2. Скворцов С. І. Адміністративно-правове регулювання адміністративного нагляду за особами, звільненими з місць позбавлення волі: дис. ... канд. юрид. наук: 12.00.07 «Адміністративне право і процес, фінансове право, інформаційне право». МВС України, НАВС. К.: 2018. 215 с.

3. Павлик Р. І. Відмінність понять «державний контроль» і «державний нагляд»: нормативно-правовий аспект. *Демократичне врядування.* 2017. № 20. URL : http://lvivacademy.com/vidavnitstvo_1/visnyk20/fail/Pavlyk.pdf.

4. Ковальов С. І. Запобігання міліцією порушенням правил адміністративного нагляду особами, звільненими з місць позбавлення волі. *Вісник Запорізького нац. ун-ту.* 2010. №4. С. 142–146.

5. Ягунов Д. В. Електронний моніторинг в пенальних практиках зарубіжних країн та перспективи його запровадження до національної системи кримінальної юстиції. *Актуальні проблеми політики.*. Одеса: Фенікс. 2012. № 46. С. 184–193.

6. Марчук А.І. Напрямки реформування контрольних повноважень Національної поліції щодо осіб, звільнених з місць позбавлення волі, з урахуванням позитивного зарубіжного досвіду. Одеса: Видавничий дім «Гельветика». 2017. С. 264–267.

7. Про пробацію: Закон України від 5 лютого 2015 р. № 160-VIII. *Відомості Верховної Ради України.* 2015. № 13. Ст. 93. (Дата звернення: 19.03.2020).

8. Денисова А. В. Систематизація видів і суб'єктів адміністративного нагляду органів виконавчої влади. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція*. 2017. № 27. С. 22–25.

9. Петренко О. А. Суть адміністративного нагляду міліції за особами, звільненими з місць позбавлення волі, в системі адміністративного примусу. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2012. № 1. С. 323–332.

УДК 351.746.1:004.056.5(73)(045)

ІНФОРМАЦІЙНА БЕЗПЕКА США: ПРОБЛЕМИ ТА ВИКЛИКИ В ДОБУ ДОНАЛЬДА ТРАМПА

І. О. Черновол, І. Ю. Чарських

Анотація. Дане дослідження акцентує увагу на актуальних проблемах та викликах інформаційній безпеці США за адміністрації Дональда Трампа. Надано стислу інформацію стосовно поняття інформаційної безпеки, історії розвитку систем її захисту, наявних суперечок між двома основними політичними партіями США щодо реалізації інформаційної безпеки, а також російського втручання в американський електоральний процес. На основі системного підходу, з використанням методу критичного аналізу досліджено основні проблеми, загрози та виклики інформаційній безпеці США, окреслено можливі шляхи їх вирішення.

Ключові слова: інформаційна безпека США, Д. Трамп, міжпартійні суперечки, російське втручання.

Вступ. На початку XXI ст. залежність людства від інформації стала беззаперечною, оскільки розвиток інформаційних технологій зумовив проникнення інформаційних ресурсів практично в усі сфери життєдіяльності людини, що викликало збільшення та ускладнення загроз інформаційній безпеці. Навмисний або випадковий вплив, який послаблює останню, може стати серйозною загрозою національній безпеці держави, безпеці особистості і суспільства в цілому. Ретроспектива у вивченні ролі інформаційного протиборства у міжнародних відносинах дозволила науковцям виробити концептуальну базу для подальших досліджень інформаційної безпеки держави та її захисту. В умовах бурхливого розвитку інформаційного суспільства та становлення постіндустріального способу виробництва інформаційне протиборство стало невід'ємною частиною міждержавних відносин.

Сполучені Штати Америки – сильна країна, один зі світових економічних та технологічних лідерів, держава з потужним військово-промисловим комплексом, вагомий гравець у геополітичних відносинах на світовій арені. Без сумніву, це держава з надзвичайно розвинутим інформаційним сектором економіки та значними бюджетними і корпоративними витратами на нього. Закономірно, що настільки благополучний суб'єкт і лідер інформаційно-технологічної гонки став одним з основних об'єктів інформаційних

атак з боку «недоброзичливих сусідів» – інших країн, державних/недержавних акторів міжнародних відносин, зокрема – хакерських, терористичних угрупувань тощо. В результаті виявилися потенційно вразливі місця інформаційної сфери, а саме – небезпечний когнітивний вплив у негативній конотації з боку певних засобів масової інформації та соціальних мереж на суспільну думку всередині країни, а також прогалини в сфері захисту персональних даних, державних та приватних комп'ютерних мереж. Це зумовило виникнення потреби в захисті інформації, критично важливих даних та національної інформаційної інфраструктури в цілому від посягань з боку інших суб'єктів, які підривають стабільність країни та можуть призвести до дестабілізації певних ключових сфер державного значення і, як наслідок, спричинити падіння державного іміджу перед світовою спільнотою на міжнародній арені та поставити під сумнів демократію як одну із основних ідеологічних засад США.

Американській державі потрібно виробити єдину лінію протиборства інформаційним наступам і вона тут має багаті традиції, проте внутрішні непорозуміння між республіканцями й демократами та зовнішні загрози у вигляді навмисного іноземного втручання в інформаційну сферу гальмують даний процес, перетворивши його на гонку за політичними «дивідендами».

Актуальність даного дослідження полягає у вищевказаних наявних чітких проблемах і загрозах інформаційній безпеці Сполучених Штатів. Проблема захисту інформаційної безпеки США широко досліджується в американських та вітчизняних науково-концептуальних та суспільно-політичних колах Зокрема, Д. Альперович, Е. Накашіма, П. А. Афанасьєва, Н. Б. Бєлоусова, О. Ю. Бусол, О. В. Олійник, О. А. Собко, І. Р. Боднар, О. П. Дзьобань, В. Жуган, В. Пашков, О. М. Косогов, М. Маззетті, Дж. Маркс та інші присвятили свої дослідження проблемам реалізації інформаційної безпеки у США в умовах глобалізації суспільства та зростання інформаційних загроз. Проте, відсутність достатньої кількості досліджень даної проблеми, з точку зору врахування певних особливих факторів, таких як існування суперечок між двома альтернативними політичними осередками – республіканцями й демократами з приводу питання реалізації інформаційної безпеки та російського втручання у виборчий процес й власне вибори президента США у 2016 році, дає можливість вивчати її з іншого ракурсу.

Основна частина. Питання інформаційної безпеки сьогодні є одними з найбільш дискусійних та провокаційних в обговореннях політиків, економістів, програмістів, науковців, простих людей, експертів і аналітиків з усіх сфер суспільно-громадського життя країн, їх угрупувань та світу в цілому. З концептуальної точки зору, поняття інформаційної безпеки настільки багатоманітне, що потребує дослідження у нерозривному зв'язку не лише з традиційними поняттями «інформація», «інформаційний ресурс», «інформаційна зброя» та «інформаційна війна», а й такими категоріями, як «суспільна свідомість», «когнітивна безпека», «когнітивна зброя», «інформаційна стратегія», «рівень секретності», «рівень інформаційної потужності».

Інформаційною безпекою вважають сукупність вимог і характеристик життя, що створюють як відчуття так і, – головне, – реальне надійне збереження інформаційних ресурсів і таємниць держави та захист конституційних прав особистості й громадськості в інформаційно-технологічній сфері від різного роду загроз та посягань. Можна сказати, що інформаційна безпека – це співвідношення між ступенем негативного впливу зовнішніх загроз та ефективністю їх попередження і нейтралізації з боку людини, суспільства, держав і державних союзів.

Інформаційну безпеку та інформаційне домінування по праву можна назвати ключовими напрямами економіко-технологічного, науково-виробничого та військово-політичного лідерства США у світі. Державна політика США у сфері інформаційної безпеки пройшла тривалий еволюційний шлях, який складається з чотирьох етапів:

1 етап: виникнення – 1939–1947 рр.;

2 етап: становлення – 1947–1982 рр.;

3 етап: активний розвиток – 1983–2001 рр.;

4 етап: докорінне вдосконалення – 2001 р. – дотепер [1].

Особливістю «спадковості» політики захисту інформаційної безпеки в США є абсолютна її відсутність, тобто кожна нова президентська адміністрація пропонувала і реалізовувала свої тактичні і стратегічні дії. Говорити можна лише про найзагальніші спільні риси. Це пояснюється тим, що інформаційна політика за своєю природою виникає на основі стратегії національної безпеки, військової доктрини, зовнішньополітичної доктрини, а вони істотно різняться у впровадженні політичних курсів різних американських президентів. Так чи інакше, сьогодні США мають вирішити найскладнішу задачу інформаційного протиборства новим технологічним лідерам, котрі все частіше не керуються принципами демократії та міжнародного права. Задача ускладнюється наявністю внутрішніх політичних суперечок та конфліктів.

Національна безпека США зазвичай визначається документом, який носить назву Стратегія національної безпеки США (The National Security Strategy of the USA – далі NSS), розробляється окремо адміністрацією кожного нового президента та інтегрує зовнішню політику, національну оборону, міжнародні економічні відносини та політику допомоги у розвитку. Остаточно версія нової NSS побачила світ у грудні 2017 р. і виявилася однією з найдовших стратегій в історії США – принаймні, – майже вдвічі довшою, ніж попередня, опублікована у 2015 році [2]. Окрім того, вирізняє даний документ і той факт, що він був представлений ще до того, як закінчився перший рік діяльності адміністрації Д. Трампа. Звичайно, це досить бажано, з одного боку, однак видається практично неможливим у зв'язку із тими труднощами, що супроводжували його створення. Як показує практика, раніше підготовка таких документів вимагала набагато більше часу, а враховуючи складність поточного міжнародного сценарію – вимагала б ще довшої та ретельнішої розробки.

Після опублікування Стратегії національної безпеки адміністрація Д. Трампа була розкритикована, оскільки документ, хоч і визначав інформаційну безпеку одним із головних пріоритетів країни, не передбачав реальних заходів для її досягнення, прозаявляв, зокрема, представник Демократичної партії екс-губернатор штату Кентуккі Стівен Бешар [3].

В рамках розпорядження президента від 11 травня 2017 року №13800 «Посилення кібербезпеки федеральних мереж і критичної інфраструктури» було розроблено нову Національну кіберстратегію (The National Cyber Strategy of the USA – далі NCS), яка була опублікована у вересні 2018 року [4]. Даний документ містить цілі, подібні до тих, що поставлені у попередніх схожих документах: політикою у сфері кіберпростору адміністрації Б. Обами 2009 [5] та Національною стратегію безпеки Дж. Буша 2002 [6] щодо безпеки кіберпростору. Однак, незважаючи на схожість з планами попередніх адміністрацій, NCS Д. Трампа знову викликала критичні відгуки зі сторони його опонентів, оскільки замість того, щоб продовжувати концепцію зміцнення захисних технологій і мінімізувати вплив інформаційних загроз, адміністрація президента планує посилити наступальні попереджувальні кібероперації та змусити інші країни боятися притягнення до відповідальності за свої дії у відповідь на такі кібератаки зі сторони США. Також критики звернули увагу на той факт, що дана стратегія жодним чином не вказує на можливості щодо захисту виборів від інформаційних загроз, що є надзвичайно актуальним в світлі подій 2016 р. [7].

В американському політикумі апогеєм порушення проблеми захисту інформаційної безпеки Сполучених Штатів та символічною точкою відліку при її сучасному описі вважається російське втручання у американські президентські вибори 2016-го року. Це безпрецедентне явище, оскільки така масштабна кампанія з боку Росії, що була з успіхом проведена, мала місце вперше в контексті історії інформаційної безпеки США. Це був вагомий удар не тільки для інформаційної сфери та національної безпеки країни, але й для американської ідеології та іміджу.

Представники американських владних структур та розвідувальні служби неодноразово заявляли, що авторитарна Росія намагалася вплинути і вплинула на вибори президента США. Так, у червні 2016 року в американських мас-медіа з'явилася інформація про несанкціоноване втручання в інформаційну систему Національного комітету Демократичної Партії США, особливо було згадано російське «Агенство інтернет-досліджень» (далі IRA), яке фінансувалося Євгеном Пригожиним (російський бізнесмен, засновник «фабрики тролів» з Ольгіна, одна з ключових фігур в російсько-українській інформаційній війні) [8]. Для багатьох американців таке втручання в інформаційний простір їх країни виявилося несподіванкою, хоча для російської влади – це була довгоочікувана спланована атака, яку вона вважала виправданою роками подібних провокацій з боку Сполучених Штатів. Відомо, що кандидатури Г. Клінтон і Д. Трампа до останнього йшли у виборних перегонах з невеликим відривом, і демократи припускають, що якщо б не багаторазове «порушення» кампанії Клінтон електронними листами, викраденими російськими хакерами і опублікованими на WikiLeaks та анти-Клінтонівські повідомлення, об'єктивно спрямовані на підтримку Трампа і розповсюджувані за допомогою соціальних мереж російськими IT-фахівцями, то ситуація могла би змінитись. Однак, президент Трамп та його адміністрація категорично не погоджуються із цією думкою [9].

У 2017 році було розпочато розслідування фактів російського втручання у вибори, яке очолив спеціальний прокурор Роберт Мюллер. Розслідування було ініційовано на основі заяв про те, що в період президентської кампанії та перехідного періоду між російськими оперативниками та командою Трампа існувала змова. До розслідування були залучені такі структури, як ФБР, Комітет Сенату з питань розвідки, Постійний окремий комітет з питань розвідки, Судовий підкомітет Сенату з питань злочинності та тероризму, Комітет Палати з питань нагляду та реформування уряду, Судовий комітет Сенату. За результатами розслідування було виявлено, що російське втручання у вибори здійснювалося за трьома напрямками: викрадення та оприлюднення документів основних опонентів Д. Трампа; масове шахрайство на Facebook і Twitter з акаунтами з метою анти-пропаганди Г. Клінтон; спроби співпраці з кампанією Д. Трампа [10]. Варто підкреслити, що остання теза не знайшла підтвердження, згідно з «Доповіддю Мюллера», який провів майже два роки на чолі комісії фахівців, розслідуючи зусилля Москви саботувати президентські вибори у США, й оприлюднив свій звіт щодо даної справи, де заявив, що не виявив змови, «незважаючи на численні пропозиції від російських осіб, які допомагали кампанії Трампа» [11].

Проте, згідно даного звіту, було виявлено досить багато цікавих фактів. Наприклад, з червня 2016 року IRA за допомогою заклику у соцмережах організовувала передвиборчі мітинги в США на підтримку Трампа і на протидію кампанії Клінтон. Члени IRA видавали себе за американців. Використання соціальних мереж російськими агентствами для поширення пропагандистського контенту було дуже широким: Facebook, Twitter, Reddit, Pinterest, YouTube, Google+ та інші соцмережі. Найбільш часто використовуваною платформою був Instagram. Також, в звіті говориться про діяльність російської розвідки (ГРУ), яка зламала облікові записи електронної пошти, що належали добровольцям і працівникам президентської кампанії Клінтон, включаючи обліковий запис голови кампанії Дж. Подеста, а також пошкодила комп'ютерні мережі комітету Демократичної партії у Конгресі і Національного комітету Демократичної партії. Використовуючи шкідливі програми для вивчення комп'ютерних мереж, російські хакери зібрали десятки тисяч електронних листів і вкладень, а також видалили комп'ютерні журнали і файли, щоб приховати докази своєї діяльності. Викрадена інформація була збережена і оприлюднена поетапно протягом трьох місяців напередодні виборів 2016 року [11].

Відповідно до аналізу, здійсненого Buzzfeed, 20 найпопулярніших хибних передвиборних публікацій з фальшивих сайтів і блогів викликали більше 8,5 мільйонів відгуків та коментарів у Facebook [12].

У рекламних оголошеннях в соцмережах, які розміщувалися у період з червня 2015 року по травень 2017 року, основна увага приділялася соціальним питанням, які

роз'єднували суспільство. Було задіяно близько 3000 рекламних оголошень, які переглянули від чотирьох до п'яти мільйонів користувачів Facebook до виборів [13].

Загалом, серед основних проблем, з якими стикаються США у сфері інформаційної безпеки можна виділити такі: зростання встановлення зловмисних програм (вірусів) на мобільні пристрої, поширення вірусів шляхом розповсюдження у магазинах неліцензійного програмного забезпечення, викрадення акаунтів та особистих даних. Так, встановлення вірусних програм на мобільні пристрої протягом 2018 року збільшилося на 45%. Дослідження проведене компанією Symantec показало, що у магазинах, які розповсюджують програмне забезпечення сторонніх розробників, виявлено 99,9% зловмисних програм, що можуть отримувати доступ до персональних даних. Саме на протязі 2018 року у США було викрадено близько 12 млрд. акаунтів, що містили особисту інформацію, включаючи адресу, номер телефону, номер страхування чи інформацію про кредитну картку. Більш того, у тому ж 2018 році, 45 млн. американців постраждали від викрадення особистих даних, ця цифра значно збільшилася у порівнянні з 2017 роком, в якому 17 млн. споживачів постраждали від викрадення особистої інформації з метою її подальшого використання задля збагачення крадіїв [14].

Окремого занепокоєння викликає питання захищеності та готовності сектору інформаційної безпеки протистояти майбутнім загрозам з боку потенційно зацікавлених сторін (країн, недержавних організацій, окремих осіб тощо). Особливого значення дана проблема набуває в контексті захисту виборчого процесу та власне самих виборів президента США, які мають відбутися восени 2020 року. Наразі вона набирає значної популярності в обговореннях політиків, економістів, програмістів, науковців, простих людей, експертів і аналітиків, які цікавляться окресленою проблемою.

Висновки. На основі викладеного матеріалу бачимо чітко виокремлені проблеми та виклики, з якими Сполученим Штатам постійно доводиться мати справу, та які надходять як з середини держави, так і ззовні. Останні, комплексно мають значне дестабілізуюче значення для критично важливої інформаційної інфраструктури, а отже й складають серйозну загрозу національній безпеці держави, окремим індивідам та суспільству в цілому. Дану ситуацію можна назвати рефлексією по відношенню до малоефективної політики, яка проводиться урядом в контексті захисту даних та реалізації інформаційної безпеки від посягань, а також наявністю постійних міжпартійних суперечок, зокрема в Конгресі та мас медіа, які унеможливлюють певні конструктивні зрушення стосовно вирішення окресленої проблеми. Основним завданням уряду в таких умовах має бути вироблення та розвиток єдиного бачення державної політики щодо сфери інформаційної безпеки, з формуванням потужної системи захисту та постійним вдосконаленням останньої для протидії зовнішнім та внутрішнім загрозам. Такі кроки унеможливили б інформаційні атаки та когнітивний зовнішній вплив на громадськість в подальшій перспективі, за умови консенсусу між основними політичними силами США. До того ж, зосередженість державних, корпоративних та громадських учасників на подоланні спільної проблеми позитивно вплинула б на загальний стан справ Сполучених Штатів.

Аннотация. Данное исследование акцентирует внимание на актуальных проблемах и вызовах информационной безопасности США при администрации Дональда Трампа. Предоставлено краткую информацию относительно понятия информационной безопасности, истории развития систем ее защиты, имеющихся споров между двумя американскими основными политическими силами в отношении реализации информационной безопасности, а также российского вмешательства в американский электоральный процесс. На основе системного подхода, с использованием метода критического анализа исследованы основные проблемы, угрозы и вызовы информационной безопасности США, обозначены возможные пути их решения.

Ключевые слова: информационная безопасность США, Д. Трамп, межпартийные споры, российское вмешательство.

Abstract. This study focuses on the current problems and challenges of the US information security under the administration of Donald Trump. Brief information is provided regarding the concept of information security, the history of the development of its protection systems, the existing disputes between the two American main political

forces regarding the implementation of information security, as well as Russian interference in the American electoral process. Based on a systematic approach, using the method of critical analysis, the main problems, threats and challenges of US information security are investigated, possible ways to solve them are identified.
Key words: US information security, D. Trump, cross-party disputes, Russian intervention.

СПИСОК ЛІТЕРАТУРИ

1. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. URL : http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350
2. The White House. National Security Strategy of the United States of America. Washington DC, December 2017. 56 p. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
3. Укрінформ. Трамп ігнорує серйозні загрози для національної безпеки з боку Росії. URL : https://www.ukrinform.ua/rubric-world/2184991-so-i-ak-skazav-tramp-kongresu.html
4. The White House. National Cyber Strategy of the United States of America. Washington DC, September 2018, 29 p. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
5. The White House. Cyber Security Review. Washington DC, March 2009, 47 p. URL : https://obamawhitehouse.archives.gov/cyberreview/documents/
6. The White House. The National Security Strategy, Washington DC, September 2002. URL : https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/
7. Wolff J. Trump's Reckless Cybersecurity Strategy. URL : https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html
8. Жигалкин Ю. Доказательства вмешательства России в выборы президента США. URL : https://www.svoboda.org/a/usa-russia-indictment/29044968.html
9. Shane S., Mazzetti M. The plot of subvert the election: Unraveling the Russia story so far. URL : https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html
10. CNN. 2016 Presidential Election Investigation Fast Facts. URL : https://edition.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html
11. Mazzetti M., Bennet K. Mueller report summary. URL: https://www.nytimes.com/2019/03/24/us/politics/mueller-report-summary.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking
12. Boot M. Without the Russians, Trump wouldn't have won // Washington Post. December 27, 2018. URL: https://www.washingtonpost.com/video/editorial/opinion--heres-why-trump-wouldnt-have-won-without-russia/2018/07/30/e4098f1e-93ff-11e8-818b-e9b7348cd87d_video.html
13. Facebook Says Russian Accounts Bought $100,000 in Ads During the 2016 Election. // The New York Times. September 6, 2017. URL : https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html
14. Symantec Corporation. 10 cyber security facts and statistics for 2018. URL: https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

УДК 327-057.177(4-6ЄС)(410)(045)

ЄВРОСКЕПТИКИ ТА ЄВРООПТИМІСТИ У ЗОВНІШНІЙ ПОЛІТИЦІ ВЕЛИКОЇ БРИТАНІЇ

А. В. Шевченко, М. І. Прихненко

Анотація: У цій статті розглянуто євроскептичні та єврооптимістичні настрої британських політичних осіб, їх витоки та особливості, починаючи із закінчення Другої світової війни і до сьогодні, що трансформувались у зовнішньополітичну традицію держави. В процесі дослідження були використані наступні методи та підходи: системний підхід, який надав можливість розглянути явище, що вивчається у якості цілісної елементу, а також методи індукції та дедукції, проблемно-хронологічний метод та діалектичні методи дослідження. Автором зроблені висновки про формування та розвиток євроскептицизму та єврооптимізму в системі ідеологічних орієнтирів держави, що трансформувалась в елемент зовнішньої політики.
Ключові слова: Велика Британія, єврооптимізм, євроскептицизм, зовнішня політика Великої Британії

Відносини Сполученого Королівства з ЄС – або, політично кажучи, «Європою» – давно стали одними з найбільш розбіжних, емоційних питань у британській політиці. Ще навіть до того, як держава приєдналась до тодішнього ЄЕС, решта членів вважали їх надто