference (July 1-3, 2021). London : Cognum Publishing House, 2021. P. 69-73. URL : https://sci-conf.com.ua/xii-mezhdunarodnaya-nauchno-prakticheskaya-konferentsiya-the-world-of-science-and-innovation-1-3-iyulya-2021-goda-london-velikobritaniya-arhiv/

3. The Hackers Behind Stuxnet. URL: https://cutt.ly/wVzNXmX

4. Plans for new reactors worldwide. World-nuclear. URL : https://world-nuclear.org/information-library/current-and-future-generation/ plans-for-new-reactors-worldwide.aspx#:~:text.

5. Міжнародна комісія з великих гребель. Cawater-Info. URL: http://www.cawater-info.net/int_org/icold/classif1.htm.

6. Онищенко С.В., Глушко А.Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. № 1 (84) С. 13-20.

7. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. (2022). Increasing Information Protection in the Information Security Management System of the Enterprise. In: Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (eds) Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. Lecture Notes in Civil Engineering, vol 181. Springer, Cham. https://doi.org/10.1007/978-3-030-85043-2_67

8. Robertson J., Riley M. Mysterious ’08 turkey pipeline blast opened new cyberwar era. Bloomberg. 2010. 14 December. URL: https://web.archive.org/web/20141225013619/http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html.

9. Зеттер К. Хакерська атака Росії на українську енергосистему: як це було. ТЕКСТИ.org.ua. URL: https://texty.org.ua/articles/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak-66125/.