УДК 342.951

СТЕЖКО С.М., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-0696-2131.
ШЕВЧЕНКО Т.О., молодший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-5849-5566.

СУЧАСНИЙ ДОСВІД США У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *Розглянуто зміст та ключові аспекти Стратегії кібербезпеки США. Визначено засади державної кібербезпекової політики США. Окреслено типові загрози для США у кіберпросторі. Узагальнено державні пріоритети щодо посилення складових кіберзахисту в США. Деталізовано питання фінансування кібербезпеки у США в 2021 році. Конкретизовано засади спільної діяльності американо-українських відносин у сфері забезпечення кібербезпеки. Визначено перелік заходів, які впроваджуються в США з метою посилення спроможностей держави у сфері забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кібератака, кіберзахист, стратегічні засади кібербезпеки, кіберпростір, фінансування, США.*

Summary*. The content and key aspects of the US Cyber Security Strategy are considered. The principles of the state cyber security policy of the USA are defined. Typical threats to the United States in cyberspace are outlined. The state priorities for strengthening the components of cyber defense in the United States are summarized. The issue of financing cyber security in the United States in 2021 is detailed. The principles of joint activities of American-Ukrainian relations in the field of cyber security are specified. The list of measures implemented in the United States to strengthen the state's capabilities in the field of cyber security has been identified.*

Keywords: *cyber security, cyber attack, cyber defense, strategic principles of cyber security, cyberspace, financing, USA.*

Аннотация. *Рассмотрены содержание и ключевые аспекты Стратегии кибербезопасности США. Определены основы государственной политики кибербезопасности США. Очерчены типичные угрозы для США в киберпространстве. Обобщены государственные приоритеты касаемо усиления составляющих киберзащиты в США. Детализированы вопросы финансирования кибербезопасности в США в 2021 году. Конкретизированы основы совместной деятельности американо-украинских отношений в сфере обеспечения кибербезопасности. Определен перечень мероприятий, которые внедряются в США с целью усиления возможностей государства в сфере обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, кибератака, киберзащита, стратегические основы кибербезопасности, киберпространство, финансирование, США.*

Постановка проблеми. У XXI столітті держава, суспільство та бізнес перейшли у нове середовище існування під назвою Інтернет, а інформаційно-комунікаційні технології стали основою для усіх сучасних інноваційних управлінських систем. Інтернет та цифрові інформаційно-комунікаційні технології дедалі більш інтегруються у всі сфери життєдіяльності держави та суспільства. За таких умов одним з основних завдань політичного керівництва будь-якої держави є забезпечення гарантованого функціонування

відкритого, надійного та захищеного кіберпростору. Відсутність кордонів у кіберпросторі, а також закладена в основі сучасних Інтернет-технологій відкритість та анонімність сприяють значному зростанню кількості зовнішніх кібератак та кіберзагроз, що автоматично призводить до необхідності розробки чіткої стратегічної концепції як ідейної основи формування пріоритетних засад національної політики у кіберпросторі. Тому останнім часом колосального масштабу у світі набула проблема захисту кіберпростору та елементів системи стратегічних комунікацій сектору безпеки і оборони від загроз несанкціонованого втручання.

Практично безмежні можливості використання Інтернету підкреслюють глобальну загрозу віртуальних кримінальних правопорушень, кібертероризму та кібервійни. Анонімність глобальних інформаційних мереж, швидкість передачі інформації та простота їх використання одночасно дозволяють використовувати всі ці переваги для здійснення протиправних діянь. Інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть реагувати на це. Адже загроза кібератак, особливо таких, що керуються чи фінансуються державами та застосовуються як інструмент примусу своїх політичних супротивників, є серйозним викликом і вимагають негайного адекватного реагування.

Реалії сучасності переконливо доводять, що важливою складовою національної безпеки виступає саме кібербезпека держави. Агресія з боку РФ проти України відбувається одночасно у багатьох площинах – військовій, політичній, інформаційній тощо, що вимагає від нашої країни комплексних дій у відповідь. Саме в умовах агресивної експансійної інформаційної політики РФ, динамічних змін у зовнішньому та внутрішньому безпековому середовищі України, посилення світових тенденцій щодо мілітаризації кіберпростору, його використання розвідувальними та спеціальними військовими структурами, хакерами та кібертерористами важливим та своєчасним завданням української держави є розбудова національної системи кібербезпеки. Тому в період сучасного глобального протистояння у сфері цифрових технологій та гонки озброєння у кіберпросторі безумовним лідером залишається США. Сфера кібербезпеки не є виключенням. Базовий ландшафт інструментарію реалізації окреслених кіберзагроз характеризується зростанням її високотехнологічної складової . Враховуючи викладене, актуальним та своєчасним є визначення стратегічних засад кібербезпеки США, а також напрямків двосторонньої співпраці між Україною та США у сфері забезпечення кібербезпеки.

Результати аналізу наукових публікацій. Питання стратегічного забезпечення кібербезпеки у США певним чином досліджували у своїх працях такі фахівці, як: Ю. Геращенко [1], Н. Литвиненко [2], В. Шемчук [3], та інші. Проте розгляд останніх законодавчих ініціатив, направлених на посилення стану кібербезпеки в США, та висвітлення здобутків у рамках партнерства у цій площині між Америкою та Україною жоден із фахівців детально не розглядав, що посилює тематичну спрямованість цієї наукової статті.

Метою статті є узагальнення здобутків США у сфері забезпечення кібербезпеки, визначення сучасних засад побудови конструктивного діалогу між Україною та США у кібербезпекових питаннях.

Виклад основного матеріалу. 20 вересня 2018 року Міністерство оборони США оприлюднило Стратегію з кібербезпеки адміністрації Президента Д. Трампа [4]. Сучасний документ має значно спростити процес узгодження кібербезпекових питань між силовими й оборонними відомствами цієї країни. У стратегічних положеннях задекларовано, що американці стають більш залежними від сучасних цифрових

технологій, більш вразливими до таких загроз, як: корпоративні порушення безпеки, фішинг та шахрайство в соціальних мережах, кібератаки тощо. Додаткові можливості кібербезпеки і правозастосування мають вирішальне значення для забезпечення захисту у кіберпросторі. У Стратегії кібербезпеки США викладені нові інструкції щодо дотримання безпеки в кіберпросторі для усіх федеральних відомств. Крім того, положення стратегії декларують наступальний характер США у глобальному кіберпросторі. У її положеннях викладені пріоритети уряду США щодо захисту держави та приватних даних її громадян від іноземних хакерів та спецслужб іноземних держав, передусім КНР, РФ, Ірану, Північної Кореї. За логікою документа, США матимуть більше свободи у протидії кібератакам і здійсненні наступальних кібероперацій. У стратегії деталізується ціла низка пріоритетних напрямів забезпечення політики кібербезпеки США. Серед таких пріоритетів – розробка міжнародної Інтернет-політики і комплектування державних структур та відомств компетентними співробітниками, які мають досвід роботи в ІТ-сфері та розуміються в питаннях кібербезпеки. Кінцевою метою цієї стратегії визначено налагодження дієвого кіберзахисту, запобігання поширенню ризиків, пов'язаних із кібербезпекою, забезпечення безпеки національних інформаційних систем та мереж.

Відповідно до базових положень Стратегії кібербезпеки США [4] кібербезпека – це комплекс заходів, спрямованих на захист комп'ютерних систем (включаючи апаратні засоби, програмне забезпечення та дані) від несанкціонованого доступу або атак через мережу Інтернет. Відповідно до положень цього документа Міноборони США визнало Китай та Росію основними загрозами у кіберпросторі. У документі йдеться про те, що загрозливі дії з боку КНР у кіберпросторі, зокрема викрадення конфіденційної інформації, розмивають військове панування та економічну безпеку США у глобальному вимірі. РФ, на думку авторів стратегії, проводить інформаційні операції, щоб маніпулювати свідомістю, посягаючи на демократичні цінності та права людини в мережі Інтернет. Щоб протидіяти РФ, Ірану, Китаю і КНДР у кіберпросторі, США планує збільшити свій наступальний потенціал, а у разі війни – "боротися з супротивником за допомогою повітряних, сухопутних, морських і космічних сил". Стратегія також передбачає регулювання ринку систем і засобів захисту інформації, зокрема уніфікацію устаткування та відбір дистриб'юторів. Документ закріплює право вимагати фінансового відшкодування від виконавців та організаторів проведення кібератак.

Адміністрація США докладатиме всіх зусиль щодо екстрадиції обвинувачених у хакерстві іноземних громадян, а також посилить для них покарання за скоєні кіберзлочини. Аналіз положень зазначеної стратегії дає змогу констатувати, що з метою підвищення рівня захищеності урядові структури будуть передавати в режимі онлайн виробникам мережевого обладнання інформацію щодо ймовірних ризиків та загроз. Вірогідно, що після цього компанії виготовлятимуть дві версії устаткування: для США і для решти країн світу. Отже, російські, китайські чи іранські обчислювальні системи, що використовують американське мережеве обладнання, вже не зможуть стримувати деякі комп'ютерні атаки. Найбільш вразливими у контексті гарантування кібербезпеки в США залишаються космічна і транспортна галузі, зокрема морські вантажні перевезення, особливо – газу і нафтопродуктів. Щоб зберегти кіберпростір в якості рушійної сили динамічної цифрової економіки, США взаємодіють з іноземними партнерами та іншими групами зацікавлених сторін, включаючи громадянське суспільство і приватний сектор, для просування передового досвіду і політики, які сприяють інноваціям, відкритості та ефективності. Серед запроваджених новацій стратегії США – розробка міжнародної політики кіберстримування; спрощення

регламентних правил, що регулюють наступальні операції в мережі; масштабніші наслідки від операцій для держав-супротивників, якщо вони відбуватимуться у складі коаліції; здійснення наступальних кібер- та військових дій США в рамках реагування на кібератаку. Сучасна стратегія кібербезпеки є першим за 15 років чітко сформульованим документом США у цій сфері. Як свого часу заявив радник президента США з національної безпеки Джон Болтон, нова стратегія "розв'язує руки" в тому числі, для проведення "наступальних" операцій у відповідь на кібератаки, а не тільки для пасивної оборони від кіберзагроз. Головними джерелами кіберзагроз для США все ще залишаються Китай, Іран, Північна Корея і Росія.

Враховуючи важливість та актуальність питань забезпечення кібербезпеки та її складових, Уряд США планує у 2021 році витратити у цьому сегменті $5,4 млрд. Відповідно до інформації, оприлюдненої на сайті Міністерства оборони США у рубриці "DOD Releases Fiscal Year 2021 Budget Proposal", ці кошти планують витратити як на забезпечення кібербезпеки, так і на проведення наступальних операцій у кіберпросторі, проведення розробок у сфері штучного інтелекту, хмарні технології тощо – загалом $9,6 млрд. Також важливим напрямом залишається посилення міждоменних рішень (*cross-domain solution, CDS*) та рішень у сфері шифрування, що сприятиме зниженню ризиків кібератак на урядові мережі. $3,8 млрд. – обсяг фінансування операцій як наступальних так і оборонного характеру на виконання положень кіберстратегії.

Наприкінці березня 2021 року стало відомо, що Адміністрація Д. Байдена готує новий указ Президента США з метою посилення кібербезпеки в сучасних реаліях. Проектом цього указу визначено 12 стратегічних кроків, якими будуть впроваджені заходи щодо мінімізації кількості кіберінцидентів, напрямки посилення захисту усіх об'єктів критичної інфраструктури. У квітні 2021 року США оголосили про 100-денний план з метою посилення кібербезпеки електроенергетичної інфраструктури країни. Передбачається плідна співпраця міністерства енергетики, приватних компаній й Агентства з кібербезпеки та інфраструктурної безпеки. Причинами для цього стали останні уразливості об'єктів енергосистеми США, які неодноразово страждали від кібератак. Вашингтон вважає, що за деякими з цих атак стоять російські хакери. З метою симетричної відповіді США у квітні 2021 року запроваджено санкції проти шести російських технологічних компаній у відповідь на "ймовірні неправомірні дії", пов'язані з кібератакою на IT-компанію "SolarWinds" та зломом систем низки американських відомств, зокрема Міненерго.

США підтримують прагнення України розвивати власну кібербезпеку та здійснювати системні заходи з метою її забезпечення. У лютому 2018 року Палата представників Конгресу США підтримала законопроект "Ukraine Cybersecurity Cooperation Act of 2017", яким було окреслено засади співробітництва між Україною та США, включаючи такі ключові напрями: вдосконалення систем безпеки урядових систем, передусім тих, які захищають критичну інфраструктуру України; зменшення залежності від російських інформаційно-комунікаційних технологій; нарощування потенціалу, розширення обміну інформацією щодо кібербезпеки; співробітництво в кіберпросторі. Передбачається, що сумарний бюджет його проектів становитиме майже $500 млн. у 2019 – 2022 роках.

У 2020 році США схвалили рішення про виділення Україні $38 млн. міжнародної технічної допомоги. Цьому передував активний діалог між США та Україною з кібербезпекових питань. Так, 3 березня 2020 року Сполучені Штати Америки та Україна провели третій діалог з питань кібербезпеки у Києві з метою визначення подальших кроків у напрямку паритетної взаємодії та закріплення нашої спільної відданості

політиці забезпечення відкритого, взаємосумісного, надійного і безпечного кіберпростору, в якому всі держави поводяться відповідально на партнерських засадах. Також у фокусі уваги сторін були такі питання, як: технологічне забезпечення зв'язку п'ятого покоління 5G, розбудова кіберпотенціалу, засад міжнародної політики стосовно забезпечення цифрового інформаційного простору, у тому числі перспективна участь у багатосторонніх заходах (форумах, конференціях, самітах), питання публічної відповідальності за наслідками кібератак.

Демонструючи свою постійну прихильність до підтримки кібербезпеки, США оголосили, що надають ще $8 млн. на кібербезпеку від Державного департаменту, у додаток до $10 млн., які були виділені у 2017 році. Частина цього фінансування буде спрямована на підтримку нового проекту з кібербезпеки Агентства США з міжнародного розвитку, за яким планується інвестувати загалом до $38 млн. протягом чотирьох років у розбудову потенціалу кібербезпеки України шляхом підтримки правової та регуляторної реформи, розвитку робочої сили у галузі інформаційних технологій, залучення приватного сектору. Очікується, що фінансування буде спрямовано на практичну реалізацію таких проектів: посилення кібербезпеки критичної інфраструктури; розробка та реалізація оновленої кіберстратегії; підвищення рівня кіберзахисту, реагування на інциденти, засоби обміну інформацією; підвищення обізнаності щодо кібербезпеки для всіх зацікавлених сторін; підготовка кадрів із надійного захисту систем промислового управління і цифрової криміналістики. Ці проекти доповнюють американо-українське співробітництво з інших питань кібербезпеки.

Важливим здобутком для України стала підготовка у березні 2021 року закону США про безпекове партнерство з нашою країною. Очікується, що з набуттям чинності цим законом безпекове партнерство з Україною буде значно активізовано та авторизовано багаторічну безпекову допомогу, визначено напрямки заохочення прискорення реформування сектору безпеки і оборони України. Нормативне забезпечення процесів стратегічного партнерства сприятиме наданню додаткового фінансування оборонної сфери України та допоможе покращити підготовку, озброєння та матеріально-технічне забезпечення військових, дозволить пришвидшити перехід на стандарти НАТО. Наприкінці квітня 2021 року Комітет Сенату США підтримав законопроект з "Безпекового партнерства з Україною". Зокрема, законодавчо задекларовано, що попри кричуще ігнорування Росією міжнародних законів і зобов'язань, Україна залишається надійним партнером США і активно протидіє масштабам зловмисного впливу держави – агресора.

Останнім часом США занепокоєні прогресивними досягненнями КНР у сфері цифрових технологій та відчувають загрозу з боку Китаю у сфері кібербезпеки. Враховуючи загрози та виклики у цій площині, Сенат США приступив до розробки законопроекту про державну підтримку виробництва чипів (напівпровідників) та готується до його розгляду у травні 2021 року. Очікується, що на створення національного технологічного виробництва напівпровідників буде виділено не менш $30 млдр. Таким чином, для політичної влади США останнім часом питання забезпечення кібербезпеки набула не аби якої актуальності на фоні збільшення кількості кібератак та чисельних й масштабних випадків несанкціонованого витоку та викрадення конфіденційної інформації. У переважних випадках відповідальність за ці спроби та таку протиправну діяльність Вашингтон покладає на китайських та російських хакерів, які цілеспрямовано діють під егідою тієї чи іншої держави.

Висновки.

Між Україною та Сполученими Штатами Америки існує стратегічне партнерство, яке треба постійно розвивати. Першочерговим аспектом залишаються фінансова підтримка та технічна допомога для України з боку США. Аналіз викладених матеріалів дозволяє констатувати, що США й надалі готові відігравати важливу роль у забезпеченні кібербезпеки України. 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. Засади державної кібербезпекової політики США демонструють, що ця країна визначає кібербезпеку як важливу складову національної безпеки та докладає кардинальних зусиль з метою її посилення та забезпечення, у зв'язку з чим на законодавчому рівні схвалюються нормативні акти, які є своєрідною реакцією на поширення новітніх загроз у кіберпросторі.

Використана література

1. 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.

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

3. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 4. С. 119-124.

4. 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

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