18. The Administrator of the Economic Cooperation Administration (Hoffman) to the Acting Secretary of State (1949) Washington, January 19, 1949. *Foreign Relations of the United States. The Far East: China,* vol. IX Document, 297, p. 270 (in English).

19. The Consul General at Taipei (Krentz) to the Secretary of State (1949). Taipei, January 15, 1949. *Foreign Relations of the United States, The Far East: China,* vol. IX Document, 295, p. 267–269 (in English).

20. The Consul General at Shanghai (Cabot) to the Secretary of State (1949). Shanghai, January 26, 1949. *Foreign Relations of the United States, The Far East: China,* vol. IX Document, 302. p. 277 (in English).

21. The Consul General at Taipei (Krentz) to the Secretary of State (1949). Taipei, January 27, 1949. *Foreign Relations of the United States, The Far East: China,* vol. IX Document, 303, p. 277 (in English).

22. Note by the Executive Secretary of the National Security Council (Souers) to the Council (1949). Washington. February 11, 1949. *Foreign Relations of the United States, The Far East: China,* vol. IX Document, 314? p. 284–286 (in English).

Матеріал надійшов до редакції 17.09.2024 р.

УДК 323.28(100):004.9.056

Олександр Гоманюк,
здобувач за спеціальністю 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»,
alex.ua.man@gmail.com,
ORCID ID: 0009-0001-7635-6519,
DOI 10.29038/2524-2679-2024-03-19-34

КІБЕРЗАГРОЗИ ТА ГЛОБАЛЬНА БЕЗПЕКА: ВІД НАЦІОНАЛЬНИХ СТРАТЕГІЙ ДО МІЖНАРОДНОЇ СПІВПРАЦІ

У статті розглянуто питання кібербезпеки в сучасному світі, де інформаційні технології відіграють важливу роль у політичній, економічній та військовій сферах. Зростання цифрової інфраструктури супроводжується збільшенням кіберзагроз, які можуть бути спрямовані як проти держав, так і проти міжнародної спільноти. Увагу акцентовано на тому, що кібербезпека стає критично важливим аспектом національної

та міжнародної безпеки, вимагаючи колективних зусиль для захисту від потенційних загроз, таких як кібератаки на державні установи, критичну інфраструктуру, а також шпигунство й соціальну інженерію. Особливу увагу приділено аналізу різних форм кіберзагроз та їх впливу на глобальну безпеку. Описано конкретні приклади кібератак, як-от: утручання у виборчі процеси в США й атака на енергетичну інфраструктуру України. Автори висвітлюють ключові аспекти кібербезпеки, уключаючи технічні, правові та освітні заходи, що спрямовані на забезпечення безпеки в цифровому просторі. У статті також розглядається роль міжнародної співпраці в контексті кібербезпеки, підкреслено важливість об'єднаних зусиль урядів, приватного сектору та міжнародних організацій, як-от: ООН, НАТО і ЄС. Розглянуто стратегії різних країн, зокрема США та Ізраїлю, у сфері кіберзахисту, а також кроки, які робить Україна для посилення своєї кібербезпеки на тлі російської агресії. У статті обговорюються також виклики, пов'язані з кібербезпекою, уключаючи недостатнє фінансування, швидкість технологічного прогресу, людський фактор і відсутність єдиних міжнародних правових рамок у сфері кіберпростору. У статті підкреслено необхідність розвитку національних стратегій кібербезпеки та тісної співпраці між державами для протидії зростаючим кіберзагрозам у глобалізованому світі.

Ключові слова: кібербезпека, кібератаки, кіберзагрози, інформаційна безпека, критична інфраструктура, гібридна війна, міжнародна співпраця, національна безпека, цифрова інфраструктура.

Oleksandr Homanyuk,
ORCID ID: 0009-0001-7635-6519

CYBER THREATS AND GLOBAL SECURITY: FROM NATIONAL STRATEGIES TO INTERNATIONAL COOPERATION

The article examines the issues of cybersecurity in the modern world, where information technologies play an important role in the political, economic and military spheres. The growth of digital infrastructure is accompanied by an increase in cyber threats, which can be directed against both states and the international community. The article emphasizes that cybersecurity is becoming a critically important aspect of na-

tional and international security, requiring collective efforts to protect against potential threats, such as cyber attacks on state institutions, critical infrastructure, as well as espionage and social engineering. Special attention is paid to the analysis of various forms of cyber threats and their impact on global security. Specific examples of cyberattacks are described, such as interference in the US election process and an attack on the energy infrastructure of Ukraine.

The authors highlight key aspects of cybersecurity, including technical, legal and educational measures aimed at ensuring security in the digital space. The article also considers the role of international cooperation in the context of cybersecurity, emphasizing the importance of joint efforts of governments, the private sector and international organizations such as the UN, NATO and the EU. The strategies of various countries, in particular the USA and Israel, in the field of cyber defense are considered, as well as the steps that Ukraine is taking to strengthen its cybersecurity in the face of Russian aggression. The article also discusses the challenges associated with cybersecurity, including insufficient funding, the speed of technological progress, the human factor and the lack of a unified international legal framework in cyberspace. The article emphasizes the need to develop national cybersecurity strategies and close cooperation between states to counter growing cyber threats in a globalized world.

Key words: cybersecurity, cyber attacks, cyber threats, information security, critical infrastructure, hybrid warfare, international cooperation, national security, digital infrastructure.

1. ВСТУП

Постановка проблеми. У сучасному світі інформаційні технології відіграють ключову роль у всіх сферах життя, уключаючи економіку, політику, військові дії та міжособистісні комунікації. Із розвитком цифрової інфраструктури зростає й кількість кіберзагроз, що ставлять під загрозу як окремі держави, так і міжнародну спільноту загалом. Кібербезпека стала однією з ключових складових частин національної та міжнародної безпеки, що вимагає колективних зусиль для її забезпечення. Це питання охоплює різні аспекти, починаючи від захисту критичних інфраструктур і закінчуючи попередженням глобальних кібератак, спроможних дестабілізувати геополітичну ситуацію. Це питання не лише технологічне, але й геополітичне, оскільки загрози можуть походити як від окремих хакерів,

так і від державних акторів. З огляду на гібридні війни, кібератаки та інформаційні кампанії, які активно застосовуються як інструменти впливу, захист національних інтересів у кіберпросторі стає одним із ключових завдань для урядів. Для України, яка вже тривалий час перебуває в стані військової агресії з боку російської федерації, кібербезпека є важливим компонентом національної безпеки, особливо з огляду на масштабні кібератаки, що супроводжують військові дії. Незважаючи на декларовані бажання основних геополітичних суб'єктів протидіяти мілітаризації кіберпростору, можемо констатувати збільшення ролі суто військових структур у забезпечення безпеки національної критично важливої інфраструктури (національного кіберпростору). Найімовірніше, ініціативи в межах ООН щодо вироблення комплексних підходів до міжнародної інформаційної безпеки будуть або повністю невдалими, або обмежено вдалими (на рівні декларативної згоди). У таких умовах Україна має бути готова не лише до ведення оборонних війн, але й активно створювати власні наступальні засоби ведення війни в кіберпросторі.

Мета дослідження – проаналізувати сучасні загрози кібербезпеці, зокрема у сфері захисту критичної інфраструктури держави, а також визначені ролі міжнародної співпраці в протидії кібератакам і гібридним загрозам. Дослідження фокусується на тому, як ефективно зміцнювати інформаційну безпеку та підвищувати стійкість до кібератак у глобалізованому цифровому середовищі.

Методи дослідження – аналіз документів – вивчення законодавчих актів, міжнародних угод та стратегій кібербезпеки; порівняльний аналіз – порівняння кібербезпекових підходів різних країн; метод кейс-стаді – аналіз конкретних прикладів успішних і невдалих кіберзахисних операцій та атак; емпіричні дослідження – збір й аналіз даних про актуальні кіберзагрози та інциденти; контент-аналіз – вивчення медійних повідомлень й інформаційних кампаній у контексті гібридної війни. Ці методи дають змогу комплексно оцінити як поточний стан кіберзагроз, так і необхідні заходи для їх подолання.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Кібербезпека визначається як сукупність заходів, спрямованих на захист інформаційних систем, комп'ютерних мереж і даних від несанкціонованого доступу, атак, руйнувань та зловживань. Вона охоплює як технічні, так і організаційні, правові й освітні аспекти, що спрямовані на забезпечення безперебійної та безпечної роботи систем. Важливість

кібербезпеки зростає пропорційно до рівня цифровізації суспільства і його залежності від інформаційних технологій.

Згідно зі стандартом ISO/IEC 27032:2012, кібербезпека, безпека кіберпростору (cybersecurity, cyberspace security) – збереження цілісності, конфіденційності та доступності інформації, що циркулює в кіберсистемі (тобто інформації, що надходить у кіберсистему, накопичується й зберігається в ній для подальшої обробки), із метою забезпечення стійкості та безперервності реалізації кіберсистемою управлінських функцій щодо відповідних об'єктів управління [16]. Відповідно, кіберпростір – частина інформаційного простору, утворена інформаційними потоками й інформаційними полями, що породжуються в процесі функціонування кібернетичних систем [14, с. 45].

У світі, де фінансові системи, державні установи, енергетична інфраструктура, військові мережі та навіть побутові технології залежать від інтернету, будь-які вразливості можуть мати глобальні наслідки. За даними різних досліджень, кібератаки спричиняють щорічні збитки в трильйони доларів і можуть дестабілізувати економіки цілих держав, підірвати довіру до урядів та корпоративних структур, а також призвести до людських жертв у випадку атак на критичні інфраструктури.

Кіберзагрози мають різні форми й можуть бути спрямовані на різні об'єкти. Серед найпоширеніших загроз можна виділити [9]:

• кібератаки на державні установи: спроби викрасти інформацію, зламати системи національної безпеки чи вплинути на політичні процеси, такі як вибори. Яскравим прикладом є втручання у виборчі процеси в США у 2016 р., коли хакери намагалися вплинути на результат виборів;

• атаки на критичну інфраструктуру: енергетичні системи, водопостачання, транспортні мережі та інші об'єкти можуть стати об'єктами кібератак, що призводить до катастрофічних наслідків. Атака на українську енергетичну систему у 2015 р. стала одним із перших прикладів успішної кібератаки на критичну інфраструктуру;

• шкідливі програми та віруси: шкідливе програмне забезпечення, зокрема віруси, трояни й програми-здирники, можуть бути використані для викрадення даних, пошкодження систем або вимагання грошей. Наприклад, вірус WannaCry у 2017 р. заблокував комп'ютери по всьому світу, вимагаючи викуп за їх розблокування;

• кібершпигунство: держави можуть використовувати кіберзасоби для шпигунства за іншими країнами або для викрадення секретної інформації, що може призвести до загострення міжнародних конфліктів;

• соціальна інженерія та фішинг: ці методи використовують психологічні трюки для того, щоб змусити користувачів розкрити конфіденційну інформацію або завантажити шкідливе програмне забезпечення.

Сьогодні багато країн уключають кібербезпеку як невід'ємну частину своїх національних стратегій безпеки. Уряди держав створюють спеціальні агентства та центри, що займаються питаннями кіберзахисту, розробляють відповідне законодавство й підтримують розвиток відповідної інфраструктури. Наприклад, у США функціонує Агентство з кібербезпеки та безпеки інфраструктури (CISA), яке відповідає за захист від кіберзагроз як державних, так і приватних об'єктів. У Європейському Союзі діє Агентство з мережевої й інформаційної безпеки (ENISA), яке допомагає країнам-членам координувати свої зусилля у сфері кібербезпеки.

Багато країн також вносять питання кіберзахисту в рамки своєї військової стратегії. Кіберпростір вважається п'ятим театром військових дій, нарівні із сушею, водою, повітрям та космосом. Військові кібервідділи займаються як захистом власних систем, так і розробкою наступальних кібератак. Це включає можливість паралізувати ворожі системи управління, комунікації, енергозабезпечення та інші критичні інфраструктури.

Загрози в кіберпросторі стають усе більш складними й різноманітними. Серед основних загроз можна виокремити такі:

• кібершпигунство. Використання кіберзасобів для збору інформації про урядові, військові та економічні структури інших держав може стати серйозною загрозою для національної безпеки. Викрадена інформація може бути використана для впливу на внутрішні та зовнішні політичні процеси;

• кібертероризм. Хакери можуть атакувати критичні інфраструктури держави (електростанції, водопостачання, транспортні системи), що призводить до масових катастроф і дестабілізації країни;

• кібервійни. У сучасних військових конфліктах кіберзброя застосовується нарівні з традиційними військовими засобами. Держави розвивають кібервійськові підрозділи для проведення наступальних і захисних операцій у кіберпросторі;

• дестабілізація інформаційного простору. Через фейки, дезінформацію та пропаганду може порушуватися політична стабільність, підриватися довіра до державних інститутів, що впливає на національну безпеку.

Кібератаки, спрямовані проти України, мають такі самі основні риси: російські спецслужби активно застосовують кіберінструменти для збору

інформації про політичні, військові й економічні процеси в Україні. Такі атаки спрямовані на здобуття стратегічної інформації та подальше її використання для дестабілізації ситуації. Як засвідчили випадки з енергосистемами, кібернапади можуть паралізувати важливі об'єкти інфраструктури, завдаючи серйозної шкоди економіці та безпеці країни. Кібератаки часто супроводжуються інформаційними операціями, що спрямовані на підрив довіри до українських інститутів, створення паніки чи вплив на громадську думку. З огляду на те, що багато стратегічно важливих інфраструктур перебувають у приватних руках, атаки на компанії стають ще однією формою кіберзагрози [8].

Міжнародна кібербезпека не може бути забезпечена без тісної співпраці між державами, оскільки кібератаки не знають кордонів. Інтернет є глобальним – й атаки, організовані в одній країні, можуть завдати шкоди іншим державам. Тому співпраця на міжнародному рівні є надзвичайно важливою для створення ефективних механізмів протидії кіберзагрозам.

Організація Об'єднаних Націй, НАТО, Європейський Союз та інші міжнародні організації активно розробляють стандарти, політики й стратегії у сфері кібербезпеки. Наприклад, у рамках НАТО кіберзахист входить до основних пріоритетів колективної безпеки, а напад у кіберпросторі може розглядатися як привід для застосування статті 5 Статуту НАТО, яка передбачає колективну оборону.

У рамках ООН проводяться конференції та консультації щодо розробки глобальних правил і норм поведінки держав у кіберпросторі. Спроба створити міжнародний кодекс поведінки в кіберпросторі має на меті обмежити застосування кіберзасобів у воєнних цілях і забезпечити стабільність цифрового простору.

Незважаючи на всі зусилля, кібербезпека залишається серйозним викликом для міжнародної спільноти. Важливою проблемою є відсутність єдиних міжнародних правил та норм у сфері кіберпростору. Багато держав використовують кіберзасоби для досягнення власних геополітичних цілей, що призводить до конфліктів і напруженості на міжнародній арені.

Іншим важливим аспектом є технологічний прогрес. Із появою нових технологій, таких як штучний інтелект, квантові обчислення й інтернет речей, зростають також можливості кібератак. Захист від таких загроз вимагає постійного вдосконалення кіберзахисних систем і підвищення рівня підготовки спеціалістів у цій сфері.

У п.п. 2000-х років найбільш впливовими й активними вважаються військові кіберпідрозділи Китаю та США. Інформація щодо потенціалу,

чисельності й завдань китайських кібервійськ практично відсутня. У серпні 2010 р. компанія Armorize мала оприлюднити дослідження про реальний потенціал китайських і тайванських кібервійськ на конференції Black Hat, але через вимогу керівництва Тайваню цього не сталося. За даними, що не містять конкретних указівок щодо потенціалу кібервійськ Китаю, у середині серпня 2010 р. Міністерство оборони США опублікувало доповідь про військову міць Китаю, де висловлюється припущення про можливу підтримку атак на мережі, що належать уряду США з боку Народно-визвольної армії Китаю або самого китайського уряду. За даними видання The Daily Beast, ФБР підготувало секретний звіт, у якому Китай названо «найбільшою загрозою для США у сфері кібертероризму», спроможною знищувати життєво важливу інфраструктуру та отримувати доступ до стратегічних баз даних. Згідно з цим звітом, Китай наразі має армію з 180 000 хакерів, які активно здійснюють атаки на американські кібермережі, уключаючи 90 000 атак лише у 2009 р. проти комп'ютерів Міністерства оборони США [8].

Різні країни розробляють свої підходи до кібербезпеки, але існують спільні риси у формуванні стратегій. Американська стратегія кібербезпеки передбачає захист критичної інфраструктури, розвиток наступальних кіберможливостей та активне міжнародне співробітництво. США також активно інвестують у розвиток технологій штучного інтелекту й квантових обчислень для покращення кіберзахисту. Ізраїль вважається одним зі світових лідерів у галузі кібербезпеки завдяки інтенсивній співпраці між урядом, приватним сектором та університетами. Ізраїльські кібервійська визнані одними з найефективніших у світі, а країна активно розвиває експорт технологій кіберзахисту. У 2013 р. Європейський Союз ухвалив Стратегію кібербезпеки, метою якої є відкритий, надійний і безпечний кіберпростір. Для цього передбачені заходи з таких напрямів, як досягнення кіберстійкості, суттєве скорочення кіберзлочинності, розробка політики кібероборони, пов'язаної зі Спільною політикою безпеки й оборони, розвиток виробничих і технологічних ресурсів для кібербезпеки, створення узгодженої міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС [3].

Аналіз тенденцій у політиці кібербезпеки ЄС указує на те, що розвиток цифрових технологій та інформаційних систем призвів до нових загроз для національної безпеки європейських країн. Сучасні інформаційні технології роблять інформаційні системи вразливими до кібератак, що потребує вжиття заходів для зменшення негативних наслідків цих загроз [Бірець; Запорожець, 2009].

Європейський Союз активно працює над удосконаленням своїх систем безпеки в кіберпросторі відповідно до сучасних викликів. Це включає впорядкування нормативно-правової бази, розробку європейських принципів стійкості інтернету, збільшення кількості підрозділів, що займаються кібербезпекою, зміцнення контролю над національним інформаційним простором і захист критичної інфраструктури. Також проводяться пан'європейські навчання та дослідження щодо інцидентів безпеки в мережі [4; 5].

Європейський Союз активно оновлює свої сектори безпеки в кіберпросторі відповідно до сучасних викликів. Цей процес уключає впорядкування нормативно-правової бази, що забезпечує цілісність державної політики в цій сфері; розробку європейських керівних принципів для забезпечення стійкості інтернету і їх просування на міжнародній арені; збільшення кількості підрозділів, залучених до системи кібербезпеки; посилення контролю за національним інформаційним простором; посилення захисних механізмів для критичної інформаційної інфраструктури ЄС; проведення загальноєвропейських навчань і досліджень із питань безпеки інцидентів в інтернеті; зміцнення співпраці між державним і приватним секторами; створення європейського форуму для обміну інформацією між країнами-членами; створення європейської системи раннього попередження про кіберзагрози тощо [1].

Для України важливо стати активним учасником цих процесів, адже це не лише покращить її міжнародний імідж, а й вплине на формування організаційно-правових основ національної кібербезпеки. В умовах гібридної війни питання кібербезпеки повинні бути в центрі державної політики. Стратегія зовнішньої політики України у сфері кібербезпеки має чітко визначати цілі та методи їх досягнення, щоб сприяти вигідному партнерству з ЄС у забезпеченні національних інтересів.

За рейтингом Online services Index, міжнародного дослідження E-Government Development Index, Україна посіла п'яте місце за рівнем розвитку цифрових державних послуг у світі (рис. 1). Рейтинг оцінює 193 країни та розробляється ООН. Його лідером стала Південна Корея, Данія – на другому місці, Естонія – третє. Водночас Україна опинилася на п'ятому місці після Саудівської Аравії. Віцепрем'єр-міністр з інновацій, розвитку освіти, науки й технологій, міністр цифрової трансформації України Михайло Федоров підкреслив, що у 2018 р. Україна в аналогічному дослідженні була на 102-му місці. Отже, держава за шість років піднялася на 97 позицій: «Першими прирівняли електронні документи до паперових і четвертими в Європі запустили цифрові водійські права. Реєстрація

ФОП в Україні – найшвидша в усьому світі, усього 4 секунди. Крім 5-го місця за рівнем розвитку цифрових послуг, ми на першому місці щодо залученості громадян до державних процесів через онлайн». Водночас він наголосив, що Дією користуються близько 21 млн українців [13].

Зважаючи на це, Україна потребує створення адекватної системи безпеки у світі, що трансформується, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз. Активність із боку провідних держав світу у кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах у кіберпросторі, – усе це обумовлює необхідність вироблення рекомендацій щодо коротко- й довгострокових пріоритетів трансформації вітчизняного безпекового сектору з урахуванням вищезазначених трендів [8].

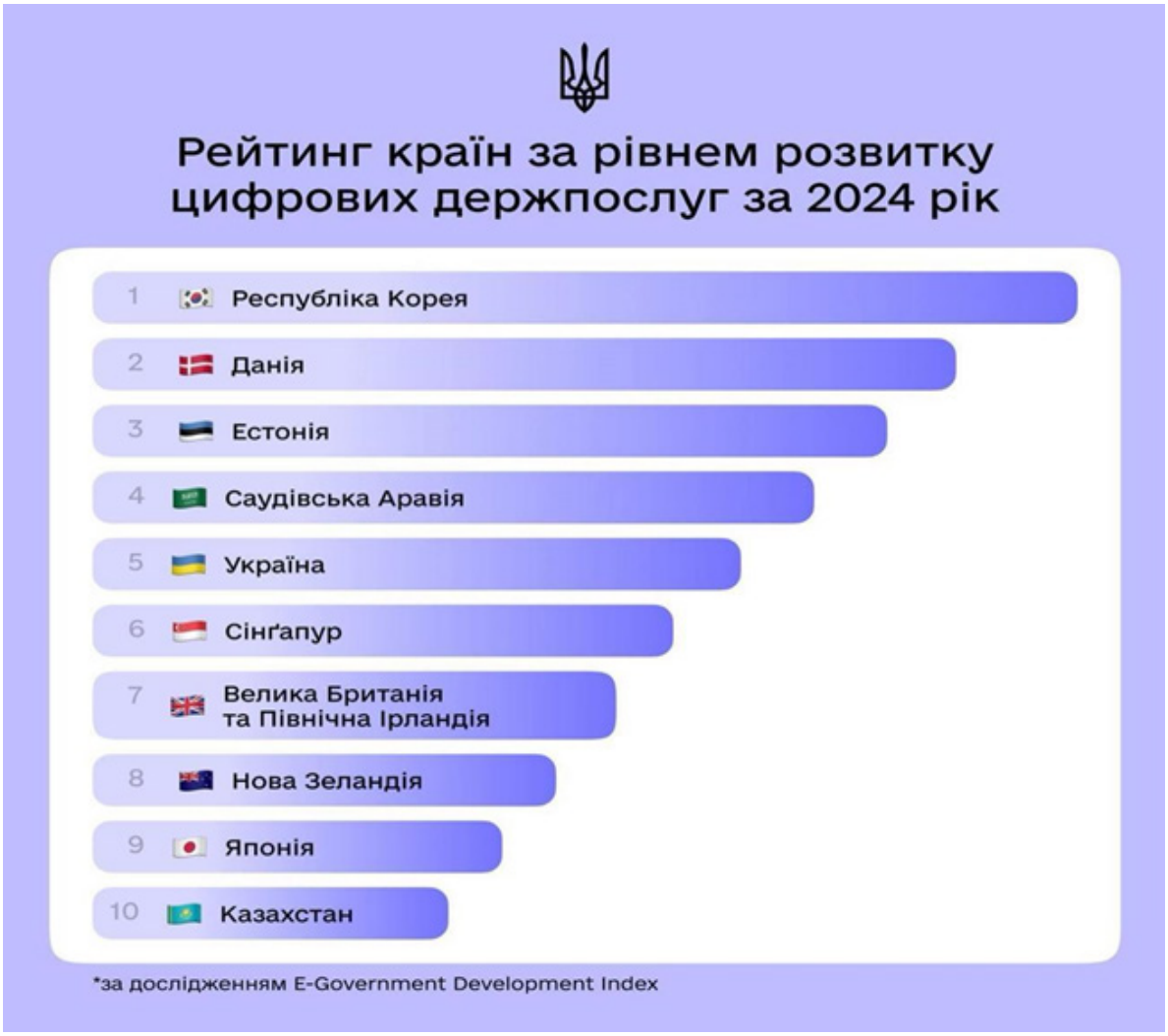

Рис. 1. *E-Government Development Index, 2024*

Із початком російської агресії у 2014 р. Україна зіткнулася з низкою потужних кібератак, що змусило державу переглянути свої підходи до кіберзахисту. Перший у світі зафіксований випадок успішної хакерської атаки на енергетичну інфраструктуру стався 23 грудня 2015 р. в Україні. Унаслідок цього виведено з ладу автоматизовані системи керування енергетичними підстанціями, що призвело до відключення електромереж на період від трьох до восьми годин. Про інцидент повідомили Київобленерго, Прикарпаттяобленерго та Чернівціобленерго [9].

Українська кіберполіція виявила понад 3600 кіберзлочинів у 2023 р., що на 59 % перевищує аналогічний показник у 2022 р. Цифровий простір відкриває безліч можливостей, але разом із цим вносить нові загрози та ризики. Для того щоб захистити себе в цьому світі, треба мати належне розуміння цифрової безпеки [12].

У країні створено нові структури, як-от: Національний координаційний центр кібербезпеки, а також посилено співпрацю з міжнародними організаціями, такими як НАТО та ЄС. У контексті кібербезпеки важливою є тісна взаємодія між державою й приватним сектором, адже багато критичних інфраструктур, зокрема банки, телекомунікації, енергетика, зосереджені в приватній власності. Урядові органи повинні забезпечити створення регуляторних рамок, що дають змогу компаніям ефективно захищати свої інформаційні ресурси, а також сприяти обміну інформацією про потенційні загрози. Приватний сектор відіграє ключову роль у розвитку нових технологій захисту й у впровадженні стандартів безпеки. Інвестиції в кібербезпеку дають змогу компаніям зменшити ризики кібератак, зберегти конфіденційність даних та захистити свою репутацію.

Реалізація національних стратегій кібербезпеки стикається з низкою викликів, як-от:

• недостатнє фінансування. У багатьох країнах інвестиції в кібербезпеку залишаються недостатніми, що ускладнює розвиток необхідної інфраструктури й підготовку фахівців;

• швидкість технологічного прогресу. Розвиток нових технологій, таких як штучний інтелект, квантові обчислення, а також інтернет-речей, створює нові загрози, до яких держави можуть бути не готові;

• проблема людського фактора. Навіть найсучасніші технології захисту можуть бути марними, якщо користувачі допускають помилки. Навчання та підвищення обізнаності серед державних службовців і громадян залишається критичним аспектом забезпечення кібербезпеки;

• міжнародне право та його відсутність. Наразі відсутні єдині міжнародні правові рамки для боротьби з кібератаками. Це ускладнює співпрацю між державами й створює лазівки для кіберзлочинців, які можуть діяти з території однієї країни, не зазнаючи переслідувань з боку іншої.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої й зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей і інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а інші нормативно-правові акти, що приймаються на виконання законів України. А також Закон України «Про основні засади забезпечення кібербезпеки України» [10], який визначає Національну систему кібербезпеки як сукупністю суб'єктів забезпечення кібербезпеки й взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Закон України «Про основні засади забезпечення кібербезпеки України» заклав загальну архітектуру національної системи кібербезпеки й розподіляє завдання та повноваження між основними суб'єктами забезпечення кібербезпеки (Національним координаційним центром кібербезпеки, Міністерством оборони, Генеральним штабом Збройних сил, Державною службою спеціального зв'язку та захисту інформації, Службою безпеки України, Національною поліцією, Національним банком, розвідувальними органами України) [10].

Важливим документом є також Стратегія кібербезпеки України, що затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» [17].

У відповідь на кіберзагрози Україна розробила Національну стратегію кібербезпеки, яка визначає пріоритети та заходи для посилення кіберзахисту. Основні елементи цієї стратегії включають:

• зміцнення нормативно-правової бази. Важливим кроком стало ухвалення Закону «Про основні засади забезпечення кібербезпеки

України», який визначає основні напрями діяльності держави у сфері кібербезпеки. Крім того, створено Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України;

• розвиток інституційної інфраструктури. Україна створює спеціалізовані підрозділи з кібербезпеки як на рівні військових структур, так і цивільних. Ці органи займаються моніторингом кіберзагроз, аналізом даних та розробкою оперативних заходів реагування на кібератаки;

• міжнародне співробітництво. Україна активно співпрацює з міжнародними партнерами, зокрема з ЄС і НАТО, у сфері обміну інформацією про кібератаки та розробки спільних механізмів кіберзахисту. Це співробітництво дає змогу Україні отримувати необхідні технології й експертизу для зміцнення власного кіберпростору;

• захист критичної інфраструктури. Україна посилює заходи для захисту критичних об'єктів інфраструктури, таких як енергетичні, транспортні та фінансові системи. Це включає як посилення фізичного захисту, так і впровадження сучасних технологій кіберзахисту;

• освітні програми й підготовка кадрів. Важливою складовою частиною стратегії є підготовка фахівців у галузі кібербезпеки. Українські університети розробляють спеціалізовані навчальні програми, що готують нове покоління кіберспеціалістів для державного та приватного секторів.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Кібербезпека є важливою складовою частиною сучасної міжнародної безпеки, оскільки кіберзагрози можуть мати глобальні наслідки. Ефективне розв'язання проблем кібербезпеки потребує міжнародної співпраці, гармонізації законодавства, розвитку нових технологій захисту й постійного вдосконалення стратегій. Держави та міжнародні організації повинні активізувати зусилля для створення безпечного й стабільного кіберпростору, який стане фундаментом глобальної безпеки. Національна стратегія безпеки України чітко визначає кібербезпеку як пріоритетний напрям у захисті держави. Кіберзагрози в Україні не є гіпотетичними – із 2014 р. країна стала об'єктом масштабних кібератак на ключові державні, військові та енергетичні об'єкти. Отже, кібербезпека для України є не лише питанням захисту інформаційної інфраструктури, але й безпеки життєво важливих галузей. Уряд України й міжнародні партнери активно працюють над створенням надійної системи кіберзахисту, яка забезпечить безпеку державних установ, економіки, громадян та критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. About ENISA / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa (дата звернення: 10.09.2024).

2. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (дата звернення 10.09.2024).

3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2017). URL://http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (дата звернення 10.09.2024)

4. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-singlemarket/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity (дата звернення 10.09.2024).

5. EU cybersecurity initiatives working towards a more secure online environment / European Union. URL: http://ec.europa.eu/information_society/newsroom/image/document/2017- 3/factsheet_cybersecurity_update_january_2017_41543.pdf (дата звернення 10.09.2024).

6. National Cyber Security Index. NCSI. URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 07.11.2023).

7. Бірець, К. Є. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. URL: 15739.pdf (vntu.edu.ua) (дата звернення: 10.09.2024).

8. Дубов, Д. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. Національний інститут стратегічних досліджень (НІСД). URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini (дата звернення: 10.09.2024).

9. Ємельянов, В. М., Бондар, Г. Л. (2019). Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Публічне управління та регіональний розвиток,* (5), 493–523. URL: https://doi.org/10.34132/pard2019.05.02 (дата звернення: 10.09.2024).

10. Закон України Про основні засади забезпечення кібербезпеки України. *Відомості Верховної Ради (ВВР),* 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

11. Запорожець, О. Ю. (2009). Політика Європейського Союзу в сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин,* вип. 87, ч. ІІ, с. 36–45.

12. Кібербезпека: Захист та безпека в цифровому світі, 18.04.2024. URL: https://filter.mkip.gov.ua/kiberbezpeka-zahyst-ta-bezpeka-v-czyfrovomu-sviti/

13. Куркіна, Д. Україна посіла 5 місце у світі за рівнем розвитку цифрових держпослуг. 20 верес., 2024. URL: https://espreso.tv/tekhnologiyi-ukraina-posila-5-mistse-u-sviti-za-rivnem-rozvitku-tsifrovikh-derzhposlug#:~:text=Про%20це%20повідомив%20віцепрем%27єр-міністр%20з%20інновацій%2C%20розвитку%20освіти%2C,Данія%20посіла%20друге%20місце%2C%20коли%20Естонія%20-%20третє.

14. Ліпкан, В. А., Ліпкан, О. С. (2018). Національна і міжнародна безпека у визначеннях та поняттях: навч. посіб. вид 2-ге, переробл. і доповн. Київ, 400 с.

15. Про основні засади забезпечення кібербезпеки України: Закон України №2163-VIII від 05.10.2017 р. *Відомості Верховної Ради (ВВР),* 2017, № 45, 403 с.

16. Сліпченко, Т. (2020). Кібербезпека як складова системи захисту національної безпеки: європейський досвід. *Актуальні проблеми правознавства,* 1 (21), с. 128–133.

17. Указ Президента України № 392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 26.11.2023).

REFERENCES

1. About ENISA / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa (дата звернення: 10.09.2024).

2. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (дата звернення: 10.09.2024).

3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2017). URL://http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (дата звернення: 10.09.2024)

4. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-singlemarket/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity (дата звернення: 10.09.2024).

5. EU cybersecurity initiatives working towards a more secure online environment / European Union. URL: http://ec.europa.eu/information_society/newsroom/image/document/2017- 3/factsheet_cybersecurity_update_january_2017_41543.pdf (дата звернення: 10.09.2024).

6. National Cyber Security Index. *NCSI.* URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 07.11.2023).

7. Birets, K. Ye. Kiberbezpeka yak vazhlyva skladova systemy zakhystu natsionalnoi bezpeky yevropeiskykh krain. URL: 15739.pdf (vntu.edu.ua) (data zvernennia: 10.09.2024).

8. Dubov, D. Suchasni trendy kiberbezpekovoi polityky: vysnovky dlia Ukrainy. Analitychna zapyska. *Natsionalnyi instytut stratehichnykh doslidzhen (NISD).* URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini (data zvernennia 10.09.2024).

9. Iemelianov, V. M., Bondar, H. L. (2019). Kiberbezpeka yak skladova natsionalnoi bezpeky ta kiberzakhyst krytychnoi infrastruktury Ukrainy. *Publichne upravlinnia ta rehionalnyi rozvytok,* (5), 493–523. URL: https://doi.org/10.34132/pard2019.05.02 (data zvernennia: 10.09.2024).

10. Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. *Vidomosti Verkhovnoi Rady (VVR),* 2017, № 45, st. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

11. Zaporozhets, O. Iu. (2009). Polityka Yevropeiskoho Soiuzu v sferi informatsiinoi bezpeky. *Aktualni problemy mizhnarodnykh vidnosyn,* vyp. 87, ch. II, p. 36–45.

12. Kiberbezpeka: Zakhyst ta bezpeka v tsyfrovomu sviti. 18.04.2024. URL: https://filter.mkip.gov.ua/kiberbezpeka-zahyst-ta-bezpeka-v-czyfrovomu-sviti/

13. Kurkina, D. (2024). Ukraina posila 5 mistse u sviti za rivnem rozvytku tsyfrovykh derzhposluh. 20 veresnia. URL: https://espreso.tv/tekhnologiyi-ukraina-posila-5-mistse-u-sviti-za-rivnem-rozvitku-tsifrovikh-derzhposlug#:~:text=Pro%20tse%20povidomyv%20vitseprem%27ier-ministr%20z%20innovatsii%2C%20rozvytku%20osvity%2C,Daniia%20posila%20druhe%20mistse%2C%20koly%20Estoniia%20-%20tretie.

14. Lipkan, V. A., Lipkan, O. S. (2018). Natsionalna i mizhnarodna bezpeka u vyznachenniakh ta poniattiakh: navch. posib., vyd 2-he, pererobl. i dopovn. Kyiv, 400 p.

15. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy №2163-VIII vid 05.10.2017 r. *Vidomosti Verkhovnoi Rady (VVR),* 2017, № 45, 403 p.

16. Slipchenko, T. (2020). Kiberbezpeka yak skladova systemy zakhystu natsionalnoi bezpeky: yevropeiskyi dosvid. *Aktualni problemy pravoznavstva,* 1 (21), p. 128–133.

17. Ukaz Prezydenta Ukrainy №392/2020 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy». URL: https://www.president.gov.ua/documents/3922020-35037 (data zvernennia: 26.11.2023).

Матеріал надійшов до редакції 11.09.2024 р.

УДК 327.01-049.5

Анастасія Присташ,
ад'юнкт Військового інституту,
Київський національний університет імені Тараса Шевченка,
pristashnastasiya@knu.ua,
ORCID ID: 0009-0000-5534-3578
DOI 10.29038/2524-2679-2024-03-34-45

НАУКОВІ ПІДХОДИ ДО ТРАКТУВАННЯ ПОНЯТТЯ «МІЖНАРОДНА БЕЗПЕКА»

Сьогодні система міжнародної безпеки як складова частина багатокомпонентної світової політики переживає значні зміни з огляду на наростання як регіонального протистояння, так і динамічне зростання глобальних проблем.