ФІЛОСОФІЯ ТА ПОЛІТОЛОГІЯ В КОНТЕКСТІ СУЧАСНОЇ КУЛЬТУРИ
ISSN 2663-0265 (print) ISSN 2663-0273 (online)
Journal home page: https://fip.dp.ua/index.php/FIP

МІЖНАРОДНІ ВІДНОСИНИ

Олександр Сергійович БІЛОУСОВ
Доктор політичних наук, професор кафедри міжнародних відносин та права,
Національний університет «Одеська політехніка»,
пр. Шевченко, Одеса, 1, 65044, Україна
E-mail: o.s.bilousov@op.edu.ua,

Дмитро Дмитрович ТАТАКІ
Старший викладач кафедри міжнародних відносин та права,
Національний університет «Одеська політехніка»,
пр. Шевченко, Одеса, 1, 65044, Україна
E-mail: d.d.tataki@op.edu.ua,

Олена Олегівна ТАТАКІ
Старший викладач кафедри інформаційної діяльності та медіа-комунікацій,
Національний університет «Одеська політехніка»,
пр. Шевченко, Одеса, 1, 65044, Україна
E-mail: tataki.olena@op.edu.ua,

Oleksandr BILOUSOV
Doctor of Political Science,
Professor of the Department of International Relations and Law,
National University of Odessa Polytechnic,
1 Shevchenko Ave., Odessa, 65044, Ukraine
ORCID: https://orcid.org/0000-0002-6709-9899

Dmytro TATAKI
Senior lecturer of the Department of International Relations and Law,
National University of Odessa Polytechnic,
1 Shevchenko Ave., Odessa,
65044, Ukraine
ORCID: https://orcid.org/0000-0003-3091-3540

Olena TATAKI
Senior lecturer of the Department of Information Activities and Media Communications,
National University of Odessa Polytechnic,
1 Shevchenko Ave., Odessa,
65044, Ukraine
ORCID: https://orcid.org/0000-0003-0724-0755

УДК: 327

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА В США

Received 29 October *2023; revised 20 November 2023; accepted 10 December 2023*
DOI: 10.15421/352346

Анотація

Вивчення досвіду країн, що досягли успіхів у сфері міжнародної інформаційної безпеки, є важливим етапом для нашої держави. Продовження реформ та модернізації інформаційної безпеки українського суспільства буде сприяти створенню ефективної системи захисту від кібератак та інших загроз, забезпеченню правового підґрунтя для інформаційної безпеки та для підвищення готовності нашої держави до інформаційної війни.

Врахування та впровадження досвіду США у сфері інформаційної безпеки, може стати ключовим фактором у підвищенні рівня інформаційної безпеки в Україні, забезпечити захист від кібератак та негативних впливів інформаційної війни, сприяти розвитку національної інформаційної безпеки та захисту критичної інфраструктури України.

Метою дослідження є визначення на основі аналізу системи національної безпеки США пріоритетів міжнародної інформаційної політики, США в сучасних умовах.

Міжнародна інформаційна безпека є важливим питанням для США, оскільки залежність від інформаційних технологій та відкритість публічного простору робить їх уразливими перед кібернетичними загрозами з боку іноземних держав і недобросовісних суб'єктів.

США сприяє укріпленню кібербезпеки та обміну інформацією між країнами для забезпечення світової стабільності та безпеки. Сполучені штати активно працюють над заходами з попередження кібератак, виявлення та припинення кіберзлочинів, посилення кіберзахисту критичних інфраструктур. Основні пріоритети міжнародної інформаційної політики, США у сучасних умовах включають: створення сильного кіберзахисту; забезпечення інформаційної безпеки; підвищення кваліфікації фахівців, що працюють у сфері кібербезпеки США; боротьба з кіберзлочинністю; виявлення та реагування на кіберзагрози.

Ключові слова: кібербезпека, цифрові технології, інформаційна політика.

INTERNATIONAL INFORMATION SECURITY IN THE USA

Abstract

Studying the experience of countries that have achieved success in the field of international information security is an important step for our country. Continued reforms and modernisation of the information security of Ukrainian society will help to create an effective system of protection against cyberattacks and other threats, ensure a legal basis for information security and improve our country's readiness for information warfare.

Taking into account and implementing the US experience in the field of information security can be a key factor in improving the level of information security in Ukraine, providing protection against cyberattacks and the negative effects of information warfare, and contributing to the development of national information security and protection of Ukraine's critical infrastructure.

The purpose of the study is to determine, based on the analysis of the US national security system, the priorities of international information policy of the United States in the current conditions.

International information security is an important issue for the United States, as its dependence on information technology and the openness of public space makes it vulnerable to cyber threats from foreign states and unscrupulous actors.

The United States promotes cybersecurity and information sharing between countries to ensure global stability and security. The United States is actively working on measures to prevent cyberattacks, detect and suppress cybercrime, and strengthen the cyber defence of critical infrastructures. The main priorities of the US international information policy in the current environment include: creating a strong cyber defence; ensuring information security; improving the skills of specialists working in the field of US cybersecurity; fighting cybercrime; detecting and responding to cyber threats.

Keywords**: **cybersecurity, digital technologies, information policy.

Постановка проблеми.

Вивчення досвіду країн, що досягли успіхів у сфері міжнародної інформаційної безпеки, є важливим етапом для нашої держави. Продовження реформ та модернізації інформаційної безпеки українського суспільства буде сприяти створенню ефективної системи захисту від кібератак та інших загроз, забезпеченню правового підґрунтя для інформаційної безпеки та підвищенню готовності нашої держави до інформаційної війни.

Врахування та впровадження досвіду США у сфері інформаційної безпеки, може стати ключовим фактором у підвищенні рівня інформаційної безпеки в Україні, забезпечити захист від кібератак та негативних впливів інформаційної війни, сприяти розвитку національної інформаційної безпеки та захисту критичні інфраструктури України.

Аналіз останніх досліджень.

Ряд відомих вітчизняних та експертів з кібербезпеки, інформаційних технологій захисту інформації займаються проблемами інформаційної безпеки, беруть участь в. розробці інформаційних технологій; заходів щодо захисту інформації, а також консультують урядові структури та організації з різних аспектів кібербезпеки. Зокрема це такі науковці: В.Бабін, В.Волков, Н.Криницька, О.Клименко, О.Чечел, І.Юсипенко, І.Різун. Означені науковці проводять дослідження в галузі кібербезпеки, Вони публікують свої результати в авторитетних наукових журналах та беруть участь у конференціях та семінарах з кібербезпеки.

Провідними вітчизняними дослідниками, які займаються проблемами інформаційної безпеки є: В.Бебик, В.Ліпкан, Є.Магда, Г.Почепцов, Г.Хоружий, І.Чиж та ін. Окремі аспекти міжнародної інформаційної безпеки США розглянуті в наукових дослідженнях: Є.Богданович, Н.Вознюк, Н.Захаренко, Є.Марко, К. Ничипорчук, Г.Піскорської, І.Чарських, І.Черновол, Л.Яковенко.

Проте, подальшого дослідження потребує з'ясування пріоритетів міжнародної інформаційної політики, США у мінливих умовах сучасності.

Метою дослідження є визначення на основі аналізу системи національної безпеки США пріоритетів міжнародної інформаційної політики, США у сучасних умовах.

Виклад основного матеріалу.

США – одна з найсильніших фінансових

систем у світі. Долар США є однією з найважливіших світових резервних валют, і більшість міжнародних фінансових операцій здійснюється саме в доларах США.

Вражає своєю масштабністю технологічний потенціал Сполучених Штатів. Новітні комунікаційні та інформаційні технології використовуються в усіх сферах суспільного життя, зокрема в бізнесі, медицині, освіті, авіакосмічному секторі, обчислювальній техніці та зв'язку [Military Strength Ranking 2023].

Сполучені Штати мають неабиякий потенціал у сфері науки та технологій. Вони є лідером у медицині, біотехнологіях, космічних дослідженнях, інженерії та інформаційних технологіях. Чимало великих дослідницьких центрів та університетів США широко відомі своїми науковими дослідженнями в усьому світі.

Найбільша і найпотужніша армія у світі належить Сполученим Штатам Америки. Сполучені Штати мають широкий спектр високотехнологічних озброєнь, ядерну зброю, військово-повітряні сили, військово-морський флот і високорозвинену кібернетичну оборону. Так, згідно з даними авторитетного індексу «Рейтинг військової сили» (Global Firepower далі – індекс GFP). США 10 років поспіль демонструє високі показники в ключових матеріальних, фінансових і ресурсних категоріях. Крім того, У 2023 році США у Рейтингу військової сили знову посіла 1 місце серед 145 країн [United States Military 2023].

Передові військові можливості США ґрунтуються на їх економічному та технологічному лідерстві у світі та потужній науково-технічній базі країни. Крім того, США мають найбільший військовий бюджет у світі, що дає їм змогу фінансувати та розвивати низку стратегічних програм проєктів з міжнародної інформаційної безпеки.

Усі ці фактори перетворюють Сполучені Штати на одну з найпотужніших наддержав сучасного світу і можуть впливати на політичні, економічні та геополітичні події у світі.

Комп'ютерний/телекомунікаційний сектор США є високорозвиненим завдяки існуванню всебічного інформаційного законодавства. Наприклад, 1947 року було ухвалено Закон про національну безпеку США [Milestones: 1945-1952], на основі якого згодом було створено нормативну базу для законодавства про національну розвідку захисту інформації.

Низка стандартів і сертифікатів, розроблених у США, дають змогу забезпечити захист інформації на законодавчому рівні. Наприклад, Федеральний стандарт опрацювання інформації (FIPS) [FIPS Home Page 2023] встановлює вимоги до криптографічних алгоритмів і продуктів, що використовуються в урядових системах.

Цифрові технології дозволили США здійснювати чимало транзакцій в електронному вигляді та зберігати великі обсяги даних в електронному вигляді, однак вони також зробили США вразливими до кіберзагроз. Кібератаки можуть мати глобальний вплив на економічні та політичні сфери. Так, хакерські атаки на різні сектори економіки, наприклад, на фінансові установи та енергетичну галузь, можуть спричинити серйозні економічні збитки та порушити національну стабільність. Такі загрози також можуть вплинути на глобальну економіку, оскільки низка американських компаній і банків мають дочірні компанії та партнерів за кордоном. Тому захист конфіденційної інформації та персональних даних, разом із національною та військовою таємницею, інтелектуальною власністю та комерційною інформацією, мають надзвичайно важливе значення для міжнародної національної безпеки та конкурентоспроможності США.

Отже, міжнародна інформаційна безпека США грає вагому роль у забезпеченні економічної та політичної стабільності, протидії глобальним кіберзагрозам та захисті чутливої інформації у світі.

Без перебільшення можемо зазначити, що сьогодні США має найпотужніший і всеохоплюючий режим управління інформаційною безпекою. Зокрема, за інформаційну безпеку та захист урядових систем та державної інфраструктури США відповідають ціла низка державних та федеральних структур, зокрема, Федеральне агентство кібербезпеки та інфраструктури (CISA) [Website. CISA 2023],

Рада національної безпеки [National Security Council 2023], Федеральне бюро розслідувань (ФБР) [FBI 2023], Агентство національної безпеки (АНБ) [National Security Agency/ Central Security Service 2023], Міністерство оборони (МО) [Department of Defense.U.S 2023], Комісія з цінних паперів та бірж (SEC) [SEC.gov 2023], [SEC.gov 2023], [SEC.gov 2023], [SEC.gov 2023], [SEC.gov 2023], [SEC.gov 2023], [SEC.gov 2023]. Всі ці установи та організації у своїх внутрішніх структурах мають власні відділи, які займаються питаннями інформаційної безпеки та запобіганням до інформаційних атак, а також підготовкою до кібератак.

Для захисту інформаційних систем так званих «потужних організацій» (військових і розвідувальних служб) необхідне застосування особливих підходів і методів. До штату Агентств і організацій, що займаються захистом інформаційних систем, входять зазвичай експерти з кібербезпеки.

Починаючи з 1992 року Міністерство оборони США організовує свою діяльність у сфері інформаційної безпеки на основі концепції «інформаційної війни». Ця концепція полягає в тому, що хакери та кіберзлочинці можуть використовувати інформаційні технології для підриву національної безпеки. Тому Міністерство оборони зосереджується на протидії хибним системам командування та управління, інакше кажучи, на постійній основі досліджується питання щодо запобігання злому та неправомірному втручанню у військові інформаційні системи.

Одним із важливих напрямів подальшого розвитку інформаційної безпеки є підвищення ефективності військових інформаційних систем США. Це включає розробку та впровадження низки заходів щодо захисту від кібератак, а також застосування механізмів для забезпечення цілісності, конфіденційності та доступності інформації.

Агентство національної безпеки США («АНБ») має безпосереднє відношення до інформаційної безпеки США. АНБ є розвідувальною організацією національного рівня. Прообразом АНБ був підрозділ із дешифрування зашифрованих повідомлень у період час Другої світової війни. У 1952 р. Президент Гаррі Трумен створив Агентство національної безпеки – незалежну агенцію з дешифрування. Сьогодні АНБ є найбільшою розвідувальною організацією США за чисельністю персоналу та бюджетом; її місія полягає в глобальному моніторингу, збиранні та обробці розвідувальної інформації для зовнішньої та внутрішньої розвідки та контррозвідки [National Security Agency 2023].

АНБ забезпечує конфіденційність, цілісність і доступність даних і комунікацій, життєво важливих для США, а також протидіє кібератакам, тероризму, шпигунству та іншим загрозам національній безпеці. Крім того, АНБ розробляє протоколи та стандарти, що дають змогу американським силам безпечно обмінюватися інформацією із союзниками, НАТО і коаліційними силами по всьому світу [Central Security Service 2023].

У структурі АНБ функціонує Управління розвідки сигналів (SIGINT), що відповідає за забезпечення політиків, військових, президента, Конгресу, військового командування, інших урядових установ США та іноземних партнерів розвідувальною інформацією щодо іноземних сигналів у рамках спільних розвідувальних програм та угод.

Місія SIGINT полягає у зборі й аналізі розвідувальної інформації стосовно електронних сигналів від іноземних об’єктів і забезпеченні її оперативного застосування в інтересах національної безпеки США [Overview of Signals Intelligence (SIGINT)].

Завданням SIGINT є збір й ретельний аналіз розвідувальної інформації стосовно електронних сигналів від іноземних об’єктів і забезпечення її оперативного застосування для забезпечення національної безпеки США [Signals Intelligence (SIGINT) Overview 2023].

У 1972р. заснована Центральна служба безпеки (CH/CSS) США. Ця організація співпрацює з АНБ, з криптологічними елементами Збройних сил США та забезпечує криптологічну підтримку військовому криптологічному товариству.

CH/CSS координує розвідку сигналів і політику кібербезпеки, а також здійснює керування з підтримки військової інтеграції. У ре-

зультаті злиття Центрального агентства безпеки та АНБ було створено подвійне керівництво, яке очолило криптографічну діяльність. Голова Центрального агентства безпеки також є головним радником директора АНБ з питань військової криптографії [NSA Supporting the Military 2023]. Керівник АНБ відповідає за керівництво і координацію роботи АНБ, Кіберкомандування США (USCYBERCOM) і Криптологічного підрозділу, стежить за тим, щоб ці організації виконували свої місії та використовували свої ресурси для забезпечення національної безпеки та кібербезпеки. Заступник директора з питань криптографії (DCH/CSS) є головним радником директора АНБ з питань військової криптографії та військового потенціалу. Він керує військовою криптографічною системою і координує роботу АНБ/CSS зі службами криптографічного компонента, а також забезпечує реалізацію Національної криптографічної стратегії.

У розвідувальній діяльності АНБ співпрацює з рядом розвідувальних агентств США, зокрема із ЦРУ та Розвідувальним агентством Міністерства оборони (DIA).

Розвиток інформаційної безпеки передбачає навчання та підготовку фахівців з кібербезпеки на спеціалізованих навчальних програмах, тренінгах та проходження сертифікацій у сфері інформаційної безпеки.

АНБ співпрацює з багатьма розвідувальними службами США, зокрема з ЦРУ та Розвідувальним управлінням Міністерства оборони (DIA).

Успішний розвиток сфери інформаційної безпеки передбачає проведення навчання та підвищення кваліфікації фахівців з кібербезпеки за допомогою різноманітних спеціалізованих навчальних програм, а також отримання освіти та сертифікації у сфері інформаційної безпеки.

АНБ співпрацює з науково-освітніми та академічними закладами задля проведення спільних науково-технічних проєктів з інформаційної безпеки в США. Зокрема, у 1998-2001 роках Стенфордський університет уклав контракт з Агентством національної безпеки США щодо створення Консорціуму з дослідження інформаційної безпеки та політики (Consortium for Research on Information Security and Policy – далі CRISP) – програми, спрямованої на забезпечення форуму для аналізу та розроблення інформації про кібербезпеку критично важливих національних інфраструктур. У CRISP брали участь різні академічні організації, науково-дослідні інститути, інформаційно-технологічні компанії та окремі урядові структури. Програма провела дослідження інтернет-додатків у різних країнах і оцінила їхню вразливість і безпеку, а також організувала форум із кібербезпеки для обговорення рішень. Результати цих досліджень були оприлюднені у вигляді звітів і статей

Загалом, програма CRISP стала важливим та вдалим етапом у розвитку національного діалогу з питань кібербезпеки [Consortium for Research 2023].

Управління інформаційною безпекою на державному рівні в США має вагоме значення для розвитку міжнародного співробітництва та інформаційної безпеки. Сполучені Штати відіграють дуже важливу роль у світі, зокрема у сфері політики, економіки та міжнародних відносин. Отже, це означає, що кіберзагрози, які безпосередньо впливають не тільки на США, а й на інші країни, можуть мати глобальні наслідки, тому управління інформаційною безпекою на національному рівні має неабияке значення для забезпечення стабільності та безпеки не тільки Сполучених Штатів, а й інших країнах світу.

Сполучені Штати дуже активно та плідно співпрацюють з різними країнами та міжнародними організаціями у сфері інформаційної безпеки. Так, наприклад, Сполучені Штати часто організовують спільні навчання та обмінюються інформацією зі своїми союзниками з НАТО та іншими міжнародними партнерами. Адже, це по-перше, може допомагати США забезпечити колективну безпеку своїх союзників, включно з доступом до новітніх інформаційних технологій, обміном досвідом із союзниками та партнерами, підвищенням рівня обороноздатності та захистом союзників від потенційних розвідувальних загроз. По-друге, взаємодія з союзниками та партнерами допомагає Сполученим Штатам краще зрозуміти глобальні виклики та шляхи їх подолання.

По-третє, Сполучені Штати можуть впливати на ухвалення рішень у НАТО і користуватися розвідувальними ресурсами інших членів Альянсу.

По-четверте, участь у НАТО дозволяє Сполученим Штатам зміцнювати свої дипломатичні відносини з іншими країнами та демонструвати свою глобальну лідерську роль, зокрема у сферах міжнародної безпеки та інформаційної безпеки. Північноатлантичний альянс співпрацює з низкою країн – партнерів, залучених до спільних зусиль із захисту глобального кіберзахисту. Наприклад, Центр кібербезпеки НАТО й Організація зв'язку та розвідки НАТО (NCI Agency) співпрацюють з іншими організаціями з кібербезпеки, організовуючи спільні навчання, семінари, тренінги з метою підвищення знань і навичок персоналу та обміну передовим досвідом і технологіями в галузі кібербезпеки [Employment Love technology 2023].

Як член НАТО, Сполучені Штати постійно організовують спільні навчання та обмінюються досвідом. Тому необхідно встановити єдині міжнародні норми та правила, що регулюють цю сферу.

У 2021 році НАТО розробила комплексну політику кіберзахисту, яка визначає ключові завдання кібербезпеки, спільну позицію Альянсу щодо захисту держав-членів від кіберзагроз [Cyber defence. NATO. 2023]. Програму було додатково доопрацьовано на саміті НАТО у Вільнюсі у 2023 році. Альянс прийняв концепцію зміцнення зусиль НАТО щодо кіберзахисту та стримування, а також створив новий потенціал НАТО з підтримки віртуальних кіберінцидентів (VCISC) для підтримки національних зусиль із пом'якшення наслідків у відповідь на значну зловмисну кіберактивність [Vilnius Summit 2023].

Як провідний член НАТО, Сполучені Штати активно співпрацюють з країнами-партнерами, освітніми та дослідницькими установами, щоб обмінюватися досвідом, навчати експертів і покращувати загальні можливості кіберзахисту. Члени Альянсу також роблять внесок у кібербезпеку держав-членів, надаючи підтримку та консультації. Одним із прикладів співпраці НАТО з міжнародними партнерами є Координаційний центр передових експериментів із кіберзахисту (CCDCOE), якій створено в Естонії завдяки спільній ініціативі 10 держав-членів НАТО, членів (включаючи США) і країн-партнерів. CCDCOE проводить дослідження, тренінги та консультації у сфері кіберзахисту та сприяє підвищенню кваліфікації фахівців у IT сфері [CCDCOE – The NATO 2023].

У зв'язку з постійним зростанням загроз кібербезпеці, НАТО покладає велике значення на розвиток кіберздатності та забезпечення стійкості своїх комунікаційних та інформаційних систем.

Альянс звертає значну увагу на розробку новітніх технологій та інноваційних рішень у сфері кіберзахисту.

Важливо відзначити, що США та НАТО підтримує принцип пропорційності та дотримання міжнародного права в кіберпросторі.

Всі члени Північноатлантичного альянсу вважають, що кіберзахист є важливою складовою безпеки та стійкості, і зосереджує зусилля на його забезпеченні, як на національному рівні, так і в рамках співробітництва з партнерами.

Така співпраця допомагає покращити взаємодію між країнами та забезпечити спільний підхід до реагування на кіберзагрози.

Усі ці заходи спрямовані на забезпечення безпеки та стабільності Альянсу в кіберпросторі, а також на посилення спроможності членів НАТО реагувати на кібератаки та запобігати їм.

Кіберзахист залишається одним із найважливіших пріоритетів безпеки НАТО, оскільки кіберзагрози продовжують зростати та стають дедалі складнішими.

Однак варто підкреслити, що участь США в НАТО також тягне за собою значні фінансові витрати та зобов'язує країну підтримувати своїх союзників у разі військового нападу.

Крім того, напруга може виникнути через різні погляди та інтереси країн-членів. США активно співпрацюють з країнами Європейського Союзу, особливо з країнами-учасницями Північноатлантичного альянсу. Вони спільно проводять навчання та бойові дії, обмінюються інформацією та розвіддани-

ми, спільно розробляють оборонну техніку та озброєння.

Участь США в програмі НАТО є важливим аспектом їхньої зовнішньої політики, що сприяє захисту та розвитку національної безпеки та інформаційних технологій, а також глобальному розвитку.

США є активним учасником багатьох міжнародних організацій, таких як ООН, ОБСЄ, Всесвітня організація торгівлі.

Ці організації дозволяють Сполученим Штатам співпрацювати з іншими країнами з питань, пов'язаних із міжнародною інформаційною безпекою, кіберзахистом і стандартами, інструментами, методами, стратегіями чи підходами кібербезпеки.

США мають міжнародні програми співпраці з такими країнами, як Ізраїль, Японія, Південна Корея, Австралія та інші.

Ці партнерства дозволяють обмінюватися досвідом та новітніми інформаційними технологіями, спільно розв'язувати проблеми міжнародної інформаційної безпеки.

Міжнародне співробітництво та співробітництво у сфері міжнародної інформаційної безпеки мають стратегічне значення для Сполучених Штатів, оскільки дозволяють США підтримувати високий рівень обороноздатності та забезпечувати інформаційну безпеку.

Крім того, це також сприяє стабільності та миру у світі, оскільки міцне партнерство є гарантією мінімізації кіберзагроз.

Великі ІТ-компанії в США, які мають доступ до значних ресурсів і розробляють нові інформаційні технології та програмне забезпечення, здатні забезпечити міжнародну інформаційну безпеку в сучасних умовах.

Висновки.

Міжнародна інформаційна безпека є важливим питанням для США, оскільки залежність від інформаційних технологій та відкритості публічного простору робить їх уразливими перед кібернетичними загрозами з боку іноземних держав і недобросовісних суб'єктів.

З точки зору міжнародної безпеки, Сполучені Штати відіграють ключову роль у розвитку кібербезпеки та обміні інформацією між державами для підтримки стабільності та забезпечення глобальної безпеки.

Сполучені Штати вживають активних заходів для запобігання кібератакам, виявлення та припинення кіберзлочинів, а також посилення безпеки об'єктів критичної інфраструктури.

Основні пріоритети міжнародної інформаційної політики, США у сучасних умовах включають:

1. Створення сильного кіберзахисту. США постійно вкладають великі фінансові та матеріальні ресурси у розробку та впровадження прогресивних інформаційних технологій, які дозволяють виявляти та нейтралізовувати кіберзагрози. Компанії та урядові структури активно співпрацюють зі спеціалістами з кібербезпеки для виявлення й усунення вразливостей у своїх системах.

2. Забезпечення інформаційної безпеки. США активно співпрацюють з іншими країнами та міжнародними організаціями (ООН, ОБСЄ, НАТО ЄС та інші) з метою обміну інформацією щодо кіберзагроз та виявлення вразливостей у критичних інфраструктурах. Країна також підтримує зусилля у формуванні міжнародних стандартів і правил щодо кібербезпеки.

3. підвищення кваліфікації фахівців, що працюють у сфері кібербезпеки США. Зараз у державі є багато приватних компаній та урядових структур, шкіл, курсів та стажувань для спеціалістів з кібербезпеки. Країна активно працює над привертанням талановитих фахівців та надає підтримку для їх професійного розвитку.

4. Боротьба з кіберзлочинністю. Уряд США постійно налагоджує співпрацю з урядами інших країн, правоохоронними органами та приватним сектором для виявлення, припинення та покарання злочинців, які здійснюють кібератаки.

5. Виявлення та реагування на кіберзагрози. Урядові організації США, які відповідальні за міжнародну інформаційну безпеку активно моніторять та виявляють потенційні кіберзагрози. Країна має ефективний механізм для швидкого реагування на такі загрози та нейтралізації їхнього впливу.

Бібліографічні посилання / References

«Vilnius Summit Communiqué». (2023). *NATO*. Retrieved October 20, 2023 from https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

CCDCOE. (2023). *The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.* Retrieved October 21, 2023 from https://ccdcoe.org/

Consortium for Research on Information Security and Policy. (2023). *Freeman Spogli Institute for International Studies|FSI.* Retrieved October 21, 2023 from https://fsi.stanford.edu/research/consortium_for_research_on_information_security_and_policy

Cyber defence. (2023). *NATO.* Retrieved October 27, 2023 from https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en#defence

Employment Love technology? Use your skills to contribute to the Alliance. (2023). *NATO COMMUNICATIONS AND INFORMATION AGENCY.* Retrieved October 20, 2023 from https://www.ncia.nato.int/about-us.html

FBI. (2023). Retrieved October 22, 2023 from http://www.fbi.gov

Home Page. CISA. (2023). *Home Page | CISA*. Retrieved October 20, 2023 from https://www.cisa.gov/

Milestones: 1945-1952. (2023). *Office of the Historian.* Retrieved October 21, 2023 from https://history.state.gov/milestones/1945-1952/national-security-act#:~:text=The%20National%20Security%20Act%20of,National%20Security%20Council%20(NSC).

National Security Agency. (2023). *Central Security Service.* Retrieved October 20, 2023 from https://www.nsa.gov/About/Mission-Combat-Support/

National Security Agency. (2023). *National Security Agency|Central Security Service*. Retrieved October 20, 2023 from https://www.nsa.gov/.

National Security Agency/Central Security Service». (2023). *Signals Intelligence (SIGINT) Overview.* Retrieved October 23, 2023 from https://www.nsa.gov/Signals-Intelligence/Overview/

National Security Council (2023). *The White House.* Retrieved October 15, 2023 from https://www.whitehouse.gov/nsc/#:~:text=The%20National%20Security%20Council%20is,these%20policies%20across%20federal%20agencies

NSA Supporting the Military. (2023). *National Security Agency*. Retrieved October 14, 2023 from https://www.nsa.gov/about/central-security-service/

SEC.gov. (2023). *HOME.SEC.gov|HOME.* Retrieved October 21, 2023 from https://www.sec.gov/

The FIPS Home Page. (2023). *Wayback Machine*. Retrieved October 11, 2023 from https://web.archive.org/web/20040826081308/http://www.itl.nist.gov/fipspubs/

U.S. (2023). *Department of Defense.* Retrieved October 19, 2023 from https://www.defense.gov/

United States Military Strength. (2023). *Global Firepower – 2023 World Military Strength Rankings.* Retrieved October 18, 2023 from https://www.globalfirepower.com/country-military-strength-detail.php?country_id=united-states-of-america

United States Military Strength. Global Firepower – 2023. (2023). *World Military Strength Rankings.* Retrieved October 20, 2023 from https://www.globalfirepower.com/country-military-strength-detail.php?country_id=united-states-of-america