УДК 004.056:330.341.1

https://doi.org/10.32689/2617-2224-2021-2(27)-3

Панченко Олег Анатолійович,
доктор наук з державного управління, доктор медичних наук, професор, заслужений лікар України, директор, ДЗ «Науково-практичний медичний реабілітаційно-діагностичний центр Міністерства охорони здоров'я України», президент, Громадське об'єднання «Всеукраїнська професійна психіатрична ліга», 85110, м. Костянтинівка, Донецька область, вул. О. Невського, 14, e-mail: oap@ukr.net, https://orcid.org/0000-0001-9673-6685

Panchenko Oleh Anatoliiovych,
Doctor of State Administration, Doctor of Medicine, Professor, Honored Doctor of Ukraine, Director, State Institution "Scientific-Practical Medical Rehabilitating-Diagnostic Center of the Ukrainian Ministry of Health", President, All-Ukrainian Professional Psychiatric League, 85110, Kostiantynivka, Donetsk region, O. Nevsky str., 14, e-mail: oap@ukr.net, https://orcid.org/0000-0001-9673-6685

Ігнатенко Валерій Сергійович,
кандидат економічних наук, науковий співробітник, ДЗ «Науково-практичний медичний реабілітаційно-діагностичний центр Міністерства охорони здоров'я України», 85110, м. Костянтинівка, Донецька область, вул. О. Невського, 14, e-mail: rdckonst@ukr.net, https://orcid.org/ 0000-0003-2659-9202

Hnatenko Valerii Serhiiovych,
Candidate of Economic Sciences, Chief Researcher, State Institution "Scientific and Practical Medical Rehabilitation and Diagnostic Center of the Ministry of Health of Ukraine", 85110, Kostiantynivka, Donetsk region, O. Nevsky str., 14, e-mail: rdckonst@ukr.net, https://orcid.org/0000-0003-2659-9202

ЕКОНОМІЧНА КІБЕРБЕЗПЕКА В ДЕРЖАВНІЙ СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Анотація. ***Мета роботи*** – дослідити сутність понять «цифрова економіка», «кіберпростір» та «кібербезпека» у контексті національної безпеки, виділити сучасні тренди економічних кіберзагроз та напрями удосконалення державного управління у сфері економічної кібербезпеки.

Методологія. Безпека цифрової економіки у державній політиці потребує виокремлення проблемного поля у розрізі врахування загроз національній безпеці та побудови відповідних механізмів їх протидії. Хоча державна політика у галузі кібербезпеки і має еволюційні тенденції, темпи її розвитку не відповідають сучасним вимогам. Отже, існує нагальна потреба в дослідженні напрямів покращення ситуації щодо питань кіберзахисту. У роботі визначені поняття «кіберпростір» та «кібербезпека» в економічній площині. Їх взаємозв'язок та роль у цифровізації економіки дали змогу відобразити модель системи національної безпеки у кібереконо мічному розрізі.

Високий рівень розвитку кіберпростору і організації кіберзагроз вказує на необхідність зміни парадигми стратегії кібербезпеки: вона повинна базуватися не на реагуванні за фактом, а бути побудованою за принципом прогнозування і планування захисту від майбутніх дій кіберзлочинців. Для цього потрібно постійно аналізувати сучасні тренди економічних кіберзагроз. У роботі виділені найбільш актуальні з них на даний час.

Наукова новизна. Акцентовано, що для успішного протистояння розглянутим викликам Україні потрібна нова кіберстратегія. Важливо, щоб шлях, яким рухається Україна у розбудові власної кібербезпеки, набув відповідних і невідкладних змін, а сам цей рух був доволі швидким. Виділено заходи, що мають знайти першочергове втілення у цьому напрямі.

Висновки. Результати дослідження показують важливість усвідомлення серйозних проблем щодо забезпечення кібербезпеки, що вимагають розробки і впровадження більш ефективних механізмів функціонування і забезпечення роботи кіберпростору, підвищення надійності основних механізмів і компонентів глобальної інтернет-мережі та інших пристроїв ІКТ, врахування людського фактору, комплексного і системного підходу у визначенні методичних засад та інструментів формування державної політики з забезпечення кібербезпеки.

Ключові слова: цифрова економіка, кіберпростір, кібербезпека, економічна кібербезпека, національна безпека.

ECONOMIC CYBER SECURITY IN THE STATE SYSTEM OF NATIONAL SECURITY

Abstract. ***Objective of the paper***. To investigate the essence of the "digital economy", "cyberspace" and "cybersecurity" concepts in the context of national security, highlight current trends in economic cyber threats and areas of improvement of public administration in the field of economic cybersecurity.

Methodology. The security of the "digital economy" in public policy requires the identification of the problem area in terms of taking into account threats to national security and creation of appropriate mechanisms for counteraction. Although public policy in the field of cybersecurity has evolutionary trends, the pace of development does not meet modern requirements, so there is an urgent need to explore ways to improve the cybersecurity situation. The concepts of "cyberspace" and "cybersecurity" in the economic plane, their interconnection and role in the digitalization of the economy allowed to reflect the model of the national security system in the cyber-economic context.

The high level of cyberspace development and the organization of cyber threats indicates the need to change the paradigm of cybersecurity strategy: it should be based not on responding to the facts, but rather on the principle of forecasting and planning protection against future actions of cybercriminals. This requires constant analysis of current trends in economic cyber threats. The work highlights the most relevant of them nowadays.

Academic novelty. It was emphasized that in order to meet the considered challenges, Ukraine needs a new cyber strategy. It is important that Ukraine's path in creation its own cybersecurity changes accordingly and at a rapid pace. Measures to be implemented in this direction are highlighted.

Conclusions. The study results show the importance of understanding the serious problems of cybersecurity, which require the development and implementation of more effective mechanisms for the functioning and operation of cyberspace, improving the reliability of basic mechanisms and components of the Internet and other ICT devices, taking into account the human factor, a comprehensive and systematic approach in determining the methodological principles and tools for the formation of state policy to ensure cybersecurity.

Key words: digital economy, cyberspace, cybersecurity, economic cybersecurity, national security.

1. Вступ

Основним глобальним трендом сучасного суспільного буття є все більш прогресуючий перехід у віртуальний інформаційний простір – онлайн. Цій об'єктивній революційній зміні неможливо і безглуздо чинити опір. Але можливо і вкрай необхідно враховувати нові тенденції і нові загрози.

Революція у сфері зв'язку та комунікацій стала суттєвим чинником розвитку цифрової економіки, світового економічного зростання та вагомим інструментом забезпечення сталого розвитку. З одного боку, це дало можливість підприємствам та споживачам в усьому світі отримати вигоди від ефективності, швидкості та зручності цифрових операцій та обміну інформацією, а з іншого – зумовило зростання ймовірності отримання фінансових збитків, витоку даних та репутаційних збитків через кіберзлочинні дії. Це зумовлює відповідне реагування з боку традиційних суспільних інститутів (зокрема, держави). Зазвичай державна політика проявляється у двох основних аспектах – державній підтримці розвитку (концепції, стратегії, доктрини, державні програми) та державному регулюванні відносин (нормативно-правові акти). Слід зазначити, що безпекова проблема цифрової економіки у державній політиці наразі трактується ще доволі звужено, зокрема, або у контексті нормативного забезпечення захисту інформації, або в контексті протидії комп'ютерній злочинності. З огляду на це важливо в умовах розвитку новітніх інформаційних технологій виокремити проблемне поле у сфері цифрової економіки у розрізі врахування загроз національній безпеці та побудови відповідних механізмів протидії. Проблему захисту від загроз, що виникають і продовжують розвиватися, в загальному вигляді можна позначити поняттям «кібербезпека». Забезпечення кібербезпеки в умовах цифрової економіки актуалізує необхідність прийняття адекватних заходів з боку держави.

Формулювання цілей (мети) статті. Мета статті – дослідити сутність понять «цифрова економіка», «кіберпростір» та «кібербезпека» в контексті національної безпеки, виділити сучасні тренди економічних кіберзагроз та напрями удосконалення державного управління у сфері економічної кібербезпеки.

2. Державна політика у галузі кібербезпеки

Сучасний розвиток суспільства характеризується інтеграцією безпекових аспектів інформаційних та економічних процесів, що переводить державне управління у сфері економіки на більш високий рівень за вимогами до ефективності. Вказана інтеграція є наслідком процесів, що об'єднані в поняття «цифровізація». Розвиток цифрової економіки в останні два десятиліття є стратегічною задачею провідних держав світу. Концепції, що розроблялись ними у цьому напрямі, містили перелік заходів державного управління, підтримки окремих видів економіки, подолання технологічних, організаційних, правових, культурних бар'єрів тощо.

За даними, наведеними у доповіді про цифрову економіку (Доклад о цифровой экономике, 2019), розмір цифрової економіки у 2019 році становив від 4,5 до 15,5% світового ВВП. Майже 40% доданої вартості, що створюється в світовому секторі інформаційно-комунікаційних технологій, припадає на США та Китай. Найбільша доля цифрової економіки в ВВП, за даними джерела (Коноплева, Корыстов, Тесленко, 2019, с. 49–55), є в Китаї (30%) та Великобританії (15%).

Що стосується України, то розпорядженням Кабінету Міністрів України від 17.01.18 р. № 67-р схвалено Концепцію розвитку цифрової економіки та суспільства на 2018–2020 роки. Зазначений документ (чинний на даний момент) передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрової інфраструктури, набуття громадянами цифрових компетенцій, а також визначає критичні сфери та проєкти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій (Концепція розвитку цифрової економіки та суспільства на 2018–2020 роки, 2018).

Генеральний секретар ООН Антоніу Гутерриш зазначає: «У дуже короткий термін прогрес у цифрових технологіях привів до створення колосального багатства, зосередженого, однак, у невеликої групи осіб, компаній і країн. Без відповідних зусиль не вдасться подолати цифровий розрив, за якого більше половини населення світу має лише обмежений доступ до інтернету або не має його зовсім...» (Доклад о цифровой экономике, 2019). Отже, Концепція є актуальною в плані подолання відставання від провідних країн світу.

Водночас Антоніу Гутерриш наголосив, що цифрова економіка створює також нові ризики, включаючи загрози кібербезпеки, полегшення незаконної економічної діяльності і зазіхання на недоторканність приватного життя. Пошук нових рішень вимагає спільних зусиль урядів, громадянського суспільства, академічних кіл, наукової спільноти та технологічного сектора. Зі сказаним

перегукується і Принцип 7 Концепції: «Інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками».

В оновленій «Стратегії національної безпеки України», затвердженій Президентом України 14 вересня 2020 року, серед пріоритетів національної безпеки вказується посилення спроможності національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі. У п. 52 Стратегії вказується: «Основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема й в умовах цифрової трансформації» (Указ Президента України № 392/2020, 2020). Нині розробляється «Стратегія кібербезпеки України», що передбачена статтею 31 Закону України «Про національну безпеку України» (Закон України «Про національну безпеку», 2018). Стратегія визначатиме пріоритети національних інтересів України у сфері кібербезпеки, а також основні підходи та напрями формування кіберзахисту.

Отже, державна політика у галузі кібербезпеки має еволюційні тенденції.

І це закономірно, адже проблема вже не може бути повноцінно вирішеною традиційними засобами інформаційної безпеки. Новітні загрози потребують системного підходу до створення комплексної системи, здатної протидіяти цим загрозам. Слід зазначити, що основою для прогресу в цьому напрямі став Закон України «Про основні засади забезпечення кібербезпеки України» (Закон України «Про основні засади забезпечення кібербезпеки України», 2017), в якому вперше вводиться значна кількість понять та засад, що є новими для правового поля України. Прискорення прийняття Закону (поданий до розгляду в 2015 році, прийнятий в жовтні 2017, введений в дію в травні 2018) спонукала, на думку експертів, атака вірусу Petya влітку 2017 року, яка принесла збиток до 10 млрд доларів.

3. Система національної безпеки у кіберекономічному розрізі

Розглянемо два головних поняття із Закону, важливих для нашого дослідження – «кіберпростір» і «кібербезпека».

За визначенням Закону, *кіберпростір* – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Загалом таке визначення в якійсь мірі трактує окремі аспекти поняття, але схиляє до неточного його розуміння, адже можна зробити висновок, що ідеться більше про технологічну складову інформаційного середовища, тобто про комп'ютерні та телекомунікаційні інфраструктури, але випущене з розгляду питання про діяльність на основі цієї інфраструктури. Більш релевантним, на наш погляд, слід вважати визначення, наведене в міжнародному стандарті ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity: «Кіберпростір – це комплексне віртуальне середовище, яке не має фізичного втілення, сформоване в результаті дій людей, програм і сервісів в мережі Інтернет за допомогою відповідних мережевих і комунікаційних технологій» (Марков, Цирлов, 2014, с. 28–35). Однак і це визначення не є досконалим, адже воно обмежує середовище тільки мережею Інтернет. Існують і інші глобальні мережі передачі даних, і це підкреслено у першому визначенні. Об'єднуючи обидва визначення, можна стверджувати, що при чіткій вказівці на зв'язаність кіберпростору з ІКТ-інфраструктурою, увага повинна бути звернена не тільки на технології, а й на діяльність людей, які використовують ці технології. Важливо, що основний зміст кіберпростору полягає в діяльності користувачів цифровими інформаційними ресурсами і ІКТ-інфраструктурою. Спираючись на дослідження (Безкоровайный, Татузов, 2014, с. 22–27) та беручи до уваги наведені визначення, кіберпростір можна розглядати як тріаду з таких складових частин:

1) інформації як в статичному (файли, записані на носії даних), так і в динамічному представленні (потоки, команди, запити тощо, що передаються мережами, обробляються в автоматизованих системах і подаються на засоби відображення в графічному або текстовому вигляді);

2) технічної інфраструктури, ІКТ, комп'ютерів, гаджетів, програмного забезпечення, за допомогою яких здійснюється реалізація основних дій з інформацією – збір, обробка, зберігання і передача;

3) інформаційної взаємодії суб'єктів (всі види діяльності користувачів або учасників кіберпростору) з використанням інформації одержуваної (передаваної) і оброблюваної за допомогою технічної інфраструктури.

Усі ці складники в сукупності утворюють сутність, яку можна назвати кіберпростором. Зупи-

нимося на його властивостях, які зумовлюють необхідність заходів кібербезпеки.

По-перше, кіберпростір – це система, що складається з великої кількості об'єктів. Істотне зменшення числа функціонуючих пристроїв в кіберпросторі або порушення їх нормальної роботи є певною загрозою кіберпростору, але не основною. Важливішою загрозою є порушення здатності системи оперувати інформацією (забезпечувати сервіси) із заданою якістю, тобто здійснювати дії, які пов'язуються з інформаційними технологіями.

По-друге, важливим є забезпечення активного оперування інформацією і збереження цією інформацією головних її властивостей – цілісності, доступності, конфіденційності тощо. На відміну від інформаційної безпеки, ідеться не про інформацію взагалі, а про ту інформацію, яка циркулює в кіберпросторі і становить важливу його частину. Порушення роботи окремого комп'ютера, підключеного до кіберпростору, або втрата інформації, яка в ньому міститься, чи порушення її властивостей, безумовно, є важливим для користувача даного комп'ютера, але навряд чи може розглядатися як загроза кібербезпеці.

По-третє, добропорядність – це здатність кіберпростору передавати, одержувати і обробляти інформацію з повним збереженням її важливих для цілей застосування властивостей.

По-четверте, важливим є «розумне управління». Важливо враховувати управління технічною основою кіберпростору, але визначальну роль відіграє управління учасниками кіберпростору – користувачами і їх групами. Під управлінням розуміється комплекс зусиль, спрямованих на стимулювання сприятливих для розвитку кіберпростору дій і придушення або пряму заборону зловмисних дій. Управління суб'єктами кіберпростору відіграє визначальну роль у виникненні, існуванні і підтримці основних властивостей цього утворення.

Багаточисленність елементів кіберпростору та взаємозв'язків між ними, можливість застосування спеціальних технік управління діями цих елементів інтенсифікують розвиток різноманітних загроз. Однак ці ж самі особливості кіберпростору можуть стати важливим фактором у підвищенні ефективності систем, які забезпечують захист від загроз. Для цього необхідно координувати зусилля всіх зацікавлених учасників, створювати механізми, що сприяють найкращому розподілу їхніх зусиль. Потрібно правильно прогнозувати небезпеки і обґрунтовано вибирати раціональні заходи захисту. Саме кібербезпека має на меті вирішення цих питань і забезпечення нормального функціонування кіберпростору, захищаючи його від виникнення загроз ефективним чином.

Згідно із Законом (Закон України «Про основні засади забезпечення кібербезпеки України», 2017) *кібербезпека* – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. На нашу думку, це досить вдале визначення, адже воно містить як статичну (захищеність), так і динамічну (забезпечення) складові частини. З огляду на таке визначення констатуємо, що основний акцент повинен бути зроблений на збереженні сприятливого стану кіберпростору.

Кібербезпека з огляду на тріаду складових кіберпростору охоплює не тільки інформацію як об'єкт захисту, не тільки технічні засоби, які визначають можливості функціонування інформації, а і захист способів функціонування нової сутності – кіберпростору. Захищається діяльність людей, яка здійснюється за допомогою інформації, поширюваної за допомогою технічної інфраструктури ІКТ. При забезпеченні кібербезпеки важливо враховувати зазначені особливості кіберпростору і його найбільш важливий аспект – наявність взаємозв'язків між учасниками (користувачами), що призводить до можливості виникнення синергетичного ефекту.

Переводячи охарактеризовані поняття «кіберпростір» та «кібербезпека» в економічну площину, зазначимо, що їх сутність не змінюється, а акцентується тільки галузь їх застосування у сфері національної безпеки. Систему національної безпеки в такому розрізі пропонується розглядати за прикладом на рис. 1.

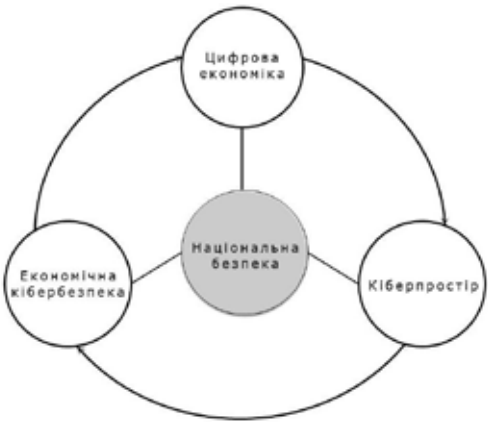

Рис. 1. Система національної безпеки у кіберекономічному розрізі

Наведемо логіку побудови такої системи.

Інтереси національної безпеки потребують якнайшвидшого впровадження цифрової економіки, функціонування якої переважно відбувається у кіберпросторі. Останній фактично становить загальний простір взаємодії інформаційних потоків, в якому спостерігається глобалізація у всьому різноманітті її проявів. Кіберпростір не виокремлюється межами національних держав, його межі рухливі і мінливі, він розсіяний повсюди, хоча і не відображений ні на одній карті світу. З'являється новий формат соціально-економічних процесів і внутрішніх відносин, включаючи нові форми транскордонної соціалізації (через розваги, роботу, приналежність до груп інтересів тощо), що робить зв'язок із національними кордонами дедалі примарнішим (Закон України «Про основні засади забезпечення кібербезпеки України», 2017).

Новітні економічні процеси в кіберпросторі потребують адекватних безпекових заходів. Економічна кібербезпека починає відігравати надзвичайне значення для національної безпеки, адже кіберзлочини у вигляді кібершпигунства (викрадення інформації про новітні технологічні розробки, фінансові операції тощо) та кібератак, ціллю яких є порушення роботи систем життєзабезпечення, програмного забезпечення, відключення або вивід із ладу техніки, можуть нанести непоправної шкоди стратегічно важливим об'єктам як державного, так і приватного сектору, створити умови для масового невдоволення населення. Поряд з уже згадуваним вірусом Petya, можна навести атаку у 2015 на енергосистему «Прикарпаттяобленерго», в результаті чого вона була виведена з ладу. Із останніх кіберінцидентів можна виділити масштабну кібератаку Sunburst (Сонячні промені), яка сталася в грудні 2020 року, на більш ніж 200 державних установ і великих компаній США, в тому числі і приватні компанії, такі як FireEye і Microsoft. Хакери, зокрема, отримали доступ до електронної пошти міністерств фінансів, юстиції та торгівлі США, а також інших агентств. Як вважають в американських відомствах, метою злому мереж федеральних установ було отримання розвідданих, пов'язаних із забезпеченням національної безпеки. Відзначимо, що в подібних злочинах беруть участь не поодинокі особи, а спеціально створені під егідою держави-зловмисника установи. Тобто економічне протистояння набуває характерних ознак кібервійни. У травні 2019 р. навіть (вперше в історії) була застосована реальна військова сила з метою запобігання кібератаки: повітряні сили Ізраїлю здійснили удар по будівлі в Газі, звідки здійснювалася діяльність хакерів. За заявою представників ізраїльських збройних сил, кібернапад був спрямований на шкоду якості життя громадян Ізраїлю.

М.А. Ческідов підкреслює особливості інформаційної війни як загрози економічній безпеці в кіберпросторі (Ческидов, 2013):

– поляризація масштабів джерела і об'єкта впливу (окремий індивід чи локальна група, використовуючи сучасні інформаційно-комунікаційні технології, може завдати значної шкоди великим соціально-економічним системам);

– латентний характер, зумовлений складністю розпізнавання інформаційно-мережевих технологій і суб'єктів інформаційної агресії, а також високою вартістю методів боротьби;

– незворотність наслідків (у разі викрадення інформації неможливо відновити її конфіденційність, цілісність і повноту);

– неможливість повної ліквідації і викорінення інформаційної агресії, що зумовлена об'єктивністю існування глобального кіберпростору;

– вплив на відстані, що обмежує можливості застосування санкцій щодо кіберагресорів;

– кумулятивний ефект поширення форм інформаційної агресії в економіці (первинне застосування шкідливих технологій надалі не піддається контролю і активно нарощує масштаби).

Економічна кібербезпека в приведеній на рис. 1. системі має бути спрямована на превенцію, виявлення і ліквідацію таких загроз:

– кібершпигунства і маніпулювання унікальною інформацією, що ведуть до порушення стійкості розвитку економіки, ослаблення валюти, нереалізації намічених програм, підриву інвестиційних проєктів;

– економічних кібервійн, що ведуть до відставання ВВП, викликаного зростанням непродуктивних витрат, формуванням нового сегмента тіньової економіки – «чорного» кіберринку і порушенням ринкових механізмів і принципів конкуренції, монополізацією економіки;

– інформаційного домінування розвинених країн, що веде до набування ними технологічної ренти і посилення від них економічної залежності, витіснення слабкої національної економіки зі світового інформаційного ринку.

Останній пункт прямо вказує на необхідність розвитку національної цифрової економіки. Однак впровадження будь-якої новітньої технології несе ризики кібербезпеці. Це свідчить про те, що розвиток безпекового аспекту є фунда-

ментом ефективності цифрової економіки (що і відображено стрілкою на рис. 1). Про це опосередковано свідчать і результати досліджень, наведених у джерелі (Аллахвердиева, Бахшалиев, 2019, с. 41–50):

– у розвинених країнах рівень кібербезпеки і показники розвитку цифрової економіки в середньому вищі, ніж в країнах, що розвиваються;

– чим вище в країні рівень кібербезпеки, тим більше число здійснюваних в ній цифрових платежів, і навпаки;

– підвищення рівня кібербезпеки може бути недостатнім для підвищення рівня розвитку цифрової економіки, оскільки на цей процес впливає низка інших факторів, таких як загальний рівень економічного розвитку країни, рівень розвитку сфери ІКТ, міжнародна відкритість тощо (це твердження свідчить про причинно-наслідковий зв'язок між цифровою економікою та кібербезпекою – *П. О., Г. В.*).

4. Зміна парадигми стратегії кібербезпеки

Високий рівень розвитку кіберпростору і організації кіберзагроз вказує на необхідність зміни парадигми стратегії кібербезпеки: вона повинна базуватися не на реагуванні за фактом, а на принципах прогнозування і планування захисту від майбутніх дій кіберзлочинців. Для цього потрібно постійно аналізувати сучасні тренди економічних кіберзагроз. На основі матеріалів, викладених спеціалізованими компаніями Positive Technologies (https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/), Group-IB (https://www.group-ib.ru/blog/results), та дослідження (Шитова, Шитов, 2019, с. 22–30), виділимо найбільш актуальні із них на даний час.

Провідним і найнебезпечнішим трендом є використання кіберзброї в конфліктах між державами, що набуває нових форм, а кіберактивність відіграє провідну роль в цьому деструктивному діалозі. Атаки на критичну інфраструктуру і цілеспрямована дестабілізація мережі Інтернет в окремих країнах відкривають нову епоху проведення кібератак, які можуть призвести не тільки до порушення технологічних процесів, а і до людських жертв.

Зростає кількість атак з метою шпигунства, отримання конфіденційних даних. При цьому атаки, спрямовані на розкрадання інформації, часто містять фінансовий підтекст: вкрадені дані потім використовуються для крадіжки грошей, шантажу або розміщуються для продажу на тіньовому ринку, тобто кіберзлочинність більше переплітається з іншими видами злочинної діяльності, які зазвичай не потрапляють в поле зору фахівців з інформаційної безпеки. Ще один з актуальних трендів глобального рівня – злом персональних пристроїв головних посадових осіб держави та бізнесу.

Часто відбуваються цілеспрямовані атаки на фінансові установи. Сучасний досвід хакерів та спеціалізоване програмне забезпечення здатні зламати багаторівневу захисну систему банку і зняти кошти. Триває процес консолідації і зростання хакерських груп, з'являються нові, ще більш витончені методи, відбувається швидкий «обмін досвідом» і спільні координовані дії різних угруповань, що ускладнює процес їх ідентифікації. На ринку кіберпослуг з'являтиметься все більше готових програмних продуктів для масового використання. В результаті одні й ті ж програми будуть використовуватися різними групами кіберзлочинців, що істотно ускладнить їх атрибуцію.

Атака мережевих пристроїв і перехоплення трафіку – найсвіжіший тренд розвитку кіберпрзлочинності, що полягає у зломі не кінцевих комп'ютерів, а мережевих пристроїв, що керують трафіком. В результаті здійснюється не тільки аналіз і крадіжка даних, але й складні комбінації з підміною мережевих адрес, що дозволяють перенаправляти трафік з справжніх на фейкові фішингові сайти. Одним з показових є приклад, коли, використовуючи протокол BGP, зловмисники змогли перенаправити трафік сервісу Amazon Route 53 (DNS-сервіс, що надається Amazon) на свій DNS-сервер, який надавав сайту MyEtherWallet.com IP-адресу серверу атакуючих, що містить трохи підправлений клон оригінального сайту. У разі прийняття сертифіката і аутентифікації на фішинговому сайті у користувача списувалися всі кошти з гаманця. Всього за дві години, поки не було помічено підміну, зловмисникам вдалося вкрасти ~ 137 тис. доларів (https://habr.com/ru/post/354384/).

Розвиток і вдосконалення шифрувальників і здирників (ransomware) – окремий тип вірусного ПЗ, що є особливо небезпечним в економічному плані. Проникаючи на машини, шкідливий код даного типу шифрує дані і вимагає грошовий викуп за дешифрування (наприклад, уже згадуваний вірус Petya).

Проте найбільша небезпека – не в сумі грошей, а в загрозі бізнесу. Наприклад, кожна п'ята компанія, що піддалася атаці здирників, була змушена закрити свій бізнес (дані 2017 року). У 48% компаній сталася втрата даних або обладнання, а з 42%, які заплатили викуп, чверть

була обманута (https://www.fortinet.com/blog/industry-trends/ransomware-are-you-paying-attention). Спеціалісти з кібербезпеки впевнені, що крадіжка даних з вимогою викупу залишається важливим напрямом кібератак і одним з основних каналів заробітку злочинців.

Відбулася еволюція способів соціальної інженерії (психологічної маніпуляції). Зловмисники удосконалюють методи психологічної маніпуляції для отримання банківських даних, використання підроблених акаунтів у соцмережах, здійснюють дзвінки з надійних номерів, купують для надійності бази паспортних даних тощо. До відносно нових методів соціальної інженерії можна віднести управління телефоном за допомогою програм віддаленого доступу, які жертви встановлюють на свої пристрої на прохання телефонних шахраїв.

Щоб протистояти розглянутим викликам, Україні потрібна нова кіберстратегія. Як було зазначено, робота в цьому напрямі вже ведеться. Важливо, на наш погляд і на думку низки експертів (Янковський, Корсун, Барановський, 2019), щоб шлях, яким рухається Україна у розбудові власної кібербезпеки, набув відповідних невідкладних змін. Поступ цей має бути швидким. Необхідність змін підтверджена постійними атаками на об'єкти критичної інфраструктури та багатьма іншими інцидентами. За останніми даними СБУ (9 березня 2021 року) лише за 2020 рік Служба:

– заблокувала понад 2,5 тис. спільнот у соцмережах з мільйонною аудиторією та понад 20 ботмереж потужністю більше 60 тис. акаунтів;

– нейтралізувала понад 600 кіберінцидентів та кібератак на інформаційні ресурси органів державної влади;

– припинила діяльність 20 хакерських угруповань, причетних до таких атак.

Наголошено, що через такі мережі злочинці збирають розвідувальні та персональні дані громадян України, а потім атакують органи влади та об'єкти критичної інфраструктури держави (https://ssu.gov.ua/novyny/u-spetssluzhbakh-rf-ye-pidrozdily-yaki-pratsiuiut-vykliuchno-za-ukrainskym-napriamom-departament-kiberbezpeky-sbu).

Серед заходів, що мають знайти першочергове втілення, відзначимо такі:

1) в умовах наростання цифровізації економіки і суспільства необхідне інтенсивне підвищення ефективності нормативної бази, спрямованої на реалізацію системи управління кібербезпекою. Зокрема, необхідно замінити НД ТЗІ, який вже давно застарів, більш ефективним та сучасним базовим стандартом і запровадити галузеві стандарти кібербезпеки. Для прискорення цього можна задіяти міжнародні стандарти, які зарекомендували себе в розвинених країнах світу. Що стосується галузевих стандартів, то питання регулювання та контролю можна делегувати галузевим регуляторам або саморегулятивним організаціям, як це зроблено у провідних країнах;

2) роль держави у розбудові вітчизняної системи кіберзахисту потребує переосмислення. Згідно з новою Стратегією держава має перейти від моделі, коли вона контролює кібербезпеку, зокрема в приватних організаціях, до саморегуляції. Виключення мають бути тільки для об'єктів критичної інфраструктури. Критерії віднесення об'єктів до критичної інфраструктури мають бути чітко визначені і розроблятися експертами та бути такими, що можна виміряти;

3) важливим кроком має стати створення Експертної ради з питань кібербезпеки за участю фахівців з інформаційної безпеки, професійних спільнот, практичних психологів з управління персоналом, представників бізнесу та державних органів. Така рада має готувати пропозиції щодо нормативно-правових актів у цій сфері, давати рекомендації з функціонування національної системи кібербезпеки та вирішувати інші завдання та проблеми, які потребують належної експертизи;

4) необхідне налагодження обміну інформацією про кіберінциденти та тісна співпраця держави з дослідниками та приватними компаніями. Створення галузевих центрів реагування на кіберінциденти та центрів обміну інформацією про кібератаки допоможе з вирішенням цієї проблеми. При цьому ці центри мають тісно взаємодіяти з міжнародною мережею подібних організацій;

5) Щоб мінімізувати збитки від кібератак, важливо фокусуватися не лише на захисті, але й на побудові вивірених процесів реагування на інциденти. Рівень обізнаності українців з питань кібербезпеки потребує розвитку на покращення. Необхідна затверджена Державна програма навчання для громадян та організацій, формування як загальної інформаційної культури, так і культури кібербезпеки в суспільстві.

5. Висновки

Революція у сфері зв'язку та комунікацій стала суттєвим чинником розвитку цифрової економіки та кіберпростору, в якому вона функціонує. Водночас виникають кібербезпекові проблеми, що потребують вирішення з точки зору національної безпеки.

Визначено поняття «кіберпростір» та «кібербезпека» в економічній площині. Їх взаємозв'язок та роль у цифровізації економіки дали змогу відобразити модель системи національної безпеки у кіберекономічному розрізі.

Узагальнення і розкриття причин і коренів кіберзлочинів, дій зловмисників залишається одним із складних завдань у сфері забезпечення кібербезпеки в умовах інтенсивної цифровізації економіки. Необхідно точно і завчасно класифікувати елементи небезпеки в кіберпросторі, вивчати їх характеристики і сутність з виділенням основних особливостей, тактик і дій зловмисників, розробляти адекватні механізми запобігання та припинення злочинних діянь.

Результати дослідження показують важливість усвідомлення серйозних проблем забезпечення кібербезпеки, що вимагають розробки і здійснення більш ефективних механізмів функціонування і забезпечення роботи кіберпростору, підвищення надійності основних механізмів і компонентів глобальної Інтернет-мережі та інших пристроїв ІКТ, врахування людського фактору, комплексного і системного підходу в визначенні методичних засад та інструментів формування державної політики з забезпечення кібербезпеки.

Необхідна постійна увага до стрімкого змінення тенденцій розвитку економічних кіберзагроз в контексті національної безпеки, тому діяльність як науковців, так і державників у цьому напрямі повинна бути перманентною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аллахвердиева Л.А., Бахшалиев Ф.Р. Кибербезопасность как фактор развития цифровой экономики. *Вестник ИЭРАН*. 2019. № 6. С. 41–50. DOI: 10.24411/ 2073- 6487-2019-10069.
2. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия. *Вопросы кибербезопасности*. 2014. № 1 (2). С. 22–27.
3. Доклад о цифровой экономике 2019 : Обзор. Организация Объединенных Наций. 2019. URL: https://unctad.org/system/files/official-document/der2019_overview_ru.pdf (дата звернення: 26.07.2021).
4. Про національну безпеку : Закон України від 21.06.2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 26.07.2021).
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163- VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 26.07.2021).
6. Коноплева Ю.А., Корыстов В.А., Тесленко Д.В. Кибербезопасность как фактор развития цифровой экономики. *Вестник Северо-Кавказского федерального университета*. 2019. № 4 (73). С. 49–55.
7. Концепція розвитку цифрової економіки та суспільства на 2018–2020 роки : Розпорядження Кабінету Міністрів України від 17.01.18 р. № 67-р. *Урядовий кур'єр*. 11.05.2018. № 88.
8. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032. *Вопросы кибербезопасности*. 2014. № 1 (2). С. 28–35.
9. Про Стратегію національної безпеки України : Указ Президента України № 392/2020 від 14 вересня 2020 року. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 26.07.2021).
10. Ческидов М.А. Экономическая безопасность государства в условиях информационной экономики : автореферат. Саратов. 2013. URL: https://www.dissercat.com/content/ekonomicheskaya-bezopasnost-gosudarstva-v-usloviyakh-informatsionnoi-ekonomiki (дата звернення: 26.07.2021).
11. Шитова Ю.Ю., Шитов Ю.А. Современные тренды экономической кибербезопасности. *Мир новой экономики*. 2019. № 13 (3). С. 22–30. DOI: 10.26794/2220-6469-2019-13-4-22-30.
12. Янковський О., Корсун К., Барановський О. та інші. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/ (дата звернення: 26.07.2021).

REFERENCES

1. Allakhverdiyeva, L.A., & Bakhshaliyev, F.R. (2019). Kiberbezopasnost kak faktor razvitiya tsifrovoy ekonomiki [Cybersecurity as a factor in the development of the digital economy]. *Vestnik IERAN, 6,* 41-50. DOI: 10.24411/2073-6487-2019-10069. [in Russian].
2. Bezkorovaynyy, M.M., & Tatuzov, A.L. (2014). Kiberbezopasnost – podkhody k opredeleniyu ponyatiya [Cybersecurity – Approaches to the Definition of the Concept]. *Voprosy kiberbezopasnosti – Cybersecurity issues, 1(2)*, 22-27. [in Russian].
3. Doklad o tsifrovoy ekonomike 2019: Obzor. [Digital Economy Report 2019: An Overview] (2019). *unctad.org*. Organizatsiya Obyedinennykh Natsiy. URL: https://unctad.org/system/files/official-document/der2019_overview_ru.pdf. [in Russian].
4. Zakon Ukrayiny "Pro natsionalnu bezpeku" [Law of Ukraine "On National Security"]. (June 21, 2018), 2469-VIII. *zakon.rada.gov.ua*. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text. [in Ukrainian].
5. Zakon Ukrayiny "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny" [Law of Ukraine "On the basic principles of cyber security of Ukraine"] (05.10.2017), 2163-VIII. *zakon.rada.gov.ua*. URL: https://zakon.rada.gov.ua/laws/show/2163-19. [in Ukrainian].
6. Konopleva, Yu.A., Korystov, V.A., & Teslenko, D.V. (2019). Kiberbezopasnost kak faktor razvitiya tsi-

frovoy ekonomiki [Cybersecurity as a factor in the development of the digital economy]. *Vestnik Severo-Kavkazskogo federalnogo universiteta. 4 (73),* 49-55. [in Russian].
7. Kontseptsiya rozvytku tsyfrovoyi ekonomiky ta suspilstva na 2018 – 2020 roky: Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 17.01.18 r. № 67-r. [The concept of development of the digital economy and society for 2018 – 2020: Order of the Cabinet of Ministers of Ukraine dated 17.01.18 № 67-r]. (05.11.2018). *Uryadovyy kuryer – Government courier, 88.* [in Ukrainian].
8. Markov, A.S., & Tsirlov, V.L. (2014). Rukovodyashchiye ukazaniya po kiberbezopasnosti v kontekste ISO 27032 [Guidelines for cybersecurity in the context of ISO 27032]. *Voprosy kiberbezopasnosti – Cybersecurity issues, 1(2)*, 28-35. [in Russian].
9. Ukaz Prezydenta Ukrayiny № 392/2020 Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny "Pro Stratehiyu natsionalnoyi bezpeky Ukrayiny" [Decree of the President of Ukraine № 392 / 2020 On the Decision of the National Security and Defense Council of Ukraine "On the National Security Strategy of Ukraine"]. (September 14, 2020). *www.president.gov.ua*. URL: https://www.president.gov.ua/documents/3922020-35037. [in Ukrainian].
10. Cheskidov, M.A. (2013). Ekonomicheskaya bezopasnost gosudarstva v usloviyakh informatsionnoy ekonomiki [Economic security of the state in the information economy]. *Avtoreferat*. Saratov. URL: https://www.dissercat.com/content/ekonomicheskaya-bezopasnost-gosudarstva-v-usloviyakh-informatsionnoi-ekonomiki [in Russian].
11. Shitova, Yu.Yu., & Shitov, Yu.A. (2019). Sovremennyye trendy ekonomicheskoy kiberbezopasnosti. [Modern trends in economic cybersecurity]. *Mir novoy ekonomiki – The world of the new economy, 13(3)*. 22-30. DOI: 10.26794/2220-6469-2019-13-4-22-30. [in Russian].
12. Yankovskyy O., Korsun K., Baranovskyy O., Aushev Y., Karpynskyy A., Styran V. Ukrayini potribna nova kiberstratehiya [Ukraine needs a new cyber strategy]. *www.pravda.com.ua*. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/. [in Ukrainian].