vseukrainskoi naukovo-praktychnoi konferentsii studentiv ta molodykh/za zah. red. O. V. Shershnovoi. Ostroh: Vydavnytstvo Natsionalnoho universytetu «Ostrozka akademiia», p. 71–80.
16. Smola, L. Ie. (2016). Aspekty vedennia informatsiinoi ta hibrydnoi viiny v konteksti zastosuvannia komunikatsiinykh tekhnolohii. *S.P.A.C.E,* № 1, p. 48–53.
17. Suchasna kremlivska mifolohiia: yak Rosiia vykorystovuie istoriiu u propahandi. 04.03.2019. URL: https://www.stopfake.org/uk/suchasna-kremlivska-mifologiya-yak-rosiya-vykorystovuye-istoriyu-u-propagandi/. (16.02.2020).
18. Tykhomyrova, Ye.B. (2019). RT (Russia Today). *Hlosarii: navchalnyi entsyklopedychnyi slovnyk-dovidnyk z pytan informatsiinoi bezpeky*/za zah. redaktsiieiu d. polit. n., prof. A. M. Shuliak, p. 386–390.
19. Turchynov, O. (17.08.2016). Formuvannia novoho svitovoho balansu syl ta peredumovy rosiiskoi ahresii proty Ukrainy. https://ua.112.ua/mnenie/formuvannia-novoho-svitovoho-balansu-syl-ta-peredumovy-rosiiskoi-ahresii-proty-ukrainy-332465.html (24.02.2020).
20. Feskov, I. V. (2016). Osnovni metody vedennia hibrydnoi viiny v suchasnomu informatsiinomu suspilstvi. *Aktualni problemy polityky*, Vyp. 58, p. 66–77.
21. Wasiuta, O., Wasiuta, S., (2017). *Wojna hybrydowa Rosji przeciwko Ukrainie.* Arcana: Kraków.

УДК 351.746.1:007(73)

Шуляк Назарій,
магістр кафедри міжнародних комунікацій та політичного аналізу,
Східноєвропейський національний університет імені Лесі Українки,
43024, Україна, Волинська обл., м. Луцьк, вул. Винниченка, 28, каб. 8
ORCID ID 0000-0002-9835-731X

ДО ПИТАННЯ ПРО ОСНОВИ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ США

У роботі розглянуто складові частини державної інформаційної політики щодо забезпечення інформаційної безпеки країни й визначено основні напрями діяльності органів державної влади в цій сфері. Проаналізовано внутрішні та зовнішні інформаційні загрози національній безпеці держав «великої сімки» й шляхи гарантування інформаційної безпеки країн. Інформаційну безпеку розглянуто як складник національної безпеки держави, а також як глобальну проблему захисту інформації, інформаційного простору, інформаційного суверенітету країни та інформаційного забезпечення прийняття урядових рішень. Запропоновано підходи щодо забезпечення процесу безперервності функціонування системи інформаційної безпеки держави задля моніторингу нових загроз, визначення ризиків і рівнів їх інтенсивності.

Ключові слова: *держава, політика, безпека, загрози, ресурси, США.*

1. ВСТУП

Постановка проблеми та її значення. Нині активно відшуковуються шляхи подолання небезпек, варіанти ведення інформаційних війн, залучення ресурсів «м'якої сили» тощо. Об'єктивний той факт, що необхідність в інформаційній безпеці виникла з появою мас-медіа як засобу комунікації між людьми, у тому числі й у політичній сфері, та усвідомленням спільності інтересів, забезпечення яких можливе за посередництва ЗМІ. Завдавання збитків і шкоди комунікаціям призводить до руйнування інформаційного обміну між різними елементами політичної системи. Натомість заходи інформаційної безпеки можуть стати новим стратегічним імпульсом діяльності органів державної влади, інститутів громадянського суспільства, для формування й реалізації демократичної інформаційної політики.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Кожна держава розгортає свою мережу зовнішньополітичної комунікації, яка забезпечує її національні інтереси. Завдання зовнішньополітичних установ – розробляти стратегію керування інформаційними потоками. Сучасне суспільство все менше піддається впливу засобів прямої агітації.

Тож у міжнародних відносинах використовують нові технології впливу на цільову аудиторію. Уміння керувати ними є однією з умов інформаційної безпеки. На сьогодні кращими практика інформаційної безпеки володіють держави «великої сімки», тому вважаємо за доцільне саме їхній приклад застосувати для України, яка перебуває в стані гібридної війни.

Захист комп‟ютерних мереж охоплює заходи, спрямовані на захист інформації, комп‟ютерів і мереж від проникнення, пошкодження або знищення противником. До найбільш уразливих елементів національної інформаційної інфраструктури належать такі, як обладнання, уключаючи периферійне й комунікаційне; комп‟ютери, теле-, відео- та аудіо- обладнання; програмне забезпечення; мережеві стандарти й коди передачі даних; інформація як така, представлена у вигляді баз даних, аудіо- та відеозаписів, архівів й ін.; фахівці, котрі працюють в інформаційній сфері. Розуміючи, що стійке функціонування держави і всіх її інститутів все більше залежить від стабільної роботи ключових систем безпеки, у тому числі й інформаційних, американський уряд розпорядженням № 13010 від 15 липня 1996 р. створив президентську комісію із захисту критичних інфраструктур (Presidential Commission for Critical Infrastructure Protection – PC-CIP). Вона в жовтні 1997 р. опублікувала звіт «Критичні основи. Захист американської інфраструктури». Керуючись його рекомендаціями, президент США в травні 1998 р. підписав дві директиви – № 62 «Боротьба з тероризмом» та № 63 «Захист критичної інфраструктури», – у яких зафіксовано основні напрями дій щодо захисту національних об‟єктів критичної інфраструктури, зокрема інформаційних [52].

Директива № 63 серед іншого визначає відомства, відповідальні за пріоритетні напрями діяльності, так чи інакше пов‟язані із захистом критично важливих об‟єктів інфраструктури, у тому числі за національну оборону – МО, міжнародні відносини – державний департамент, розвідку – ЦРУ й законодавче забезпечення цієї діяльності – міністерство юстиції та ФБР. З урахуванням рекомендацій провідних відомств і національної економічної ради президент США повинен був сформувати Національну раду з безпеки інфраструктури (National Infrastructure Assurance Council – NIAC), покликаний поліпшити взаємодію в цій сфері між державним та приватним секторами. Однак, незважаючи на ці заходи, безпосереднє завдання забезпечення безпеки критично важливих об‟єктів інфраструктури залишилося досі не виконаним.

Відповідно до Закону про єднання й згуртування США задля вжиття заходів для боротьби з тероризмом (Uniting and strengthening America by Providing Appropriate Tools, Required to Intercept and Obstruct Terrorism – USA PATRIOT Act), прийнятим конгресом 26 жовтня 2001 р., критичну інфраструктуру визначено як «сукупність фізичних або віртуальних систем і засобів, важливих для країни такою мірою, що їх вихід із ладу або знищення може призвести до згубних наслідків у сфері оборони, економіки, охорони здоров‟я й безпеки нації».

У січні 2001 р. опубліковано звіт комісії з національної безпеки (комісія Харта-Рудман), у якому йдеться про «необхідність кардинальних змін у структурі та діяльності американських відомств, що забезпечують національну безпеку». Зокрема, запропоновано зробити проблематику «внутрішньої безпеки» пріоритетною й створити самостійне агентство внутрішньої безпеки (АВБ).

Ще в березні 2001 р. президент США Джордж Буш, виступаючи в штаб-квартирі ЦРУ в Ленглі, перерахував головні загрози безпеці Сполучених Штатів. На другому місці після тероризму в цьому переліку значиться інформаційна війна й уже за нею – поширення зброї масового ураження та засобів її доставки.

Після терористичних атак 11 вересня 2001 р. в кінці 2001 – початку 2002 р. США здійснили низку організаційних і законодавчих заходів щодо підвищення безпеки національної території. Президент Дж. Буш призначив Т. Ріджа, колишнього губернатора штату Пенсильванія та свого особистого друга, на новостворену посаду радника з питань внутрішньої безпеки, а невдовзі після цього заснував АВБ, при якому створено раду внутрішньої безпеки. До складу цього органу увійшли президент (голова), віце-президент, міністри фінансів, оборони, юстиції, охорони здоров‟я й транспорту, директора федерального агентства з надзвичайних ситуацій, ФБР і ЦРУ, помічник президента з внутрішньої безпеки та інші посадові особи виконавчої гілки влади, яких глава держави може, за необхідності, запрошувати на засідання ради. Керівники адміністрацій президента й віце-президента, а також помічник президента з національної безпеки мають вільний доступ на будь-які збори ради. Держсекретар, міністри сільського господарства, внутрішніх справ, енергетики, праці та торгівлі, секретар у справах ветеранів, керівник агентства із захисту навколишнього середовища, помічники

президента з економічної та внутрішньої політики запрошуються лише на ті засідання, де розглядаються питання, що належать до їх компетенції [59].

У ході радикальної реструктуризації й зміцнення виконавчої владі 25 листопада 2002 р. Дж. Буш підписав Закон про внутрішню безпеку, відповідно до якого в січні 2003-го АВБ перетворено в міністерство внутрішньої безпеки (МВБ). Очолив міністерство Т. Рідж, а його заступником став міністр ВМС США Г. Інгланд.

1 березня 2003 р. в штат МВБ передані та приступили до виконання своїх обов"язків за рішенням «завдань аналізу інформації та захисту інфраструктури такі підрозділи центральних органів виконавчої влади уряду США, як управління безпеки критичної інфраструктури міністерства торгівлі (Infrastructure Assurance Office – CIAO), Національний центр захисту інфраструктури при ФБР міністерства юстиції (National Infrastructure Protection Center-NIPC), Національний центр моделювання та аналізу інфраструктури при інституті проблем захисту інформаційної інфраструктури міністерствами з енергетики (National Infrastructure Simulation and Analysis Center – NISAC), федеральний центр захисту інформаційних ресурсів адміністрації загальних служб (Federal Computer Incident Response Center of the General Services Administration – FedCIRC), управління безпеки енергетичних систем міністерства енергетики (Energy Assurance Office of the Department of Energy – EAO), Національна система зв"язку МО (National Communication System – NCS). Під час підготовки війни в Іраку американська адміністрація прийняла три нові директивні документи в інтересах забезпечення внутрішньої безпеки: «Національну стратегію боротьби з тероризмом» (The National Strategy for Combating Terrorism), «Національну стратегію щодо захисту кібер-простору» (The National Strategy to Secure Cyberspace) і «Національну стратегію фізичного захисту критичної інфраструктури». У них уперше отримала офіційне визнання «повна залежність інфраструктури США від інформаційних систем і мереж» та вразливість останніх. Крім того, вони націлюють уряд, промисловість, бізнес і суспільство в цілому на створення так званої єдиної національної системи реагування на кібернетичні атаки (National Cyberspace Security Response System) як сукупності територіальних, відомчих і приватних центрів аналізу й розподілу інформації (ISAC) у різних секторах економіки країни [59].

У структурі МВБ створено підрозділ кібернетичної безпеки (National Cyber Security Division – NCSD), головним елементом якого є новостворений за рахунок об"єднання трьох груп негайного реагування (CC/CERT, NCS, NTPC) центр екстреного реагування на комп"ютерні події в США (US Computer Emergency Response Team – US-CERT). Головними завданнями US-CERT визначено виявлення факту нападу (вторгнення) на інформаційну структуру США й видачу попередження (рекомендації) всім адміністраторам інформаційних систем країни протягом не більше ніж 30 хв із моменту виявлення загрози.

Основні завдання в галузі інформаційної безпеки відповідно до нової стратегії полягають у тому, щоб «запобігти кібернетичним нападам на критичну інфраструктуру, знизити вразливість нації до таких нападів, а також мінімізувати збитки й час відновлення». При цьому під кібертероризмом у США сьогодні розуміють «навмисне руйнування, переривання або спотворення даних у цифровій формі або потоків інформації, що мають далекосяжні політичні наслідки в політичному, релігійному або ідеологічному плані». У цілому стратегія інформаційної безпеки втілюватиметься в життя за класичною схемою системи цивільної оборони: навчання, попередження, оповіщення й ліквідація наслідків [51].

Відповідно до статті 1502 Закону про внутрішню безпеку, глава МВБ представив президенту план реорганізації цього міністерства в термін до вересня 2003 р. Ним передбачено закінчити всі необхідні організаційно-штатні заходи й повністю забезпечити роботу МВБ як органу, відповідального за безпеку громадян, сухопутних і морських кордонів, об"єктів інфраструктури, усіх видів транспорту та інформаційних ресурсів США (на той час загальний штат МВБ вже нараховував 180 тис. службовців).

Уперше стратегію забезпечення внутрішньої безпеки розроблено й оприлюднено ще в рамках АВБ у липні 2002 р. Той факт, що вона була прийнята незабаром після теракту 11 вересня, істотно вплинув на запропоноване в документі визначення поняття «внутрішня безпека». Як заявив Дж. Буш, «нація в небезпеці, наше суспільство є практично нескінченним набором потенційних цілей, удару по яких може бути завдано різними методами». Саме тому однією з ключових завдань стратегії став захист критично важливих інфраструктур. Причому одним з основних напрямів такої діяльності визнано захист кіберпростору.

Завдання розробки комплексного плану захисту критично важливих об‟єктів інфраструктури відображено в президентській директиві 2003 р. «Визначення критичної інфраструктури, розстановка пріоритетів і захист». У цьому документі Міністерство внутрішньої безпеки названо провідним національним відомством у цій сфері. Слідуючи вказівкам, МВБ за сприяння представників приватного бізнесу виробили Національний план захисту інфраструктури (National Infrastructure Protection Plan – NIPP), у якому підкреслено, що стан американської економіки й національної безпеки значною мірою залежить від працездатності інформаційних систем, які широко використовуються громадськими службами США [40].

NCSD створено в червні 2003 р. на базі управління безпеки критично важливих інфраструктур, Національного центру із захисту інфраструктури, федерального центру реагування на комп‟ютерні збої й низки інших структур. У його завдання входять міжвідомча координація та налагодження взаємодії з приватним сектором і зарубіжними партнерами у сфері забезпечення інформаційної безпеки. Технічну підтримку забезпечувала US-CERT. В обов‟язки цього підрозділу входять аналіз і виявлення джерел кіберзагроз та вразливих місць, а також поширення інформації про зміну рівня такої загрози. Крім того, US-CERT координує дії з відновлення федеральних комп‟ютерних мереж і систем після збоїв та кібератак.

Збір розвідувальних даних із комп‟ютерних систем противника дає змогу отримувати про нього дані стратегічного й оперативного характеру та виявляти вразливі місця в його інформаційних системах.

У США на офіційному рівні визнають, що контроль над секретними комунікаціями противника за одночасного захисту своїх власних надає їм унікальні можливості для збереження лідируючих позицій у світі.

Відповідно до президентського указу № 12333 від 4 грудня 1981 р. всі питання, пов‟язані з забезпеченням доступу до секретних або шифрованих даних інших держав і захистом своїх інформаційних ресурсів від засобів технічної розвідки, перебувають у віданні Управління національної безпеки/Центральної секретної служби (УНБ/ЦСС). УНБ формально працює в рамках міністерства оборони, однак насправді є одним із ключових елементів американського розвідувального співтовариства. ЦСС при цьому відіграє роль координатора між агентством і тими структурами МО, які займаються питаннями криптоанализа. Основними завданнями УНБ є ведення радіотехнічної розвідки, криптоаналіз і захист федеральних комунікаційних та інформаційних систем від загроз, що виходять від інших держав. Нині агентство відповідає за захист комп‟ютерних мереж, що належать федеральним міністерствам і відомствам, від можливих атак.

Роботу УНБ сконцентровано на двох напрямах: ведення радіо- й радіотехнічної розвідки (Signal Intelligence – SIGINT), якою займається відповідне управління (Signal Intelligence Directorate – SID), і забезпечення безпеки інформації (Informational Assurance – IA), що перебуває у віданні Управління інформаційної безпеки (Information Assurance Directorate – IAD).

Одним із найбільш відомих і таких, що привернули увагу широкої громадськості, проектів УНБ є глобальна система перехоплення даних «Ешелон». Довгий час саме її існування американською владою ретельно приховувалося та й сьогодні відкрита інформація про неї досить обмежена. Проте у звіті тимчасового комітету Європарламенту (2001) факт існування цієї системи переконливо доведено. За даними звіту, система створювалася в рамках угоди між США і Великобританією. Крім них, у проекті брали участь Канада, Австралія та Нова Зеландія.

Можливості перехоплення інформаційних комунікацій залежать від того, які системи використовуються – радіорелейні, супутникові, тропосферних, кабельні або оптоволоконні. До 50-х років минулого століття для військового та дипломатичного інформаційного обміну застосовували переважно короткохвильові радіопередавачі. Із 60-х років із цією метою задіюються супутники зв‟язку, виведені на геостаціонарні орбіти. На думку більшості дослідників, саме для перехоплення супутникових комунікацій і призначена система «Ешелон».

У принципі розміщення станцій забезпечує перехоплення всіх інформаційних супутникових комунікацій. Однак вони стали відігравати значно меншу роль у результаті початку широкої експлуатації оптоволоконних ліній зв‟язку. Для прослуховування цих комунікацій потрібно безпосередньо підключатися до ліній, а отже, станції радіоперехоплення в цьому випадку абсолютно марні.

Виявлення, оповіщення й реагування на виникаючі кібернетичні загрози, а також розробку систем шифрування для безпечного інформаційного обміну між системами в рамках УНБ покладено на Управління інформаційної безпеки. IAD проводить сертифікацію для користувача систем безпеки (здійснюючи тим самим підтримку операціям із забезпечення безпеки), а також оцінку комерційного програмного й апаратного забезпечення на відповідність державним стандартам. Воно ж координує розробку систем забезпечення інформаційної безпеки для глобальної «інформаційної решітки», створюваної міністерством оборони.

У зв‟язку з цим інтерес викликають дослідні роботи, проведення яких у 2009 р. запланувало Управління перспективних досліджень МО (Defense Advanced Research Projects Agency – DARPA). Одне з них – так звана глобальна інформаційна решітка, або бездротова мережа наступних поколінь (The Wireless Network after Next – WnaN, Global Information Grid-GIG).

Планування й реалізація операцій у глобальних комп‟ютерних мережах здійснюються відповідно до концепції «сетецентрической операции» – *рос.* (Net-Centric Operations). Основою для сітьоцентрових операцій є глобальна інформаційна мережа (глобальна інформаційна решітка) GIG (Global Information Grid) міністерства оборони США, що становлять набір взаємозалежних високо захищених локальних інформаційних мереж. Вона оптимізує процеси збору, обробки, зберігання, розподілу інформації та управління нею, а також доведення її до споживачів усередині міністерства оборони й за його межами. За допомогою GIG здійснюється як адміністративне, так і оперативне управління збройними силами США. Головним відомством, відповідальним за працездатність і захист глобальної інформаційної мережі військового відомства, призначено об‟єднане стратегічне командування американських ВС [54].

На початку 2008 р. президент США Дж. Буш підписав дві секретні директиви – № 54 (із національної безпеки) і № 23 (із внутрішньої безпеки). У цих документах спецслужбам країни, передусім МВБ, а також УНБ, даються вказівки щодо посилення контролю за комп‟ютерними мережами, використовуваними американськими федеральними структурами. Крім того, заокеанські розвідники й контррозвідники повинні розширити сфери моніторингу інформації, що надходить у мережі урядових відомств Сполучених Штатів через Інтернет.

За новими директивами Пентагону дозволено розробляти плани проведення кібернетичних контратак на інформаційні мережі супротивників США. У тих випадках, коли УНБ буде встановлено конкретний факт нападу та виявлено сервер іноземної держави, із якого здійснено атаку, фахівці Міноборони завдадуть по ньому удару у відповідь, щоб запобігти новим атаки на інформаційні мережі американського уряду.

У питаннях забезпечення інформаційної безпеки УНБ працює в тісному зв’язку з МВБ. Так, у 2004 р. ЦСС і підрозділ кібернетичної безпеки домовилися про спільну розробку навчального курсу з інформаційної безпеки для центру підвищення кваліфікації персоналу агентства. У 2008 р., відповідно до президентської директиви, УНБ названо провідною організацією з моніторингу та захисту федеральних урядових мереж від кібертероризму.

Мережеві комп‟ютерні атаки охоплюють весь спектр дій, спрямованих на порушення або знищення інформації, що міститься в комп‟ютерах або комп‟ютерних мережах противника. При цьому власне інформаційні потоки безпосередньо використовуються як зброя. Наприклад, передавання інформаційного пакета з командою відключити електроенергію є атакою саме такого виду, тоді як генерація стрибка напруги в мережі живлення, у результаті чого буде знеструмлена комп‟ютерна система противника, належить уже до категорії електронної боротьби.

Сумніви в ефективності й передбачуваності наслідків мережевих операцій стали предметом обговорення на нараді урядовців та експертів у Массачусетському технологічному інституті в січні 2003 р. Заклопотаність політиків викликала перспектива виникнення транскордонного каскадного ефекту під час здійснення кібератак, спроможного порушити функціонування цивільних комп‟ютерних систем. Багато в чому керуючись результатами цієї дискусії, президент США в лютому 2003 р. видав директиву № 16 із питань національної безпеки, яка регламентує умови, за яких Сполучені Штати можуть почати мережеву атаку проти комп‟ютерних систем іншої держави. У ній також визначено посадових осіб, повноважних приймати рішення про проведення таких операцій.

За даними Пентагону, лише у 2007 р. зареєстровано близько 44 тис. інцидентів, які кваліфіковано як кібернетичні злочини, учинені іноземними арміями, спецслужбами й окремими особами.

Одним із найбільш великих таких випадків стало розкрадання кількох терабайт даних про розроблюваний у США багатоцільовий винищувач-бомбардувальник п‟ятого покоління F-35 «Лайтнінг-2». Вартість проекту бойового літака становить близько 300 млрд дол. Передбачено, що дані викрадено із серверів компаній-підрядників.

У грудні 2006 р. КНШ підготував документ «Національна військова стратегія кібернетичних операцій» (на сьогодні частково розсекречений), який серед іншого визначив стратегічні пріоритети проведення операцій для забезпечення інформаційної безпеки США:

– досягнення та утримання ініціативи в ході операцій, що проводяться всередині циклу прийняття рішення противником;

– забезпечення захисту власних комп‟ютерних систем і виконання наступальних дій у комп‟ютерних мережах противника;

– уключення операцій у кіберпросторі в систему військового планування для всього спектра збройних конфліктів задля вироблення методів ведення таких операцій (з урахуванням особливостей різних ТВД) у тісній взаємодії з видами ЗС й управліннями МО, які, зі свого боку, повинні погоджувати свої дії з іншими відомствами США, союзниками по коаліції й промисловими підрядниками;

– створення в рамках міністерства оборони необхідних умов для проведення кібернетичних операцій, уключаючи організаційні заходи, підготовку фахівців і створення відповідної інфраструктури;

– оцінка ризиків мережевих операцій, які можуть виникнути через недостатньо ефективний підбір засобів або зустрічного застосування противником вразливих місць у кіберпросторі США, а також внаслідок побічного ефекту від проведення наступальних операцій.

Очевидно, що зазначені пріоритети мають загальний характер і лише намічають орієнтири для майбутніх операцій у кіберпросторі.

На початку березня 2008 р. в Сполучених Штатах пройшли навчання під кодовою назвою «Кібершторм-2». Їх проводило МВБ за участю 18 федеральних відомств, у тому числі ЦРУ, ФБР, МО (ОСК ВС США) й УНБ, представників дев‟яти американських штатів і понад трьох десятків приватних компаній, а також відповідних служб Австралії, Великобританії, Канади й Нової Зеландії. Командний пункт навчань розмістився, як повідомляється у штаб-квартирі секретної служби США, яка відповідає за безпеку глави держави та структурно входить до складу МВБ. «Імовірний противник» не позначався, однак вважалося, що він переслідує політичні й економічні цілі і для їх досягнення зробив потужну кібератаку проти США та їхніх союзників. У ході навчань учасники відпрацьовували спільні дії, покликані дати відсіч цьому нападу.

Незважаючи на те, що багато питань, котрі стосуються проведення таких операцій, залишаються незрозумілими досі, військове відомство „США практично одночасно з прийняттям національної військової стратегії кібернетичних операцій почало обговорювати заходи зі створення відповідних підрозділів. У листопаді 2006 р. начальник штабу ВПС США М. Мослі оголосив про плани створення кібернетичного командування цього виду ВС. Очікувалося, що воно зможе почати функціонувати в повному обсязі з жовтня 2008 р., у зв‟язку з чим на перехідний період вирішено сформувати тимчасове кіберкомандування.

Однак через відсутність у Пентагоні й держдепартаменті США єдиних поглядів щодо питань забезпечення інформаційної безпеки, а також через боротьбу різних видів національних ЗС за підпорядкованість їм новостворюваних структур це командування реально так і не запрацювало.

Розвиток кіберпростору став одним з основних пріоритетів, коли прийшов до влади на початку 2009 р. президент США Б. Обама, котрий повернувся до проекту створення кіберкомандування, істотно підвищивши його рівень, але вже не в структурі військово-повітряних сил США, а в рамках ОСК ВС США.

Після свого обрання президент Б. Обама ознайомився з доповіддю Управління національної розвідки США «Глобальні перспективи-2025», у якій міститься висновок про «назрілу необхідність вжиття заходів протидії інформаційним загрозам», а також про те, що ці загрози повинні розглядатися на рівні національної безпеки країни.

До аналогічного висновку прийшли автори іншої доповіді, підготовленої в Центрі стратегічних і міжнародних досліджень та безпосередньо присвяченої політиці кібербезпеки, що проводиться Білим

домом на сьогодні. У ньому президенту Б. Обамі рекомендується вжити невідкладних заходів, аби не допустити щодо цього напряму загострення загрози національній безпеці. Дії нової адміністрації свідчать про те, що вона відносить інформаційні загрози до рівня національної безпеки. Так, у кінці лютого 2009 р. президент направив у конгрес проект федерального бюджету на 2010 р., у якому позначено контури витрат на розвідувальну діяльність («Національні розвідувальні програми»), що забезпечує ключові елементи національної безпеки США. У цьому документі загрози федеральним інформаційно-технологічним мереж характеризуються як реальні, серйозні й наростаючі, а завдання зміцнення кібербезпеки на федеральному рівні стоять на другому місці.

Можна сказати, що реформа системи забезпечення інформаційної безпеки фактично почалася з найперших днів повноважень нового президента. Значно підвищилася роль міністерства внутрішньої безпеки, агентства національної безпеки, ради з національної розвідки, ЦРУ та інших спеціальних служб. Одночасно з реформою системи забезпечення інформаційної безпеки адміністрацією Б. Обами прийнято також інші організаційні й законодавчі заходи, спрямовані на закріплення за Сполученими Штатами статусу інформаційної супердержави [55].

У травні 2009 р. офіційні представники Пентагону оголосили про намір створити нову структуру – командування бойових дій у кіберпросторі, яке покликане забезпечити безпеку не лише військових, а й цивільних інформаційних систем.

На слуханнях в комітеті з питань збройних сил палати представників США директор УНБ заявив, що нове командування поєднуватиме оборонні й наступальні інформаційні засоби МО та агентства національної безпеки. Крім того, за допомогою створюваного органу УНБ планує підтримувати міністерство внутрішньої безпеки, у чиї обов‟язки нині входить забезпечення інформаційної безпеки країни. При цьому агентство не хоче брати на себе настільки великі повноваження й зобов‟язання, однак цілком спроможне допомогти МВБ. Аби більш ефективно протистояти інформаційним загрозам, військові повинні тісніше співпрацювати з приватним сектором і МВБ.

23 червня 2009 р. міністр оборони Роберт Гейтс опублікував меморандум, у якому дано вказівку створити командування бойових дій у кіберпросторі. Саме на нього, на думку Гейтса, буде покладено відповідальність за захист військових комп‟ютерних мереж і проведення наступальних кібероперацій проти сил противника.

Штаб нового командування розміщений у Форт-Мід (штат Меріленд), поблизу м. Вашингтона. Структурно воно входить в ОСК ВС США і є сполучним елементом між УНБ і підрозділами міністерства оборони.

Під свій захист кібернетичне командування бере військові системи Сполучених Штатів – 15 тис. електронних мереж, близько 7 млн комп‟ютерів й інші інформаційно-технологічні служби. Інші ж урядові або приватні комп‟ютерні мережі залишаться за рамками його відповідальності.

Функції командувача «кібернетичними силами» покладено на главу управління Національної безпеки генерала Кейта Александера, який одночасно зберіг і свою посаду директора УНБ. Служби цього управління також зосереджені у Форт-Мід.

Американська адміністрація вважає, що формування єдиної глобальної інформаційної інфраструктури під контролем США дасть їм змогу виконати завдання стратегічного використання інформаційної зброї «аж до блокування телекомунікаційних мереж держав, які не визнають реалії сучасної міжнародної системи».

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Потрібно відзначити, що нині застосування інформаційних технологій у військових цілях фактично не регулюється міжнародним правом. На думку зарубіжних експертів, ці питання повинні розглядатися й вирішуватися на багатосторонній основі за участю всіх зацікавлених сторін. При цьому Управління інформаційним простором потрібне для забезпечення не лише національної безпеки абсолютного ІТ-лідера-США, але й міжнародної безпеки загалом. Однак із цих питань США займають особливу позицію та діють відповідно до домовленостей. Водночас США не відмовляються від планів реалізації своєї інформаційної переваги, хоча одна з основних тез стратегії проведення кібернетичних операцій – необхідність налагодження взаємодії видів збройних сил – із самого початку виявилася важковиконуваною. Можливо, це спричинить глибокий перегляд усього комплексу проблем,

пов‟язаних зі здійсненням кібератак. Розглядаючи практику забезпечення інформаційної безпеки США, можемо зробити висновки, що держава є провідною в цій сфері та в результаті співпраці з іншими країнами G7 надає консультації й поради щодо врегулювання цих питань і вирішення загрозливих ситуацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фергюссон Н. Империя. Становление и упадок британского мирового порядка и уроки для глобальной власти. Космополис. 2003. № 3. С. 66–79.
2. Cleveland. The knowledge executive. Leadership in an information society. New York: Truman Telley books, 1989. P. 32.
3. Connection Community Content: The Challenge of the Information Highway. Final Report of the Information Highway Advisory Council. URL: http://www.abebooks.co.uk/9780662237945/Connection-Community-Content-Challenge-lnformation0662237943/plp.
4. Irwin Barry V. W. Standing your ground: current and future challenges in cyber defense. Theories and Intricacies of Information Security Problems. Potsdam: Universitätsverlag, 2013. P. 100–108.
5. Kiountouzis E. A, Kokolakis S. A. Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd., 2008.
6. Pipkin D. Information security: Protecting the global enterprise. New York: Hewlett-Packard. Company, 2000.

Матеріал надійшов до редакції 26.12.2019 р.

TO THE QUESTION OF THE BASICS OF US INFORMATION AND CYBER SECURITY

The paper considers the components of the state information policy to ensure the information security of the country and identifies the main activities of public authorities in this area. The internal and external information threats to the national security of the G7 countries and the ways of guaranteeing the information security of the countries are analyzed. Information security is seen as a component of national security, as well as a global problem of information protection, information space, information sovereignty of the country and information support of government decision-making. Approaches to ensure the process of continuity of the information security system of the state in order to monitor new threats, identify risks and levels of their intensity are proposed.
Key words: state, policy, security, threats, resources, USA.

REFERENCES

1. Ferguson, N. (2003). Empire. The rise and fall of the British world order and lessons for global power. Cosmopolis, 3, 66–79.
2. Cleveland (1989). The knowledge executive. Leadership in an information society. New York: Truman Telley books, 32.
3. Connection Community Content: The Challenge of the Information Highway. Final Report of the Information Highway Advisory Council. URL: http://www.abebooks.co.uk/9780662237945/Connection-Community-Content-Challenge-lnformation0662237943/plp.
4. Irwin Barry, V. W. (2013). Standing your ground: current and future challenges in cyber defense. Theories and Intricacies of Information Security Problems. Potsdam: Universitätsverlag, 100–108.
5. Kiountouzis, E. A., Kokolakis, S. A. (2008). Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd.
6. Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard. Company.