УДК 342.951

АРПЕНТІЙ С.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0000-0003-3326-3942

СТРАТЕГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ США

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334229

Анотація. *У статті аналізується розвиток та формування стратегічних засад забезпечення кібербезпеки США. Висвітлюються основні пріоритети національних стратегій забезпечення кібербезпеки. Еволюція формування стратегій забезпечення кібербезпеки США свідчить про застосування нового комплексного підходу, зміст якого полягає у інтегрованому стримуванні агресії у кіберпросторі. Міститься аналіз нової Стратегії кібербезпеки США 2023 року, положення якої передбачають покращення співпраці між федеральним урядом та приватним сектором, а також поліпшення стандартів виправлення вразливостей у комп'ютерних системах. Констатовано, що складність зростаючих кіберзагроз, які посилені розвитком штучного інтелекту, спонукають федеральні органи США вживати більш дієвих заходів захисту комп'ютерних систем. Звертається увага, що посилення кіберзагроз змушує федеральний уряд США збільшувати бюджет на кібербезпеку, стимулювати інвестиції в дослідження штучного інтелекту для ефективного запобігання кібератакам.*

Ключові слова: *кібербезпека, кіберзагрози, стратегії забезпечення кібербезпеки, США, федеральний уряд.*

Summary. *The article analyzes the development of the formation of US cybersecurity strategies. It highlights the main priorities of national cybersecurity strategies. The evolution of the formation of US cybersecurity demonstrates the use of a new comprehensive approach, the content of which is integrated cyber deterrence of aggression in cyberspace. It contains an analysis of the new Cybersecurity Strategy of 2023, the provisions of which provide for improved cooperation between the government and the private sector, as well as improved standards for fixing vulnerabilities in computer systems. It is stated that the complexity of growing cyber threats, which are enhanced by the development of artificial intelligence, is prompting US federal agencies to take more effective measures to protect computer systems. It is noted that the increase in cyber threats is forcing the US federal government to increase the budget for cybersecurity and stimulate investments in artificial intelligence research to effectively prevent cyber attacks.*

Keywords*: cybersecurity, cybersecurity strategies, USA, federal government.*

Постановка проблеми. Захист від кіберзагроз стає дедалі більш стратегічною проблемою для всіх держав світу. XXI ст. знаменується активним формуванням кіберпростору, застосуванням сучасних інформаційних технологій, які несуть додаткові кіберризики. Кіберпростір залишається найважливішою сферою державних інтересів США. У Стратегії забезпечення кібербезпеки України зазначається: "Питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься" [1]. Водночас, прогнозується зростання інтенсивності протиборства Китаю та США і розвідувально-підривної діяльності у кіберпросторі.

Однією з цілей Стратегії забезпечення кібербезпеки України є використання кращих практик з питань кібербезпеки Сполучених Штатів Америки, налагодження з

цією країною систематичного обміну інформацією про деструктивну діяльність у кіберпросторі [1].

Результати аналізу наукових публікацій. Еволюцію формування стратегій забезпечення кібербезпеки США досліджували такі фахівці, як: Ю. Геращенко [2], Н. Литвиненко [3], С. Стежко, Т. Шевченко[4], В. Шемчук [5] та інші.

Проте залишається недостатньо дослідженим досвід формування останніх законодавчих ініціатив, направлених на посилення стану кібербезпеки в США, що зумовлює актуальність цієї наукової статті. Крім цього, війна в Україні підкреслила важливість кіберпростору як театру воєнних дій для США та її союзників.

Метою статті є аналіз та узагальнення законодавчого досвіду США у сфері розроблення стратегій забезпечення кібербезпеки для його врахування та використання на національному рівні.

Виклад основного матеріалу.

Захист кіберпростору завжди був у центрі уваги американського істеблішменту.

Ще у 2003 році була прийнята Національна стратегія кібербезпеки США (The National Strategy to Secure Cyberspase), у якій було виділено такі пріоритети: запобігання кібератакам; мінімізація наслідків; імплементація національної безпеки в національний кіберпростір, зменшення загроз національному кіберпростору; посилення національної поінформованості щодо кіберпростору; захист урядового кіберпростору; посилення міжнародної безпеки і кооперації у сфері кіберпростору [6].

У травні 2011 р у США було оприлюднено документ під назвою “Міжнародна стратегія кіберпростору” (International Strategy For Cyberspace), в якому зазначалося, що мета цієї Стратегії – уможливити, щоб глобальне кіберсередовище стало більш відкритим, інтероперабельним, безпечним і надійним. У цьому акті визначено вісім пріоритетів, серед яких виділено: розвиток національної інформаційної інфраструктури; розвиток національної економіки; захист інформаційно-комунікаційних мереж; посилення військового компонента; модернізація законодавства в інформаційній сфері; розвиток міжнародного співробітництва; створення ефективної структури для керування Інтернетом; забезпечення фундаментальних принципів і свобод в Інтернеті [7]. Також в цьому документі згадується важлива ідея кіберстримування щодо потенційних супротивників (це можуть бути держави, недержавні структури, терористичні угруповання).

У вересні 2018 року була оприлюднена чергова Стратегія з кібербезпеки США [8], яка декларувала наступальний характер держави у глобальному кіберпросторі, а її кінцевою метою визначено налагодження дієвого кіберзахисту, запобігання поширенню ризиків, пов’язаних із кібербезпекою, забезпечення безпеки національних інформаційних систем та мереж [5, с. 141]. Відповідно до цієї Стратегії кібербезпека – це комплекс заходів, спрямованих на захист комп’ютерних систем (включаючи апаратні засоби, програмне забезпечення (далі ПЗ) та дані) від несанкціонованого доступу або атак через мережу Інтернет[8]. Серед головних пріоритетів Стратегії називалися: захист держави та приватних даних її громадян від іноземних хакерів та спецслужб іноземних держав, передусім КНР, РФ, Ірану, Північної Кореї; розробка міжнародної Інтернет-політики і комплектування державних структур та відомств компетентними співробітниками, які мають досвід роботи в ІТ-сфері та розуміються в питаннях кібербезпеки; підвищення рівня захисту урядових структур; посилення покарань за кіберзлочини. При цьому Китай та Росію було визнано основними загрозами у кіберпросторі [5, с. 141].

12 жовтня 2022 р. Адміністрація США представила оновлену Стратегію національної безпеки США (National Security Strategy of The United States of America), у якій акцентується увага на двох фундаментальних стратегічних викликах: конкуренції між великими державами за формування майбутнього міжнародного порядку й транснаціональних спільних загрозах (shared threats) – це, зокрема, зміна клімату, загроза продовольчій безпеці, інфекційні захворювання, тероризм, дефіцит енергії, інфляція тощо [9].

Окрема увага в цій Стратегії приділяється модернізації і зміцненню оборонного потенціалу США. З цього приводу В. Орлик і А. Гриценко пишуть: "Для реалізації максимального ефективного стримування агресії пропонується новий комплексний підхід – інтегроване стримування (integrated deterrence). Війна в Україні підкреслила критичність потужної оборонно-промислової бази США і для самої держави, і для союзників та партнерів; посилила аргументи щодо необхідності швидкого запровадження передових технологій у кібернетичній та космічній галузях, розробках у сферах штучного інтелекту і квантових систем, які необхідно здійснювати з метою подальшого збереження військово-технологічної переваги" [9].

У березні 2022 р. Адміністрацією США було презентовано нову Стратегію національної безпеки США, де було визначено основних суперників США: КНР як єдину державу, що має потенціал до змін міжнародного порядку, та росію, яка є безпосередньою загрозою для вільної та відкритої міжнародної системи. Підкреслювалося, що КНР і РФ дедалі зближуються, проте виклики з боку кожної з цих країн різняться. Пріоритетом США залишається утримання стійкої конкурентної переваги над Китаєм з одночасним стримуванням "усе ще глибоко небезпечної" (still profoundly dangerous) Росії [10].

Кіберзахист критичної інфраструктури визначено одним з п'яти принципів цієї Стратегії поряд з ліквідацією загроз та формуванням ринкових сил, що гарантують безпеку [11].

У березні 2023 року в США представлено нову Стратегію кібербезпеки, яка: закликає до більш жорсткого регулювання існуючих практик кібербезпеки в різних галузях; пропонує створення іноземних коаліцій щоб чинити тиск на росію та Китай; передбачає покращення співпраці між урядом та приватним сектором; планує покращення стандартів виправлення вразливостей у комп'ютерних системах[12]. Ця Стратегія передбачає внесення фундаментальних змін в основу динаміки цифрової екосистеми, надавши перевагу захисту і протидії кіберзагрозам. Головна мета цієї Стратегії — це надійна, стійка цифрова екосистема, де конфіденційна чи приватна інформація буде повністю убезпечена та захищена [13]. На думку Адміністрації президента США Дж. Байдена, викорінення неправомірної поведінки в кіберпросторі вимагатиме співпраці та координації урядів багатьох країн світу. З метою реалізації цієї Стратегії планується: використання всіх доступних інструментів для протидії кіберзагрозам; активізація міжнародної співпраці з країнами, які раніше не брали участі в цьому питанні [13].

Відповідно до нової Стратегії кібербезпеки, США розширює коло партнерів по всьому світу, одночасно з цим шукаючи нові способи безпечно обмінюватись інформацією з найбільш довіреними партнерами. Так, у 2024 році було укладено цілу низку міжнародних угод про партнерство: між ENISA та CISA, формування нового партнерства між США, Південною Кореєю та Японією. Одночасно Офіс національного кібердиректора США (ONCD) активно просуває імплементацію Національної стратегії

кіберосвіти та робочої сили, прийнятої ще влітку 2023 року, проводячи дискусії з учасниками ринку[14].

На початку травня 2024 року Державний департамент США оприлюднив Стратегію міжнародного кіберпростору та цифрової політики, для того щоб стримати цифровий вплив росії та Китаю в країнах, що розвиваються, і зробити ймовірні спроби цих країн втручатися у вибори менш ефективними[15]. Ця Стратегія прагне залучити більше країн, що розвиваються, до "позитивного бачення" кіберпростору, яке відкидає цифрові репресії. В її рамках США продовжать багаторічне лобіювання серед союзників і партнерів, щоб вони не використовували ключові комунікаційні технології та програмне забезпечення, створене в автократичних країнах, таких як росія та Китай. Загалом, її можна схарактеризувати як намагання США створити коаліцію проти Китаю. Огляд подій в сфері кібербезпеки свідчить про те, що США входить в період проведення оцінок ефективності виконання стратегічних доручень Президента США у сфері кібербезпеки. Так, Управління звітності уряду Сполучених Штатів оприлюднило результати оцінки урядовими структурами Указу Президента США 14028 "Покращення кібербезпеки країни" – 49 з 55 задач (90%) були виконані. Крім того, було ухвалено оновлений План реалізації Національної стратегії кібербезпеки – до плану було додано 31 нову задачу. Одночасно з цим Офіс національного кібердиректора (ONCD) провів оцінку ефективності виконання першого Плану імплементації – було реалізовано близько 90% задач (33 з 36 запланованих ініціатив) [15]. Слід відзначити, що уряд США помітно посилив контроль за процесами виконання ухвалених ним стратегічних рішень, зробивши процедури оцінки більш регулярними та публічними.

У відповідь на низку масштабних хакерських атак, пов'язаних із Китаєм, у завершальні дні каденції президента США Дж. Байдена був опублікований Указ, який посилює стандарти кібербезпеки для федеральних агентств і підрядників, а також передбачає впровадження стандартів безпечного розроблення ПЗ. Зокрема, цей Указ передбачає: впровадження жорсткіших стандартів безпечного розроблення програмного забезпечення; можливість перевірки відповідності цим стандартам; процедуру оцінки процесу, яку проводитиме Агентство з кібербезпеки та безпеки інфраструктури США (CISA) [16].

Починаючи з 2005 року розвідувальна спільнота США публікує щорічний звіт "Annual Threat Assessment of the U.S. Intelligence Community", де міститься детальний аналіз основних загроз національній безпеці країни для того, щоб попередити уряд США, військових, а також світову спільноту як про ті небезпеки, що вже існують, так і ті, які можуть виникнути в найближчому майбутньому. Звіт, який був представлений 25-26 березня 2025 року, озвучив загрози національній безпеці США і висвітлив перелік країн, які несуть ці загрози. Серед десяти головних загроз національній безпеці США в Звіті виділяється: 1) тероризм як з боку ісламських екстремістських груп, так з боку правих екстремістів; 2) поширення зброї масового знищення; 3) конкуренція великих держав (Great Power Competition); 4) зміни клімату; 5) кризові міграційні потоки; 6) кібернетична війна та кібернапади; 7) кримінальна діяльність та транснаціональні загрози; 8) інформаційні війни та психологічні операції; 9) геополітична нестабільність та військові конфлікти; 10) технологічні загрози, включаючи штучний інтелект (далі ШІ) та застосунки з продажу інтернет-речей (IoT) [17] з урахуванням вразливості пристроїв IoT до атак і можливість їх використання для масових кібернападів.

Взагалі розвиток штучного інтелекту та його вплив на сферу кібербезпеки все частіше у фокусі уваги кібербезпекових організацій та правоохоронних органів США. Наприклад, ШІ дедалі частіше стає і предметом кібершпигунства – у травні 2024 року

невизначена APT група атакувала американських дослідників ШІ, намагаючись отримати доступ до їх даних. Моделюючи різні ситуації у кіберпросторі, кібербезпековим фахівцям з Unit42 вдалось навчити ШІ створювати дієве зловмисне ПЗ, користуючись релевантною базою вихідних даних – створене ШІ ПЗ не лише виявилось ефективним, але ШІ може оперативно модифікувати його, створювати численні варіації ядра шкідливого ПЗ та адаптувати його для різних платформ [15].

За аналізом інтернет-порталу Defense News, зростаюча складність військових мереж і цифрові "прориви" інших світових держав роблять штучний інтелект і пов'язані з ним комп'ютерні програми більш бажаними для США [18]. З вибуховим ривком високотехнологічних пристроїв, а також великою кількістю даних, які вони передають, постають додаткові вимоги щодо національної безпеки та швидкості реагування на імовірні загрози. Представники оборонного відомства США встановили кінцевий термін до 2027 року для впровадження рівня нульової довіри, який загалом налічує понад 100 різних заходів. Насамперед, ця так звана нульова довіра полягає в перегляді існуючих даних. І справа не лише в людині, яка входить у систему як особа і елемент даних, — справді потрібно дістатися до місця пошуку аномальних даних, які виникають у різних аспектах мережі, щоб набагато швидше визначити, де є слабке місце. Адже сучасні літаки, системи зброї, інші технічні засоби — усі вони генерують критичні дані та інформацію, що складає величезний масив, котрий постійно повинен бути надійно захищеним від стороннього втручання [18]. Однак, людський фактор залишається одним з ключових джерел кіберзагроз для організацій та їх інформаційних систем, про що свідчать останні дослідження Verizon та Proofpoint. Так, респонденти опитування Verizon вказали на те, що 68% порушень безпеки сталися через не зловмисний людський фактор – тобто інциденти пов'язані з інсайдерськими помилками або людьми, які потрапили на схеми соціальної інженерії [15].

Як зазначають експерти з кібербезпеки, складність і частота зростаючих кіберзагроз, які посилені ШІ, спонукають організації в усьому світі вживати більш дієвих заходів захисту. Очікується, що витрати на безпеку будуть стійко зростати найближчим часом і досягнуть $377 млрд у 2028 році. На США і Західну Європу, як і раніше, припадатиме понад 70% світових витрат на безпеку у 2025 році [19].

В даному контексті Федеральний бюджет США на 2025 рік передбачає виділення 27,5 млрд доларів на кібербезпеку, що відображає стратегічне зосередження на захисті кіберпростору [20].

Водночас, нова адміністрація президента США Д. Трампа змістила акценти у забезпеченні кібербезпеки США, призупинивши проведення та планування наступальних кібероперацій проти Росії [21]. Крім цього, у Палаті представників США знову зареєстрували законопроєкт, який передбачає введення санкцій проти китайських компаній, що фінансово підтримують військову агресію росії в Україні. У проекті йдеться про: введення санкцій проти китайських компаній, які допомагають російському військово-промисловому комплексу; обмеження для компаній, пов'язаних із кібератаками та військовою модернізацією; розширення поняття дочірні компанії, щоб охопити іноземні філії китайських компаній і російські фірми, які намагаються обійти санкції; введення санкцій проти китайських організацій, які продають зброю в інші країни [22].

Аналіз подій у сфері кіберпростору свідчить про посилення протиборства США та Китаю.

Висновки.

Досвід США у розробленні стратегій забезпечення кібербезпеки є вельми важливим та корисним для України в контексті формування стратегічних ініціатив у цій сфері. Досвід США у цій площині переконливо демонструє, що в сучасному світі кіберпростір стає ареною як наступальних, так і оборонних операцій, вимагає концентрації зусиль військового та цивільного секторів у фокусі цієї проблеми, що є наслідком чіткого визначення супротивників та союзників [6, с.144]. Огляд національних стратегій забезпечення кібербезпеки США свідчить про те, що урядовий контроль за процесами виконання ухвалених в США стратегічних рішень у сфері кібербезпеки стає більш дієвим та ефективним. В межах національних стратегій забезпечення кібербезпеки простежується нарощування фінансових і матеріальних ресурсів, які були би здатні протидіяти ворожим кібератакам. Важливим стратегічним напрямком залишається міжнародна співпраця у сфері кібербезпеки. Посилення кіберзагроз змушує федеральний уряд США збільшувати бюджет на кібербезпеку, стимулювати інвестиції в дослідження ШІ для запобігання кібератакам. Одним з ключових джерел кіберзагроз залишається людський фактор, зміст якого охоплює кіберінциденти, пов’язані з помилками людини.

Використана література

1. Стратегія кібербезпеки України: затв. Указом Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. Геращенко Ю.В. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: “Державне управління”.* 2019. Т. 30 (69). С. 140-145.

3. Литвиненко Н.П., Погоріла Н.О. Концептуальне забезпечення політики глобального лідерства США постбіполярної доби. *Актуальні проблеми міжнародних відносин.* 2017. Вип. 132. С. 44-51.

4. Шемчук В.В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник академії МВС України*. 2019. Том 24. №4. С. 119-124.

5. Стежко С., Шевченко Т. Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформація і право.* 2021. № 2(37). С. 139-144. URL:https://ippi.org.ua/sites/default/files/18_11.pdf.

6. The White House, The National Strategy to Secure Cyberspace, February 2003. Unclassified. URL: https://nsarchive.gwu.edu/document/21412-document-16.

7. INTER NATIONA L STR ATEGY FOR CYBERSPACE URL:https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

8. National Cyber Strategy of the United States of America. (2018). (n.d.). URL: https://www. whitehouse.gov/wp - content/uploads/2018/09/National - Cyber-Strategy.pdf.

9. Орлик В., Гриценко А.. Основні положення нової Стратегії національної безпеки США. URL: https://niss.gov.ua/sites/default/files/2022-10/171022_us_nss_pdf.pdf.

10. Білий дім оприлюднив нову національну стратегію кібербезпеки. URL: https://lb.ua/world/2023/03/03/547727_biliy_dim_oprilyudniv_novu.html.

11. У США оприлюднили нову стратегію кібербезпеки. URL: korrespondent.net/world/4567836-u-ssha-opryluidnyly-novu-stratehiui-kiberbezpeky.

12. США представили нову стратегію кібербезпеки на тлі зростання хакерских атак, головними загрозами вважають Китай і Росію. URL: https://forbes.ua/news/ssha-predstavili-novu-strategiyu-kiberbezpeki-na-tli-zrostannya-khakerskikh-atak-golovnimi-zagrozami-vvazhayut-kitay-i-rosiyu-02032023-12093.

13. Нова стратегія кібербезпеки США: головні напрямки. URL: https://armyinform.com.ua/2023/03/07/nova-strategiya-kiberbezpeky-ssha-golovni-napryamky.

14. Річний аналітичний огляд. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf?fbclid=IwY2xjawI-fZRleHRuA2FlbQIxMAABHcaZdkgcVIlSJ0eGnBO78x5xRCDcoBwcJ1GKrT4SAVS5reEAtY5u8ssd4w_aem_0xN1oMO3-toIy6vpuA27mA.

15. Огляд подій в сфері кібербезпеки. травень 2024. URL:https://ufss.com.ua/news/ohliad-podiy-v-sferi-kiberbezpeky-traven-2024.html.

16. Байден посилює кібербезпеку США на тлі загроз з боку Китаю. URL: https://ms.detector.media/trendi/post/37194/2025-01-11-bayden-posylyuie-kiberbezpeku-ssha-na-tli-zagroz-z-boku-kytayu/

17. Розвідка США визначила три виклики майбутнього: геополітична нестабільність, зміна клімату та кіберзагрози. URL: https://www.ukrinform.ua/rubric-world/3975076-rozvidka-ssa-viznacila-tri-vikliki-majbutnogo-geopoliticna-nestabilnist-zmina-klimatu-ta-kiberzagrozi.html.

18. Кіберпростір та штучний інтелект — США посилюють захист у цифровому просторі. URL:https://armyinform.com.ua/2023/05/13/kiberprostir-ta-shtuchnyj-intelekt-ssha-posylyuyut-zahyst-u-czyfrovomu-prostori/

19. Світові витрати на кібербезпеку у 2025 році зростуть на 12,2% – IDC URL:https://www.fixygen.ua/news/20250321/svitovi-vitrati-na-kiberbezpeku-u-2025-rotsi-zrostut-na-122-idc.html.

20. Федеральний бюджет США виділяє 27,5 млрд доларів на кібербезпеку URL:https://hackyourmom.com/novyny/federalnyj-byudzhet-ssha-vydilyaye-275-mlrd-dolariv-na-kiberbezopasnist/.

21. Сполучені Штати призупинили проведення та планування наступальних кібероперацій проти Росії. URL: https://www.ukrinform.ua/rubric-world/3966290-ssa-prizupinili-kiberoperacii-proti-rosii-cnn.html.

22. У США зареєстрували законопроєкт про санкції проти компаній КНР. URL: https://fakty.com.ua/ua/svit/20250418-u-kongresi-ssha-zareyestruvaly-zakonoproyekt-pro-sankcziyi-proty-kompanij-kytayu-za-dopomogu-rf/.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~