Міністерство освіти і науки України
Чернівецький національний університет
імені Юрія Федьковича

Факультет історії, політології та міжнародних
відносин
Кафедра міжнародної інформації

СИСТЕМА КІБЕРБЕЗПЕКИ США: ЕВОЛЮЦІЯ ПОЛІТИЧНОЇ СТРАТЕГІЇ ВІД ПРЕЗИДЕНТСТВА ДЖОРДЖА БУША ДО ДЖОЗЕФА БАЙДЕНА

Дипломна робота

Рівень вищої освіти – другий (магістерський)

Виконала студентка 6 курсу, 604 групи
Спеціальність 291 Міжнародні відносини,
суспільні комунікації та регіональні студії
Садомська Богдана Едуардівна
Керівник: к. політ. наук, доц. Макух-Федоркова І.І.
Рецензент:
_____

До захисту допущено:
Протокол засідання кафедри №_____
від_____
зав. кафедри_____ проф. Фісанов В.П.

Чернівці – 2021

ЗМІСТ

ВСТУП

Актуальність теми. Теракти 11 вересня 2001 р. вказали на незахищеність перед загрозами навіть наддержави з потужним оборонним потенціалом – Сполучених Штатів Америки. Інцидент став переломним моментом в американській зовнішній політиці, адже країна зіткнулась з явищем транснаціональних ризиків. Аналітики Інституту безпеки незабаром констатували, що в конфліктах нового століття фізичні атаки на об'єкти критичної інфраструктури супроводжуються кібернетичними – на мережі. Відтак, викристалізувалось питання місця кіберзагроз та кіберпотенціалу держави в системі національної та глобальної безпеки. Кіберпростір почав розглядатись як стратегічний об'єкт, а тодішній очільник Білого дому, Джордж Буш-молодший, охарактеризував його як нервову систему, тобто систему управління країною. Саме Джордж Буш заклав основи формування кіберполітики Сполучених Штатів, прийнявши першу Стратегію кібербезпеки, положення якої лягли в основу усіх подальших документів, які на разі складають галузеве законодавче забезпечення США.

З огляду на роль офіційного Вашингтону в сучасній системі міжнародних відносин, а також інформаційно-комунікаційний потенціал Сполучених Штатів, важливо проаналізувати процес становлення політики в сфері захисту кіберпростору та використання його можливостей задля реалізації національних інтересів держави. Зокрема, варто простежити еволюцію галузевих стратегій та вектори розвитку внутрішньої і зовнішньої політики при чотирьох президентах, чиї каденції припали на початок XXI століття – час розквіту інформаційно-комунікаційних технологій, які поряд з вигодами та можливостями призвели до значних загроз безпеці індивіда та держави. Виходячи з вище сказаного, **актуальність даного дослідження** підтверджена кількістю кібератак, які останніми роками сколихнули світ, а також спричиненими ними наслідками. Втручання хакерів-службовців ГРУ РФ в мережі Національного комітету Демократичної партії США, яке мало місце в межах комплексної дезінформаційної кампанії Кремля проти Гілларі

Клінтон, вкотре вказало на те, що кіберпростір використовується в межах політичних конфліктів, зокрема глобального протистояння між Сполученими Шатами Америки та Російською Федерацією.

Метою магістерської роботи є аналіз процесу формування програми кібергігієни та стратегії розвитку кібербезпеки Сполучених Штатів Америки від часів адміністрацій Джорджа Буша-молодшого до чинного президента Джозефа Байдена.

Для досягнення поставленої мети визначенні такі **завдання**:

1. проаналізувати основні теоретико-концептуальні засади кібергігієни та кібербезпеки держави;
2. простежити еволюцію кіберстратегій США з часу президентства Джорджа Буша до Джозефа Байдена;
3. визначити місце кіберпростору в контексті глобального гібридного протистояння між США та Росією;
4. виокремити місце кібербезпеки у зовнішній політиці США.

Об'єктом дослідження є політика кібербезпеки Сполучених Штатів Америки як інструмент впливу в системі міжнародних відносин.

Предметом дослідження є формування та механізми реалізації кіберполітики Білого дому від президента Джорджа Буша-молодшого до Джозефа Байдена крізь призму впливу Російської Федерації на політику США.

Хронологічні рамки дослідження охоплюють період з 2001 по 2021 роки. Нижня межа зумовлена вступом на посаду Джорджа Буша-молодшого, який заклав основи кіберполітики Сполучених Штатів Америки. Верхня межа обумовлена активізацією напрямків розвитку політики США в кібербезпековій сфері з приходом до влади Джозефа Байдена, що характеризується трансформацією підходів до ролі кіберпростору в зовнішніх відносинах.

Специфіка об'єкту і предмету магістерського дослідження зумовила вибір **теоретико-методологічної бази** до аналізу обраної проблематики. В

основі методів, якими користувалася авторка, покладено принцип об'єктивності, сходження від абстрактного до конкретного, раціональності наукового пошуку.

Застосовуючи **структурно-функціональний підхід**, вдалося простежити еволюцію розвитку кібербезпеки від Буша до Байдена. **Ретроспективний метод** дав можливість розглянути місце кібербезпеки у зовнішній політиці США. За допомогою **політико-правового методу** було здійснено аналіз внутрішнього законодавства та нормативно-правової бази безпекової політики Сполучених Штатів. **Контент-аналіз** став основою при опрацювання великої кількості статей та інтерв'ю, які стосувались виборчого процесу. **Компаративістський підхід**, використаний у роботі, дозволив простежити зміни концептуального забезпечення зовнішньої політики США та механізмів реалізації системи безпеки упродовж досліджуваного періоду.

Апробація результатів дослідження. Основні результати дослідження опубліковані на сайті аналітичного центру, також доповідались на студентській і міжнародних наукових конференціях:

1. Садомська Б. Е. Сполучені Штати напередодні виборів: кібератаки набирають обертів. Аналітичний центр ADASTRA, 22 жовтня 2020. URL: https://adastra.org.ua/blog/spolucheni-shtati-naperedodni-viboriv-kiberataki-nabirayut-obertiv.

2. Садомська Б. Е. Кіберполітика Сполучених Штатів: успадкована від Трампа і скерована Байденом. Аналітичний центр ADASTRA. 2 липня 2021. URL: https://adastra.org.ua/blog/kiberpolitika-spoluchenih-shtativ-uspadkovana-vid-trampa-j-skerovana-bajdenom.

3. Садомська Б.Е. Нормативно-правові основи формування кіберполітики США в період президенства Барака Обами. Матеріали студентської наукової конференції Чернівецького національного університету, м. Чернівці, 20 квітня 2021 р., факультет історії, політології та міжнародних відносин. Чернівці : Чернівецький нац. ун-т ім. Ю. Федьковича, 2021. С. 111–112.

4. Садомська Б.Е. Post-Cold War: кібернетичний вимір американсько-російського протистояння: матеріали V міжнар. наук. конф. Міжнародні конфлікти у сучасному світі: від регіонального протистояння до глобального суперництва, м. Львів, 3 грудня 2021 р. С. 136-138.

5. Садомська Б.Е. Американсько українська співпраця в кіберпросторі: точки перетину: матеріали міжнар. наук-практ. Конфр. Актуальні питання зовнішньої політики України, Чернівці, 17 грудня 2021. (в друці).

Структура магістерської роботи зумовлена метою, об’єктом, предметом і завданнями дослідження. Вона складається зі вступу, трьох розділів, які включають підрозділи, висновків та списку використаних джерел та літератури (105 найменувань). Загальний обсяг …

РОЗДІЛ ІІ. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ АСПЕКТИ КІБЕРБЕЗПЕКОВОЇ СФЕРИ

1.1. Загально-теоретичні підходи до визначення сутності понять «кібербезпека» та «кіберпростір»

Висока динаміка розвитку інформаційно-комунікаційних технологій, які повсюдно застосовуються корпораціями та урядами, подарувала широкий спектр можливостей – від онлайн-банкінгу до цифрової дипломатії. Втім, так само стрімко зростає й рівень загроз інформаційній безпеці як окремих індивідів, так і цілих держав. Хвиля хакерських атак на урядові відомства та об'єкти критичної інфраструктури породила занепокоєння міжнародної спільноти щодо вразливості кіберпростору – п'ятого фронту війни поряд з землею, повітрям, морем та космосом.

43-й президент Сполучених Штатів Америки, Джордж Буш-молодший, на початку століття назвав кіберпростір «нервовою системою – системою контролю американської держави» [15]. Відтак, Сполучені Штати взялись за розбудову кіберполітики – після терактів 11 вересня Джордж Буш зробив перші кроки у формуванні американської стратегії кібербезпеки, а кожна наступна адміністрація, зберігаючи за даним питанням його пріоритетне місце, розвивала нормативно-правове забезпечення та вживала відповідних заходів.

Для дослідження еволюції кіберполітичної стратегії Сполучених Штатів першочергово необхідно охарактеризувати понятійний апарат, з якого складається дана тема, а саме визначити сутність термінів: кіберзлочин, кібератака, кібербезпека, кібертероризм.

Поняття «кіберзлочинність» часто визначають, як «комп'ютерна злочинність», однак не варто вважати їх синонімічними. Оксфордський тлумачний словник визначає приставку «cyber-» як компонент складного слова. Її значення – «що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності» [71]. Подібне визначення подає також Кембриджський словник: приставка «cyber-» означає «що включає в себе

використання комп'ютерів або відноситься до комп'ютерів, особливо до мережі Інтернет» (як приклад зазначено «cybercrime», тобто кіберзлочинність) [38].

Таким чином, «Cybercrime» – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж, а термін «computer crime» відноситься тільки до злочинів, що здійснюються проти комп'ютерів або комп'ютерних даних. Тобто, термін «кіберзлочинність», ширше і точніше описує явище злочинності в інформаційному просторі, ніж «комп'ютерна злочинність».

Відтак, кіберзлочин – вид злочинної діяльності, що здійснюється у кіберпросторі. Отже, щоб дати повне визначення терміну «кіберзлочинність», спершу треба визначити, що таке «кіберпростір». Цей термін вперше використав у 1982 р. письменник Вільям Гібсен у новелі "Burning Chrome" («Палаючий хром»), однак поширення він набув у 1984 р. після публікації роману "Neuromancer" («Нейромант») [24, с. 37].

Визначення міститься в Модельному законі «Про кіберзлочинність» Міжнародного союзу електрозв'язку від 2009 р.: «кіберпростір – це фізичний і нефізичний простір, створений (або) сформований комп'ютерами, комп'ютерними системами, мережами, їхніми комп'ютерними програмами та контентом, рухом даних, і користувачами» [60].

Американські дослідники Д. Фаренкрог, Ф. Крамер та Л. Венц, базовою дефініцією поняття «кіберпростір» в американській традиції вважають визначення, яке міститься в «Національній військовій стратегії для операцій у кіберпросторі», а саме: «операційна сфера, де можливе використання електронних та електромагнітних засобів для запам'ятовування, модифікації та обміну даними через мережеві системи та пов'язану з ними фізичну інфраструктуру» [62, с. 2].

Інший підхід до визначення пропонує український науковець Д. Дубов. Він характеризує кіберпростір як «середовище, яке створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними

принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності» [26, с. 2].

Згідно зі ще одним українським дослідником О. Манжаєм, «кіберпростір – інформаційне середовище, що існує за допомогою комп'ютерних систем при взаємодії людей, комп'ютерних систем та при керуванні людьми такими системами» [100, с. 145].

Отож можемо підсумувати, що кіберпростір – це середовище, яке створене та функціонує завдяки комп'ютерним системам і даним з використанням мережі Інтернет, та уможливлює комунікацію і/чи реалізацію суспільних відносин.

Про роль кіберпростору в системі національної та міжнародної безпеки говорить поява концепції ведення боротьби в його межах та із застосуванням інформаційно-комунікаційних технологій. Для виконання військових операцій у низці держав сформовані спеціальні команди, які входять до складу Збройних сил. Приміром, в Сполучених Штатах Америки такі функції виконує Кіберкомандування – U.S. Cyber Command [98]. Відтак, варто визначити, що вважається кібероборотьбою.

Згідно з В. Л. Бурячком, «кібероборотьба – це комплекс заходів, метою яких є керування та/або здійснення деструктивного впливу на автоматизовані ІТ-системи опонента та захисту від такого впливу власних інформаційно-обчислювальних ресурсів через використання спеціально розроблених програмно-апаратних засобів та проведення спеціалізованих навчань» [21, с. 11].

У «Національному плані захисту інформаційних систем США» 2000 р. кібератаки визначено як «використання вразливостей компонентів управління програмного забезпечення, в яких використовуються інформаційні технології» [12, с. 148]. А науковець С. Бейделман хакаратеризує кібератаку як «сукупність операцій з боку ворога з

використанням комп'ютерів та інформаційних технологій задля досягнення цілей через кіберпростір». [35, с. 12].

Інший підхід до визначення терміну «кібератака» пропонують українські науковці. Приміром, В. Шеломенцев пропонує таку дефініцію: «процес реалізації програмно-математичних заходів, спрямованих на пошук та використання кібернетичних вразливостей інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем» [101, с. 35]. А співавтори праці «До проблеми формування понятійно-термінологічного апарату кібербезпеки» С. Мельник, О. Тихомиров та О. Лєнков кібератакою вважають «результат використання технічних недоліків механізмів безпеки сучасного кіберпростору з метою дезорганізації роботи його елементів» [101, с. 7]

Як витікає з визначення кібератаки охоплюють широкий спектр злочинів, метою яких є порушення цілісності і/чи конфіденційності інформації, втручання в роботу систем та мереж, що призупиняє їхню роботу. Відтак, варто розглянути типологію кібератак. Згідно з одним підходом, «класифікацію здійснюють за:

1. Метою впливу на об'єкт атаки (задля порушення цілісності, конфіденційності, несанкціонованого доступу до інформації);
2. За принципом впливу на об'єкт

• використання прихованих каналів (шляхів передавання інформації, що дозволяють двом процесам обмінюватися нею у спосіб, який порушує політику безпеки);

• застосування прав суб'єкта системи (користувача, процесу) до об'єкта (файлів даних, каналів зв'язку тощо).

3. За способом впливу на об'єкт атаки
4. За характером впливу (активний вплив, пасивний)
5. За об'єктом атаки (на системи загалом, на програми у внутрішніх або зовнішніх пристроях таких систем, на канали передачі даних)

6. За станом об’єкта (інформація може передаватись/оброблятись/зберігатись)

7. За використовуваною системою захисту;

8. За кількістю атакувальників;

9. За джерелами атак;

10. За засобами впливу на об’єкт атаки (стандартне програмне забезпечення чи спеціальні програми)» [21, с. 45-46].

Більш поширену та чітку класифікацію кібератак запропонували спеціалісти Internet Security Systems Inc., компанії-постачальника програмного забезпечення, виокремивши 5 категорій кібератак за метою здійснення. Відтак вирізняють злочини, ціллю яких є:

1) Збір інформації;

2) Спроби несанкціонованого доступу;

3) Відмова в обслуговувані;

4) Імітація підозрілої активності;

5) Системна атака [21, с. 46].

З початком розвитку ІКТ почав виокремлюватись новий тип тероризму – кібернетичний. Термін «кібертероризм», уведений в обіг у 80-х роках XX ст. Дж. Колліним, полягає в дезорганізації інформаційних систем, що породжує небезпеку загибелі людей, матеріальних втрат з метою порушення громадської безпеки, впливу на прийняття урядом відповідних рішень. Найбільш відомим наразі прикладом кібертерористичного акту можна вважати Stuxnet. Мережевий хробак, ймовірно розроблений Сполученими Штатами та Ізраїлем, завдав серйозної шкоди іранській ядерній програмі та зірвав термін запуску АЕС в Бушері. Експерти Лабораторії Касперського, вивчаючи Stuxnet, констатували, що застосування даного хробака – початок ери кібертероризму, кіберзброї та кібервійн [21, с. 32].

М. Полліт запропонував визначати кібертероризм як «навмисну, політично мотивовану атаку проти інформації, комп'ютерних систем,

комп'ютерних програм і баз даних у вигляді несанкціонованого вторгнення з боку міжнародних груп або секретних агентів» [99].

Українські науковці Г. Лисиченко, Ю. Забулов та Г. Хміль, аналізуючи явище кібертероризму та підходи до визначення терміну, систематизували інструментарій терористів в мережі:

- «завдання збитків окремим фізичним елементам кіберпростору через застосування відповідних програм;
- викрадення і загроза опублікування секретних даних щодо об’єктів критичної інфраструктури;
- втручання у програмне забезпечення, яке застосовується в системах управління;
- помилкова загроза кібертероризму, що тягне за собою серйозні економічні наслідки;
- руйнація або приглушення ліній зв'язку, неправильне адресування, штучне перевантаження вузлів комутації» [99].

У доповіді «Комп’ютерні атаки та кібертероризм: фактори вразливості і питання політики Конгресу» 2003 р. автор К. Вілсон характеризує кібертероризм як «використання комп’ютерів як зброї або цілі політично вмотивованими таємними агентами, національними або міжнародними групами задля впливу на уряд чи населення з метою зміни політики» [88, с. 7].

У роботі «Кібервійна та кібертероризм» 2008 р. «кібертероризм – це політично мотивовані атаки таємних агентів чи субнаціональних груп на інформаційні мережі, комп’ютерні програми чи системи, що призводить до насильства проти цивільного населення» [104, с. 13].

М. Кавелті у праці «Кібервійна: концепція, статус-кво і обмеження» 2010 р. визначив «кібертероризм» – як незаконні атаки недержавних суб’єктів на комп’ютери, мережі, а також інформацію, яку вони містять,

задля залякування уряду та впливу на його поведінку. Кавелті також розробив типологію кіберконфліктів в порядку зростання потенційної шкоди:

1. Кібервандалізм;
2. Інтернет-злочинність;
3. Кібершпигунство;
4. Кібертероризм;
5. Кібервійна [39, с. 1].

Таким чином, кібертероризм від інших злочинів з використанням комп'ютерів та комп'ютерних мереж вирізняє політичний умисел та насильство проти цивільного населення.

Формування кіберполітики відбувається комплексно, тобто з урахуванням як загроз, так і перспектив. Відтак, варто розглянути поняття «кібермогутності». Стюарт Старр, американський дослідник характеризує її як «можливість використання кіберпростору з метою створення переваг та здійснення впливу в усіх інших операційних просторах, використовуючи інструменти сили (instruments of power)» [105, с. 38].

Лі Джанг, Директор Інституту досліджень інформаційного та соціального розвитку при Китайському інституті сучасних міжнародних відносин, підсумовуючи результати дискусії щодо визначення кібермогутності між китайськими та японськими вченими, фактично трактував дане поняття, як здатність до ведення кібервійни, можливість держави впливати на кіберпростір, яку формують низка факторів, як-от:

«1. Інноваційний потенціал держави, можливість здійснювати дослідження з подальшою імплементацією розробок в промисловість;

2. IT-потенціал, тобто наявність технологічних гігантів на кшталт Microsoft, Google чи Apple

3. Можливості Інтернет-ринку – стан розвитку мережевої інфраструктури, кількість користувачів

4. Інтернет-культура: використання державної мови в мережі, рівень впливу в країні.

5. Інтернет-дипломатія, тобто можливість держави впливати на позицію організацій, які займаються управлінням Інтернету (до прикладу: Міжнародний союз електрозв'язку чи ICANN (Інтернет-корпорація з присвоєння доменних імен та номерів)

6. Кіберскладник військової сили: здатність до захисту об'єктів критичної інфраструктури та проведення наступальних операцій

7. Стан та перспективи розвитку кіберполітики. [23, с. 45-46].

Найбільш комплексно понятійний апарат, на основі якого формується кіберполітика США, визначено у доповіді Крістін М. Лорд та Тревіса Шарпа «Кібермайбутнє Америки: безпека і процвітання в інформаційну добу» 2011 р.:

- Кібер- – префікс, що широко застосовується щодо того, що стосується комп'ютерів, електронної інформація та/або цифрових мереж;
- Кібератака – акт ворожого використання комп'ютерів, електронної інформації та/або цифрових мереж, метою якого є маніпулювання, крадіжка, порушення цілісності чи руйнування критичних систем, активів, інформації або функцій;
- Кіберзахист – діяльність в кіберпросторі для виявлення, аналізу, попередження вразливостей задля захисту комп'ютерів, електронної інформації та/або цифрових мереж;
- Кіберексплуатація – допоміжні операції зі збору даних про важливі системи та активи щодо цілі чи противника з використанням комп'ютерів, електронної інформації та/або цифрових мереж;
- Кіберінцидент – кібератака, експлуатація чи вторгнення, що несе шкоду важливим системам, активам, інформації шляхом порушення конфіденційності чи цілісності комп'ютерів, електронної інформації та/або цифрових мереж;

- Кібервторгнення – несанкціонована дія в обхід маневрів щодо механізмів безпеки комп’ютерів, електронної інформації та/або цифрових мереж;
- Кібероперації – використання кіберможливостей задля досягнення цілей у кіберпросторі або з його використанням;
- Кібербезпека – захист комп’ютерів, електронної інформації та/або цифрових мереж від навмисного чи ненавмисного несанкціонованого відкриття, передачі, переривання, модифікації чи знищення;
- Кіберпростір – поняття, що характеризує простір і спільноти, які сформовані комп’ютерами, електронною інформацією і пристроями, цифровими мережами та їхніми користувачами;
- Інтернет – глобальна мережа, що базується на Протоколі використання Інтернету, яка уможливлює взаємодію різноманітних компонентів, як-то мережам, обчислювальному обладнуванню та пристроям. Індивідуальні компоненти керуються урядами, індустрією, науковими колами та приватними особами;
- Мережа – розподілена система взаємопов’язаних зв’язків комунікації [66, с. 12].

Характеризуючи український підхід до визначення понятійного апарату, слід взяти до уваги дефініцію В.Л. Бурячка, згідно з якою «кібербезпека – стан захищеності кіберпростору держави в цілому або окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам» [21, с. 15]. При чому автор вказує на те, що такий стан можливий при синхронізації розвідувальних та захисних дій.

Варто зазначити, що Д. Дубов визначає поняття безпеки кіберпростору від зворотного, тобто вказуючи на фактори, які потенційно можуть становити

загрозу. Відтак, «кібербезпека» за Дубовим – це «стан захищеності життєвоважливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, при якому мінімізується можливість завдання шкоди через:

- Неповноту та\або невірогідність інформації, яка використовується;
- Негативний інформаційний вплив;
- Негативні наслідки функціонування інформаційних технологій;
- Несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації» [26, с. 2].

Попри деякі відмінності у визначенні ключових понять між американськими та українськими науковцями, спільним є набір характеристик, притаманних злочинам, які здійснюються в кіберпросторі. Доктор юридичних наук А.Л. Осипенко, досліджуючи питання організованої злочинності в Інтернеті, визначив основні «властивості кібератак, до яких належать:

- дистанційність;
- анонімність;
- транскордонний характер деяких атак, при яких злочинець і жертва знаходяться під юрисдикцією різних країн;
- інтелектуальний характер злочину, що забезпечується високим рівнем підготовки злочинців;
- розгалужена система об'єктів, за допомогою яких здійснюється атака;
- нестандартність, постійна модернізація механізмів вчинення злочинів, використання спеціальних засобів;
- багатоепізодний характер протиправних дій при множинності жертв;
- можливість використання автоматизованого режиму;

- відсутність свідків злочину, тобто осіб, які спостерігали подію злочину та здатні впізнати злочинця» [94, с. 11].

Аналізуючи законодавство Сполучених Штатів Америки в галузі кібербезпеки можна класифікувати такі типи кіберзлочинів, як:

- несанкціонований доступ до мереж урядового відомства та/або завдання шкоди таким мережам, перешкоджання їхній роботі;
- Шпигунство/шантаж та інші злочини, здійсненні з використанням комп’ютерних технологій;
- Торгівля викраденими інструментами доступу, приміром – паролями;
- Завдання умисної шкоди лініям та мережам зв’язку, пристроям іншому відповідному майну;
- Викрадення та/або перехоплення повідомлень, що передаються каналами зв’язку, зокрема електронним способом, та подальше їхнє розголошення або загроза розголошення;
- Несанкціонований доступ до електронної пошти та інформації, яка міститься в пам’яті комп’ютера [21, с. 26].

Отож кіберзлочинність – «це сукупність злочинів, що здійснюються в кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних» [93, с. 48].

Таким чином, можна підсумувати, що немає єдиної дефініції термінів «кібербезпека», «кібертероризм», «кібератака», «кібермогутність» та «кіберпростір». Втім, підходи до визначення західних та українських вчених подібні, адже спираються на поєднання ключових факторів, як-от: комп’ютерні системи, під’єднанні до мережі Інтернет, та інформаційні потоки в межах цих систем.

- Однак, варто зазначити, що першочергово ставка робилась на технічні аспекти, що уможливлюють функціонування кіберпростору, а інформаційний потенціал як стратегічний ресурс вперше на законодавчому рівні визнали в Міжнародній стратегії для кіберпростору 2011 р. Така тенденція прослідковується і в працях науковців. В українській традиції питання ролі кіберпростору почали досліджувати пізніше: основні роботи українських фахівців, використані для підготовки магістерського дослідження, датуються 2013-2018 рр.., в той час, як праці західних спеціалістів опубліковані переважно в період з 2003 по 2011 рр.. Отож, приміром В. Шеломенцев визначає кібератаку як реалізацію програмно-математичних заходів, спрямованих на пошук та використання кібернетичних вразливостей інформаційно-телекомунікаційних систем. А С. Мельник, О. Тихомиров та О. Лєнков вказують на використання технічних недоліків механізмів безпеки сучасного кіберпростору з метою дезорганізації роботи його елементів при здійсненні кібератаки. У більш пізніх дослідженнях, на приклад працях Д. Дубова, до факторів мінімізації загрози кібербезпеці віднесені ті, що безпосередньо пов’язані з інформацією, як-от поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

1.2.Характеристика джерельної бази дослідження

Описуючи джерельну базу дослідження, варто зазначити, що вона сформована трьома основними категоріями:

1. Нормативно-правові акти, звіти та доповіді, а також офіційні сайти Білого дому та відповідних відомств;
2. Праці американських та українських науковців;
3. Інтернет-ресурси.

Так як метою магістерського дослідження є аналіз процесу формування програми кібергігієни та еволюції стратегії кібербезпеки США від часів адміністрацій Джорджа Буша-молодшого до чинного президента Джозефа Байдена, значну частину джерельної бази складають нормативно-правові акти, зокрема Стратегії кібербезпеки Білого дому, прийняті в період з 2001 по 2021 роки, а також релевантні звіти та доповіді. Для реалізації мети в роботі проаналізовано:

- Національний план захисту інформаційних систем США (2000 р.) [12];
- Національну стратегію безпечного кібепростору (2003 р.) [15];
- Комплексну ініціативу щодо національної кібербезпеки (2008 р.) [16];
- Міжнародну стратегію для кіберпростору (2011 р.) [9];
- Стратегію міністерства оборони для операцій у кіберпросторі (2011 р.) [3];
- Президентську політична директиву-20 (2012 р.) [5];
- Кіберстратегію міністерства оборони США (2015 р.) [17];
- Національну кіберстратегію Сполучених Штатів Америки (2018 р.) [11];
- Указ президента про підвищення національної кібербезпеки (2021 р.) [4];

- Доповідь Комітету із розвідки Сенату США щодо російського втручання в американські вибори 2016 р. [10];
- Звіт Р. Мюллера про розслідування втручання Росії в Президентські вибори 2016 р. [13];
- Проєкт Закону про кібердипломатію від 2017 р. [7];
- Проєкт Закону про співпрацю з Україною в кіберсфері від 2018 р. [8].

Деякі нормативно-правові акти дають визначення основних галузевих термінів. Приміром, «Національна військова стратегія для операцій у кіберпросторі» містить визначення кіберпростору, а «Національний план захисту інформаційних систем США» пропонує дефініцію кібератак.

Перша стратегія в галузі кібербезпеки, затверджена Джорджем-Бушем молодшим у 2003 р., стала фундаментальною та лягла в основу усіх подальших ініціатив. Документ виокремлює три основні цілі:

1. Запобігання атакам;
2. Зменшення вразливості кіберпростору;
3. Мінімізація наслідків від скоєних злочинів в максимально короткий термін.

Крім того, тут визначено пріоритети Сполучених Штатів в даному секторі, як-то: посилення безпеки урядових мереж; збільшення кіберграмотності; розробка систем реагування на інциденти, а також координація зусиль для зменшення ризиків.

Інша стратегія Буша – Національна військова стратегія операцій у кіберпросторі 2006 р. – окрім захисного напрямку, прописала можливість здійснення контроперацій. А вже в наступному документі, Директиві міністерства оборони D 3600.1 «Інформаційні операції», розроблено класифікацію операцій в кіберпросторі. Відтак, виділено три категорії:

1. Атака на комп’ютерні мережі;
2. Захист комп’ютерних мереж;

3. Встановлення доступу до комп’ютерних мереж супротивника з метою їхнього подальшого використання у своїх цілях.

Показово, остання категорія вказала на готовність Сполучених Штатів до контрнаступу.

Подальший крок у розвитку кіберполітики Сполучені Штати здійснили разом із виданням Джорджем-Бушем Комплексної ініціативи щодо національної кібербезпеки. Документ акцентував увагу на посиленні безпеки від кіберінцидентів відомчих установ, зокрема Міністерства внутрішньої безпеки, а також виділив 5 пріоритетів:

1. Формування лінії оборони проти наявних загроз та запобігання майбутнім викликам;
2. Збільшення можливостей американської контррозвідки, а також підвищення безпеки ланцюга поставок ключових інформаційних технологій;
3. Збільшення обізнаності щодо кіберзагроз;
4. Координація досліджень та розробок;
5. Робота над визначенням та розробкою стратегій для стримування ворожої чи зловмисної діяльності в кіберпросторі.

Перші галузеві документи, розробку яких ініціював президент 44-й президент США Барак Обама, – Огляд кіберполітики та аналітична довідка Федерального бюро розслідувань. Важливість даного аналізу полягала у визначенні джерел загроз для об’єктів критичної інфраструктури, до яких увійшли:

1. Кібершпигуни;
2. Кібертерористи;
3. Хактивісти;
4. Фінансово мотивовані хакери.

Пріоритетність інформаційного потенціалу як стратегічного ресурсу держави вперше прослідковується в Міжнародній стратегії для кіберпростору 2011 р., позаяк попередні правові механізми орієнтувались на технологічному аспекті проблеми. Крім того, вже сама назва та структура

Стратегії (документ поділений на три розділи, перший з яких – дипломатія) вказує на її зовнішньополітичну орієнтацію: автори аргументували потребу розробки норм міжнародного права в сфері забезпечення інформаційної безпеки з урахування інтересів як держав, так і недержавних акторів. Фактично, таким чином Сполучені Штати вказали на свою лідерську позицію у зміцненні міжнародної кібербезпеки. Стратегія Міністерства оборони для операцій у кіберпросторі ще раз підтвердила позицію, викладену у попередньому документі – налагодження міжнародних партнерств. Таким чином, стратегічні ініціативи Барака Обами вказали на розширення візії Білого дому з внутрішньої політики на комплекс заходів як у внутрішній, так і в зовнішній політиках.

Вагомою в контексті даного дослідження є PPD-20, тобто Президентська політична директива 20 від 2012 р., в якій містилось положення про – Offensive Cyber Effects Operations – наступальні операції з кібернаслідками. Продовженням цієї політики стала Кіберстратегія Міністерства оборони, згідно з якою створювались підрозділи для здійснення кібероперацій.

Законопроєкти про кібердипломатію від 2017 р. та про співпрацю з Україною в кіберсфері від 2018 р. доповнюють Міжнародну стратегію для кіберпростору 2011 р. та продовжують політику спільного захисту кібепезпеки як глобального виклику. Перший передбачає створення в межах Державного департаменту «Управління з питань кібернетики» та затвердженої Сенатом посади очільника з посольським рангом. Другий – покликаний сприяти Україні у процесі розвитку кіберполітики: від захисту внутрішніх мереж до забезпечення ширших перспектив для міжнародного інформаційного обміну. Дана законодавча ініціатива вкотре наголосила на лідерських амбіціях Сполучених Штатів – планується, що США разом з Україною виконуватиме чільну роль в посиленні кібербезпеки Центральної і Східної Європи.

Національна стратегія кібербезпеки США 2018 р. задекларувала два важливих принципи:

1. Превентивний захист;
2. Просування американського впливу.

Втім, для формування стійкості до кібернападів та швидкого реагування на них, перш за все, потрібно проаналізувати фактори вразливості програмного забезпечення. Саме надання матеріалів для такого аналізу вимагає Указ президента Джозефа Байдена: виробник ПЗ повинен надати покупцям безпосередньо або опублікувати на офіційному веб-сайті SBOM – Software Bill of Materials – технічний набір матеріалів, який називають «аналогічним переліку інгредієнтів на упаковці харчових продуктів».

Для аналізу ролі Російської Федерації у виборах президента Сполучених Штатів Америки 2016 р. використано заяви офіційних осіб та доповіді відповідних відомств. Приміром, у Звіті розвідувального співтовариства США (Центрального розвідувального управління, Федерального розслідувань та Агентства національної безпеки) «Оцінка діяльності і намірів Росії в ході нещодавніх виборів США» вказано на причетність Владіміра Путіна до кампанії впливу на президентські вибори з метою підірвати віру громадськості в демократичний процес Сполучених Штатів Америки та зашкодити кампанії Гілларі Клінтон. Інший ґрунтовний аналіз втручання Кремля в американські системи – звіт колишнього спеціального прокурора США Робетра Мюллера, який вказує на вину російської хакерської групи Fancy Bear в атаках на Національний комітет демократичної партії США.

Другу категорію джерельної бази магістерського дослідження складають праці американських та українських науковців.

Характеризуючи західні підходи до формування тезаурусів, а також дослідження щодо потенційних вразливостей кіберпростору як загроз національній безпеці та перспектив його використання як інструменту

впливу на міжнародній арені, варто виокремити роботи таких фахівців, як-от: Ф.Д. Крамер [62, 105], Л.К. Ленц [62, 105], С.Х. Старр [105], С. Бейделман [35], К.Г. Джеймісон [103], К. Вілсон [88], Л. Янчевський та А. Коларик [104], К.М. Лорд та Т. Шарп [66], М. Кавелті [39]

Значний вплив на розвиток сфери здійснив Франклін Д. Крамер – колишній помічник міністра оборони з питань міжнародної безпеки, співробітник, член правління Атлантичної ради (Atlantic Council) США, голова правління Ради зі світових справ Вашингтона; заслужений науковий співробітник Центру технологій та політики національної безпеки Національного університету оборони; та ад'юнкт-професор Школи міжнародних відносин Елліотта Університету Джорджа Вашингтона. В контексті кібербезпекових питань наукових доробок Ф. Д. Крамера складається з низки робіт, як-то: «Кібербезпека: зміна моделі», «Кібер і стримування: військово-цивільний зв’язок у висококласних конфліктах» та «Кібернетика, розширене стримування та НАТО. Згідно з Д. Крамарем, базовою дефініцією «кіберпростору» варто вважати ту, що міститься в «Національній військовій стратегії для операцій у кіберпросторі».

У співавторстві з Ларрі К. Венцом видали праці «Кібервплив і міжнародна безпека» у 2008 р. [62], в якій дослідники розглянули перспективи нарощення кібервпливу США, що базуються на інформаційному середовищі; політику та дії відповідальних акторів, зокрема стратегії супротивників, а також розробили рекомендації.

Спільно з Стюартом Х. Старром Д.Крамер та Л.Венц у праці «Кіберсила та національна безпека» 2009 р. [105] дослідили роль кіберінструментів в забезпеченні національних інтересів держави та обумовили потребу формування відповідної політики. С. Старр – колишній очільник Дослідного товариства військових операцій (MORS), яке займається аналітикою для Міністерства оборони – дав визначення поняттю «кібермогутність» [105, с. 38].

Один з перших проблему вразливості критичної інфраструктури США до комп'ютерних загроз та можливість кібератак з боку терористів розглядав Клей Вілсон, спеціаліст з технологій і національної безпеки Відділу закордонних справ, оборони і торгівлі. Вілсон надав визначення явищу «кіберторизму», а також розробив рекомендації для Конгресу та Міністерства оборони [88].

Вразливість телекомунікаційних ресурсів до атак та експлуатації аналізували Л. Янчевський, доцент кафедри інформаційних наук та операційного менеджменту Оклендського університету, та А.Коларик, доктор філософії в галузі інформаційних систем, у праці «Кібервійна та кібертероризм» 2008 р. [104]. Автори розробили дефініції понять «кібертероризм» та «інформаційна війна», а також рекомендації щодо боротьби з такими атаками.

Визначенням «кібертероризму» займалася Міріам Кавелті – заступниця директора з досліджень і викладання в Центрі досліджень безпеки (CSS) ETH Цюриха. В роботі «Кібервійна: концепція, статус-кво і обмеження» також наведена типологія кіберконфліктів за ступенем загрози [39, с. 1].

Комплексний понятійний апарат, який формує кіберсектор: кібератака, кіберзахист, кіберексплуатація, кіберінцидент, кібервторгнення, кібероперації, кібербезпека, кіберпростір, Інтернет та мережа – розробили віце-президент і директор наукових досліджень «Центру нової американської безпеки» Крістін М. Лорд та Тревіс Шарп, спеціаліст Центру, в першому томі праці «Кібермайбутнє Америки: безпека і процвітання в інформаційну добу» 2011 р. [66]. Автори досліджували національний інтерес у кіберпросторі та природу загроз.

Ґрунтовний аналіз ролі хакерів та тролів як інструментів Кремля в контексті глобального гібридного протистояння між США та Росією здійснила Кетлін Гол Джеймісон – докторка філософії, професорка комунікації при Університеті Пенсільванії, член Американського філософського товариства та Національної академії наук, колишня

президентка Американської академії політичних і соціальних наук. К. Джеймісон – авторка та співавторка 16 праць, крайня з яких – «Кібервійна: як російські хакери та тролі допомогли обрати президента» 2018 р. [103]. У праці авторка розглядає поетапність комплексної дезінформаційної кампанії, яку розпочали хакери Fancy Bear, продовжили «Тролі з Ольгіна», а ненавмисно завершили – професійні журналісти провідних американських медіа, як-то New York Times. Відтак К. Джеймісон дослідила як кібератаки та ботоферма вплинули на американський електорат, а Путін, відповідно, поквитався з Гілларі Клінтон, яка критикувала його режим.

Діяльність «Тролів з Ольгіна» в американському інформаційному просторі з 2012 по 2018 рр. проаналізовано в «АІД, соціальні медіа та політична поляризація в США» [59] – спільній роботі оксфордських науковців та фахівців компанії Graphika, яка спеціалізується на аналізі соцмереж з використанням Штучного Інтелекту. Зокрема, спеціалісти надали кількісні показники впливу тролів на американців – за 2 роки 30 млн. користувачів поширили контент між рідними та друзями.

В українському дискурсі питаннями кіберзагроз та кібербезпеки Сполучених Штатів та дослідженням тезаурусу даного сектору займалися Д. Дубов [23], О. Зернецька [24], М. Бережна [20], В.Л. Бурячок [21], Ю. Полтавець [26], С. Мельник [101] та О. Манжай [100].

Значну увагу питанням кібербезпеки приділяє Дмитро Дубов – завідувач відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень, кандидат політичних наук. Зокрема, в дисертації «Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України» автор дає визначення поняттям «кіберпростір», «кібербезпека» та «кіберпотужність». У монографії «Кіберпростір як новий вимір геополітичного суперництва» проаналізовано роль безпеки кіберпростору в парадигмі сучасної геополітики та геостратегії. Автор наводить низку дефініцій західних та східних дослідників «кібермогутності» та вказує на елементи, які її формують. Крім

того, Дубов аналізує тренди мілітаризації та демілітаризації кіберпростору загалом, а також внутрішні та міжнародні стратегічні ініціативи США.

Еволюцію стратегій зміцнення кіберпростору Сполучених Штатів прослідковує Ольга Зернецька, завідувачка відділу глобальних і цивілізаційних процесів Інституту всесвітньої історії НАН України. У монографії під назвою «Глобальна комунікація» 2017 р. авторка наводить дефініції понять, що складають кіберсектор: кібербезпека, кіберпростір, кібервторгнення, – а також типологію загроз (розподілення відмова обслуговування, хробаки, трояни і тд.). О. В. Зернецька здійснила аналіз кіберполітики, зокрема, стратегій, Білого дому за президентства Джорджа Буша-молодшого та Барака Обами.

Марія Бережна, кандидатка історичних наук Донецького національного університету, досліджувала роль президента Барака Обами у формуванні американської кібербезпеки. Зокрема, у праці «Розвиток інформаційної безпеки США: практичні кроки Барака Обами» 2013 р. проаналізовано процес побудови механізмів співпраці між федеральними та місцевими органами влади, а також індустрією задля синхронізованої протидії кібератакам. Крім того, М.С. Бережна дослідила вклад Барака Обами у розвиток нормативно-правового забезпечення кіберсектору Америки та роль Сполучених Штатів у розробці міжнародних галузевих документів.

Володимир Бурячок, співавтор підручника «Інформаційна та кібербезпека: соціотехнічний аспект», охарактеризував різні підходи до визначення термінології, проаналізував законодавче та інституційне галузеве забезпечення низки держав, серед яких Сполучені Штати Америки та Україна, а також розглянув класифікації кібератак та кібертероризму.

Олександр Манжай, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, запропонував визначення кіберпростору, а Юлія Полтавець проаналізувала підходи до визначення термінології західних та українських науковців і

розглянула нормативно-правове забезпечення кіберсектору Сполучених Штатів як приклад для України.

Третю категорію джерельної бази магістерського дослідження складають Інтернет-ресурси. Соціальні мережі та онлайн-медіа відіграли одну з головних ролей у комплексній дезінформаційній кампанії Кремля проти Гілларі Клінтон особисто та американської демократії загалом в контексті гібридного протистояння між Сполученими Штатами Америки та Російською Федерацією. Зокрема, в роботі використано відео- та текстові матеріали Russia Today [32, 86], яка активно працювала над популяризацією компроментуючих Гілларі Клінтон матеріалів. Крім того, розглянуто статті журналістів New York Times [34, 40, 42, 47, 48, 49, 54, 55, 65] за жовтень 2016 р., тобто напередодні виборів, заголовки яких містили згадку про Клінтон та зміст її е-мейлів, отриманих внаслідок низки кібератак на Національний комітет Демократичної партії США. Експерти онлайн-видання PolitiFakt [81] підрахували, що Дональд Трамп за останній місяць передвиборної кампанії у своїх промовах та коментарях згадав про ресурс WiliLeaks, на якому опублікували викрадені хакерами електронні листи, понад 160 разів. Таким чином вдалося визначити роль Російської Федерації у виборах президента Сполучених Штатів Америки в 2016 р.

Отож, з огляду на специфіку теми магістерської роботи та поставлену мету, значна її частина спирається на аналіз законодавчих актів та ініціатив. Для дослідження становлення кіберполітики Сполучених Штатів використано галузеві стратегії, прийняті в період з 2001 по 2021 роки, тобто з моменту президентства Джорджа Буша, який фактично розпочав роботу в даному напрямку та заклав основи законодавчого забезпечення в сфері захисту американського кіберпростору.

Друга категорія джерельної бази – праці західних та українських науковців – використано для визначення понятійного апарату, що складає дану тему, а також класифікації злочинів, що здійснюються в кіберпросторі.

Статті, опубліковані на веб-сайтах популярних американських медіа, зокрема в New York Times, допомогли прослідкувати вплив Кремля на формування американського порядку денного в межах комплексу заходів, спрямованих проти передвиборної кампанії кандидатки від Демократичної партії Гілларі Клінтон.

РОЗДІЛ ІІ. ФОРМУВАННЯ АМЕРИКАНСЬКОЇ КІБЕРПОЛІТИКИ НА ПОЧАТКУ ХХІ СТОЛІТТЯ: ВІД БУША ДО БАЙДЕНА

2.1. Нормативно-правові основи формування кіберполітики США в період президенства Барака Обами

Рубіж ХХ та ХХІ століть – час, коли основним багатством, загрозою та інструментом впливу стала інформація, що створюється, шириться та вносить свою лепту в життя окремих громадян, цілих корпорацій і навіть держав за допомогою інформаційно-комунікаційних технологій. Проте ІКТ, які уможливили е-врядування та мережеву дипломатію, на додачу стали головною зброєю сучасності у руках хакерів та кібершпигунів, котрі діють в інтересах держави. У звіті про глобальні загрози 2020 року, який щорічно публікується до проведення Всесвітнього економічного форуму в Давосі, кібератаки увійшли до десятки найбільших небезпек наступної декади поруч із глобальним потеплінням, зброєю масового ураження, стихійними лихами та інфекційними хворобами [18, с. 3]. За прогнозом експертів з кіберекономіки та кібербезпеки Cybersecurity Ventures, збитки від кіберзлочинності у 2021 р. у міжнародному масштабі сягнуть 6 трлн доларів [69]. З огляду на це, цілком логічним та раціональним кроком розвинених країн стало формування державної кіберполітики, котра має базуватись на стійкості систем, здатності розпізнавати загрози та навіть на наступальних операціях як механізмі досягнення політичних цілей.

Сполучені Штати Америки, як одна з передових держав, мають у своїй сучасній історії приклади ефектних кібернетичних нападів на опонентів та досить деструктивних кіберзлочинів проти них.

У контексті наступальних операцій у кіберпросторі, варто виокремити атаку Кіберкомандування США на іранські системи керування ракетними установками, здійснену в червні 2019 р. у відповідь на збиття Іраном американського безпілотника. Спершу Дональд Трамп віддав наказ вдарити по іранських радарах та протиракетних установках, однак, оцінивши

потенційні втрати – вбивство 150 військових – відкликав рішення, віддавши перевагу наступу в кіберпросторі.

Одним з найяскравіших прикладів масштабних та впливових кібератак проти Штатів стали так звані «соціальні кібератаки» 2016 р., тобто ті, в основі котрих була не руйнація систем, а суспільно-політичний вплив. Такої атаки американці зазнали під час передвиборної кампанії Гілларі Клінтон, коли російська хакерська група Fancy Bear, підконтрольна Головному управлінню Генерального штабу Збройних сил РФ (раніше – ГРУ), втрутилася в ресурсну базу Національного комітету Демократичної партії США. Внаслідок атаки 20 тис викрадених мейлів, компроментуючого змісту, з'явились на Wikileaks та призвели до розслідування проти Клінтон. Факту злочину у її діях не виявили, однак кандидатка втратила довіру виборців, для котрих моральний образ політика має значення: рейтинг Хілларі, яка впевнено випереджала Трампа, за тиждень (з моменту оголошення Джейсом Комі, директором ФБР, про дорозслідування) суттєво скоротився, а розрив між кандидатами зменшився з 12% до 1% [31].

Чергову спробу Кремля втрутитись в американські вибори через кіберпростір зафіксували у 2019-2020 рр. Спершу серії атак зазнала Burisma Holding – українська газова компанія, де працював син Джозефа Байдена Хантер. Згодом під прицілом хакерів опинилась SKDKnickerbocker – вашингтонська фірма, котра спеціалізується на консультаціях та розробці стратегій для американських демократів на президентських та губернаторських кампаніях, і котра, зокрема, працювала з Джозефом Байденом. Однак ефекту 2016 р. не відбулось, бо американські системи зміцніли, а самі громадяни навчились більш критично оцінювати інформацію про кандидатів.

Очевидно, що екосистема кібернетичного простору позначається на внутрішній та зовнішній політиці держави, а також впливає на її рівень на міжнародній арені, тож потреба формування кібергігієни обґрунтована.

Незабаром після терактів 11 вересня, 22 вересня 2001 р. вийшов звіт “Cyber Attacks During The War on Terrorism: A Predictive Analysis”, підготовлений експертами Інституту безпеки, технологій і суспільства США [21, с. 54]. Проаналізувавши конфлікти між США та КНР, Ізраїлем та Палестиною, а також Сербією та Північноатлантичним Альянсом, спеціалісти з’ясували, що поряд з фізичним деструктивним впливом на об’єкти критичної інфраструктури здійснюються кібератаки на мережі та сервери, підключені до Інтернету.

Отож початок роботи в цьому напрямку заклав Джордж Буш-молодший, чітко усвідомлюючи, що кіберпростір здатний забезпечити економічну конкурентоспроможність та політичний влив на міжнародній арені. Спершу кібербезпекові питання з’явились на сторінках документів, що опікувались питаннями зовнішньої політики США. У 2001 році «Чотирирічною програмою розвитку оборони США» кіберпростір було визнано новою ареною протиборства, а кібероперації виокремлені як окремий вид воєнних операцій [91]. Важливу роль відіграла і Стратегія національної безпеки США 2002 р. [89]. Даний документ відображає зростання значущості інформаційної та кібернетичної безпеки, а його прийняття відбулось поряд з впровадженням комп’ютерних мереж в системи управління. Згодом, у 2003 році Буш-молодший затвердив написану Департаментом внутрішньої безпеки першу американську Національну стратегію безпечного кібепростору. В описі документа наголошувалось на потребі захисту кіберпростору як стратегічному виклику, реалізація якого вимагає скоординованості та цілеспрямованості зусиль американського суспільства, федерального уряду, місцевих органів влади та приватного сектору. Сам документ акцентує увагу на галузевих стратегічних завданнях та відповідних національних пріоритетах. Перша категорія виділяє три основні цілі:

1. Запобігання кібернетичним атакам на об’єкти критичної інфраструктури США;

2. Зменшення національної вразливості до таких інцидентів;

3. Мінімізація наслідків кібератак та скорочення часу відновлення пошкоджених систем.

До пріоритетів віднесено:

1. Розробка системи реагування на інциденти, що становлять загрозу національній кібербезпеці;

2. Створення програм, котрі працюватимуть на зменшення загроз у кіберпросторі;

3. Збільшення національної поінформованості та кіберграмотності населення;

4. Посилення безпеки урядового кіберпростору;

5. Кооперація в галузі забезпечення національної та міжнародної кібербезпеки [15].

Вагомість цієї стратегії полягає у двох моментах. По-перше, документ заклав основи кібербезпеки не лише в урядовому секторі, але й в ОКР приватного сектору. По-друге, даний програмний документ став своєрідним фундаментом, адже його положення імплементовані в усі подальші американські стратегії щодо кібербезпеки.

За три роки, у 2006 р., Об'єднаний Комітет голів штабів опублікував «Національну військову стратегію операцій у кіберпросторі» (The National Military Strategy for Cyberspace Operations – NMS-SO), котра прописувала не лише захисні заходи, але й операції у відповідь на дії супротивника. У документі, знову ж таки, виокремлено 5 основних напрямків:

1. Радіоелектронна боротьба

2. Психологічні операції

3. Військова дезінформація

4. Операції в інформаційно-комунікаційних мережах

5. Оперативна безпека [24, с. 272].

Того ж року, 14 серпня 2006 р., видано Директиву міністерства оборони D 3600.1 «Інформаційні операції» (Information Operations) – документ, що

став кроком структуризації кібернетичних операцій, адже класифікував операції у кіберпросторі на 3 категорії, остання з яких відкрито демонструє готовність США до контрнаступу:

1. Атака на комп'ютерні мережі;
2. Захист комп'ютерних мереж;
6. Встановлення доступу до комп'ютерних мереж супротивника з метою їхнього подальшого використання у своїх цілях [24, с. 273].

Наступний, 2007 р., у еволюції американської кібергігієни ознаменувався створенням Джорджем Бушем-молодшим «Комісії з кібербезпеки на строк 44-президентства» (Securing Cyberspace for the 44th Presidency) [44], котра наголосила на тому, що питання забезпечення кібербезпеки гостро стоїть перед американським урядом. Згодом, у січні 2008 р., після низки кібератак на комп'ютерні системи деяких агентств, тодішній президент видав «Комплексну ініціативу щодо національної кібербезпеки» (The Comprehensive National Cybersecurity Initiative – CNCI) [16], котра декларувала посилення безпекових заходів деяких відомчих установ, зокрема Міністерства внутрішньої безпеки, від втручання в мережі. «Національною ініціативою з кібербезпеки» визначались такі пріоритетні напрямки:

1. Формування лінії оборони проти наявних загроз, шляхом створення чи підвищення загальної обізнаності щодо уразливостей, загроз і подій у мережі; зменшення рівня вразливості та запобігання майбутнім викликам;
2. Захист від повного спектру загроз через посилення можливостей контррозвідки США та підвищення безпеки ланцюга поставок ключових інформаційних технологій;
3. Зміцнення майбутнього середовища кібербезпеки шляхом розширення кіберпросвіти;
4. Координація та перенаправлення досліджень та розробок у рамках федерального уряду;

5. Робота над визначенням та розробкою стратегій для стримування ворожої чи зловмисної діяльності в кіберпросторі [16].

У січні 2009 р. обов'язки президента Сполучених Штатів Америки, включно із продиктованим умовами сучасного світу курсом на посилення національної кібернетичної оборони, прийняв демократ Барак Обама. Новообраний глава держави, котрий у своїй передвиборній кампанії наголошував на ядерних, біологічних та кібернетичних загрозах як трьох основних викликах для національної безпеки, майже одразу взявся за аналіз чинної кіберполітики, доручивши Раді національної безпеки в 60-денний термін оцінити стан захисту ІКТ та надати відповідні рекомендації. «Огляд кіберполітики» (Cyberspace Policy Review), підготовлений під керівництвом Старшої директорки з кіберпростору Програми національної безпеки, керівниці Центру стратегічних і міжнародних досліджень Мелісси Хафавей, був представлений у травні 2009 р. В даному документі зазначалось про незадовільність стану ІКТ та неготовність відомчих установ протистояти загрозам у кіберпросторі [83]. Усвідомлюючи, що для ефективної боротьби ворога потрібно «знати в обличчя», ФБР того ж року представило аналітичну довідку, що містила джерела загроз об'єктам критичної інфраструктури. До переліку увійшли:

1. Кібершпигуни іноземних держав, які націлені на розвідувальні операції задля збору інформації;

2. Хакерські групи, що діють з фінансовими мотивами;

3. Хактивісти, котрі проникають у сервери, аби розмістити на сайтах суспільно-політичний контент;

4. Кібертерористи, метою яких є:

a) Руйнування чи використання об'єктів критичної інфраструктури з метою нанесення збитків національній безпеці;

b) Ослаблення економіки США;

c) Дестабілізація суспільної ситуації [20, с. 48].

Виходячи з наданих експертами оцінок наявного стану захищеності інформаційно-комунікаційної інфраструктури та аналізу ймовірних загроз, при Білому домі створили спеціалізований орган під керівництвом Координатора з кібербезпеки, який входить до складу Національної економічної ради та Ради з національної безпеки [73]. Це стало поштовхом до відкриття ще низки установ для централізованого контролю за реалізацією кіберполітики, серед яких:

1. У червні 2009 р. – Військове командування щодо забезпечення кібербезпеки у складі Стратегічного командування Пентагону зі спеціалізацією на захисті інформаційно-комунікаційних мереж від російських та китайських хакерів. У 2013 р. під час другої каденції Барака Обами на вимогу Кіберкомандування Пентагону Оборонне відомство США погодило п’ятикратне збільшення чисельності штату підрозділів кібербезпеки;

2. У жовтні 2009 р. – Центр інтеграції національної кібербезпеки і комунікацій (National Cybersecurity and Communications Integration Center) зі спеціалізацією на координації всіх систем мережевого захисту шляхом сканування активності в національних мережах [20, с. 49].

В 2010 р. за адміністрації Барака Обами вийшла Стратегія національної безпеки, в якій увага акцентувалась на питаннях захисту кіберпростору. Націлюючись на міжнародну співпрацю в даному секторі, документ декларував: розробку міжнародних стандартів, норм поведінки державних акторів у кіберпросторі, вдосконалення законодавства в галузі кіберзлочинності, захисту даних та реагуванні на кіберінциденти [89].

Адміністрація 44-го президента Сполучених Штатів Америки, Барака Обами, системно та перманентно працювала над станом американської кібергігієни, тож у травні 2011 р. приурочено до Паризького саміту Великої вісімки вийшла «Міжнародна стратегія для кіберпростору» (International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World) [9]. Її вагомість полягає у ставці на інформаційний потенціал як

стратегічний ресурс держави: в той час, як попередні правові механізми регулювання відносин у кіберпросторі орієнтувались на технологічний фактор, дана Стратегія акцентує увагу на комплексі заходів у інформаційній сфері. Вагомо, що документ складається з 3 відповідних частин (формування політики, майбутнє та пріоритети кіберпростору).

Перший розділ – формування політики кібербезпеки – містить принципи і зобов'язання щодо основних свобод, конфіденційності та вільного потоку інформації.

Другий складається з двох підрозділів: майбутнє, якого прагнуть Сполучені Штати, та роль Сполучених Штатів у майбутньому кіберпросторі.

Відтак, перша частина, а саме – бажаний кіберпростір – середовище, яке:

- сприяє інноваціям та розширює можливості окремих людей;
- єднає людей і зміцнює спільноти;
- створює кращі уряди та розширює підзвітність;
- захищає основні свободи та покращує особисту конфіденційність;
- зміцнює національну та міжнародну безпеку на основі прийняття спільних норм поведінки [9, с. 8].

Міжнародна стратегія для кіберпростору прописує основні принципи, які є дорожньою картою для держав щодо міжнародних зобов'язання в кіберпросторі. Такими нормами є:

- Підтримка основних свобод, тобто свободу вираження поглядів та єднання онлайн так само, як і у фізичному світі;
- Повага до права інтелектуальної власності, зокрема патенти, комерційні таємниці, торгові марки та авторські права;
- Конфіденційність користувачів Інтернету від незаконного втручання держави;
- Державний захист користувачів від злочинності;

- Право на самооборону: відповідно до Статуту Організації Об'єднаних Націй, держави мають право на захист від будь-яких агресивних дій у кіберпросторі [9, с. 10].

Підрозділ, який описує роль Америки у майбутньому кіберпростору, складається з 3 пунктів:

1. Дипломатія: зміцнення партнерства:

- Двостороннє та багатостороннє партнерство, тобто включення питань захисту кіберпростору до широкого спектру діалогів та багатосторонньої комунікації;
- Регіональні та міжнародні організації;
- Партнерство з приватним сектором, зокрема з власниками та операторами інфраструктури, відповідальних за більшість функцій мереж з метою сприяння технічній еволюції.

2. Захист національних та міжнародних мереж через освіту, навчання та політичні відносини;

3. Розвиток та процвітання [9, с. 11-15].

Третя частина акцентує увагу на пріоритетах політики кіберпростору, до яких належать 7 ключових факторів, як-то:

1. Економіка: просування міжнародних стандартів та інновацій;
2. Захист національних мереж: підвищення рівня безпеки, надійності та стійкості;
3. Правоохоронна діяльність: розширення співпраці та верховенство права;
4. Військовий фактор: підготовка до викликів безпеки XXI століття;
5. Управління Інтернетом: просування ефективних та інклюзивних структур;
6. Міжнародний розвиток: нарощування потенціалу, безпеки та процвітання;

7. Свобода Інтернету: підтримка фундаментальних свобод та конфіденційності [9].

Проте лейтмотивом Стратегії є позиція Сполучених Штатів Америки щодо міжнародного співробітництва. Текст документа починається цитатою Барака Обами, виголошеною 29 травня 2009 р.: «Цей світ – віртуальний простір – це світ, від якого ми залежимо кожного дня ... [це] зробило нас більш взаємопов'язаними, ніж будь-коли в історії людства» [9, с. 7]. В цьому контексті цілком зрозуміло, що даний документ наголошує на глобальному аспекті проблеми, яка відповідно потребує колегіальної реакції світової спільноти. Автори окреслюють необхідність розробки норм міжнародного права в сфері забезпечення інформаційної безпеки та обов'язковість при глобальному управлінні Інтернетом, а також врахування інтересів як держав, так і неурядових гравців. Тобто, фактично цим документом Сполучені Штати підтвердили свою готовність адаптуватись до викликів сучасності, де серед усього вибудовувалась поліцентрична система міжнародних відносин, у якій Америка як держава з потужним інформаційним потенціалом виступає центральним гравцем [89].

«Кібернетичні загрози є одними з найбільш серйозних викликів громадській і національній безпеці та економіці, з якими ми стикаємося як нація», – так починається «Стратегія міністерства оборони для операцій у кіберпросторі» (Department of Defense Strategy for Operating in Cyberspace), оприлюднена вже за два місяці після попередньої [3, с. 7]. Документ визначив наростаючий вплив кіберпростору на економічну та політичну складову державного сектору, а також на приватне життя громадськості, адже кількість користувачів мережі Інтернет досягла 2 млрд. осіб [3, с. 7].

У Вступі документа кіберпростір названо «визначальною рисою сучасного життя», що наголошує на важливій ролі питання захисту інформаційних-комунікаційних мереж у системі внутрішньої та зовнішньої політики. [3, с. 7]. Це зумовлено низкою факторів, до яких належить і швидке переміщення активів, адже американські та міжнародні компанії торгують

товарами та послугами в кіберпросторі. Втім, окрім сприяння у веденні торгівлі, власне кіберпростір став одним з основних секторів економіки, інкубатором нових форм підприємництва та інновацій, середовищем поширення свободи слова, в якому ключову роль грають соціальні мережі. Об’єкти критичної інфраструктури, зокрема енергетика, банки, фінансові структури, транспортне сполучення, зв'язок, оборонна промисловість – функціонують на основі комп’ютерних мереж, інформаційного обігу та автоматизованих систем управління. Тобто, спираються на кіберпростір, а отже, можуть піддатись несанкціонованому доступу, викраденню конфіденційної інформації та/або експлуатації.

Міністерство оборони – не становить виняток. Станом на 2011 р. відомство працювало на основі 15 тис. мереж та 7 млн комп’ютерних засобів у сотнях установок в десятках країн світу [3, с. 7]. Відомство використовує кіберпростір для військових, розвідувальних, господарських потреб, як-то переміщення матеріалів та контроль операцій. Відтак потенційні супротивники можуть намагатись експлуатувати, порушити цілісність чи спричинити відмову в обслуговуванні мереж Міністерства оборони Сполучених Штатів.

Розроблена Міноборони Сполучених Штатів Стратегія проголошує 5 стратегічних ініціатив:

1. Розгляд кіберпростору як операційної сфери для організації, навчання та оснащення, щоб Міністерство оборони могло повною мірою скористатися його перевагами. Тобто, кіберпростір прирівнюється до стратегічного об’єкта при плануванні операцій, що мають відношення до національної безпеки;

2. Використання нових концепцій оборонних операцій для захисту мереж та систем Міністерства оборони. Мається на увазі, посилення безпеки та зміцнення потужностей комунікаційних систем шляхом синхронізованого та швидкого виявлення, проведення аналізу на мінімізації ризиків та вразливостей в мережі;

3. Партнерство з іншими урядовими відомствами та агентствами США, а також приватним сектором задля забезпечення повної загальноурядової кібербезпеки;

4. Розбудова міцних відносин з союзниками США та міжнародними партнерами для зміцнення колективної кібербезпеки. Цією ініціативою Міноборони підтвердило позицію, задекларовану Міжнародною стратегією кіберпростору, – налагодження міждержавних партнерств у галузі захисту спільних інтересів;

5. Збільшення національної винахідливості завдяки високому кадровому професіоналізму та швидким технологічним інноваціям, тобто інвестування у дослідження та розробки IT сфери [3].

Останні документи, прийняті за адміністрації Барака Обами, демонструють зміну, чи радше розширення, урядового вектору з внутрішньої безпеки інформаційно-комунікаційних систем на кібербезпеку міжнародної спільноти.

Окрім поступу у нормативно-правовому забезпечені механізмів регулювання відносин у кіберсекторі, Америка взялась до практичної діяльності шляхом налагодження діалогів щодо проблем кіберзлочинності з іншими державами, зокрема Росією та Китаєм. У червні 2011 р. відбулась вашингтонська зустріч між американськими та російськими представниками, метою котрої було погодження заходів укріплення довіри задля запобігання непорозумінь і ненавмисної ескалації кіберконфліктів та налагодження тісної співпраці у реагуванні на кіберінциденти. Наприкінці травня того ж року зустріч пройшла в штаб-квартирі Китайського інституту сучасних міжнародних відносин в Пекіні між делегацією американських експертів з кібербезпеки під егідою Центру стратегічних і міжнародних досліджень та представниками китайської сторони [92, с. 101]. Однак, налагодити задекларовану співпрацю виявилось непросто. Основною перепоною, як зазначив у звіті про світові кіберзагрози в 2015 р. Джеймс Р. Клаппер, Директор Національної розвідки, стала наростаюча потужність та активність

російської розвідки, націленої на об’єкти критичної інфраструктури та деякі розбіжності в питанні кіберпростору з китайською стороною. Потенційними претендентами на кіберагресію у відповідь на злочини з їхнього боку, окрім Росії та КНР, Клаппер назвав ще й Північну Корею та Іран [89].

Наступним кроком у розбудові кібергігієни Штатів стала Президентська політична директива 20 від 2012 р. (2012 Presidential Policy Directive 20), яку називають PPD-20 [5], яка регламентувала дії створеного 23 червня 2009 р. Кіберкомандування Сполучених Штатів [98]. Втім, у широкий доступ Директива потрапила лише в червні 2013 р., завдяки колишньому аналітику Агентства національної безпеки США Едварду Сноудену. До слова, адміністрація розсекретила окремі дані ще в січні, однак з наданого суспільству контенту PPD-20 виходило тільки те, що американські дії в кіберпросторі мають виключно оборонний характер та повністю корелюють з Конституцією та Міжнародною стратегією кіберпростору. Проте, Президентська політична директива 20 містила положення про OCEO – Offensive Cyber Effects Operations, тобто наступальні операції з кібернаслідками, а також розпорядження про потребу формування списку потенційних іноземних цілей для кібератак. Під «наступальними операціями з кіберрнаслідками» відповідно до даної директиви (п. 3) передбачались: «Операції, відповідні програми чи активність, відмінні від захисту комп’ютерних мереж, кіберозвідки (cyber collection) або DCEO (The Directorate on Corruption and Economic Offence's) дій із розслідування корупції й економічних злочинів, які проводяться від імені або в ім’я Американської держави (United States Government) у кіберпоросторі США або можуть спричинити наслідки поза американськими комп’ютерними мережами» [5, с. 3].

У квітні 2015 р. тодішній глава Пентагону Е. Кратер представив нову Кіберстратегію міністерства оборони США (U.S. Department of Defense Cyber Strategy), яка доповнила і деталізувала попередню, а низка інцидентів проникнення російських та китайських хакерів в мережі американських

компаній та відомств сприяла виокремленню Російської Федерації та Китайської Народної Республіки як основних загроз національним інтересам Сполучених Штатів. Кіберстратегія проголосила також формування трьох підрозділів виконання кібероперацій загальною кількістю 6200 осіб [17, с. 14]:

1. Підрозділи кіберзахисту власної інформаційної інфраструктури;
2. Оборонні підрозділи для захисту державних інтересів від кібернападів та спровокованих ними наслідків;
3. Бойові підрозділи, котрі за наказом Президента чи Міністра оборони проводитимуть наступальні операції в американському на іноземних кіберпросторах.

Як і попередній документ від 2011 р., Кіберстратегія 2015 р. продовжує п’ять стратегічних ініціатив, зокрема намір максимально реалізувати американський кіберпотенціал задля переваги в цифровому просторі: створення та підтримку в бойовій готовності сил, здатних проводити операції в кіберпросторі. У 2011 р. питання розробки і застосування з метою наступу кіберзброї у військовій доктрині викликало гарячі дискусії, тож цей фрагмент документа засекретили, а в оновленій стратегії кіберзброю визначили ефективним засобом протидії загрозам національній безпеці Сполучених Штатів.

Дана стратегія знову ж таки демонструє американську позицію готовності до кібернаступу, проте, на відміну від попередньої, деталізує структуру та порядок проведення операцій. Крім того, документ наголошує на створенні міжнародних альянсів зі стримування кіберзлочинів, де головними партнерами виступають союзники по Північноатлантичному альянсу, країни Asia Pacific регіону та Близького Заходу.

Іншим її цікавим моментом є ідея створення єдиної платформи кібероперацій, яка б інтегрувала всі можливості воєнного відомства США, адже на момент її прийняття не було єдиного вектору розвитку цифрових можливостей, тож кожен підрозділ Міноборони Штатів будував власні

платформи і конструював власні механізми проведення операцій. У підсумку – кількість поступилась якості: надмірна чисельність систем не відповідали потребам та поставленим задачам. Інтеграція, покликана виправити ситуацію, потребувала технологічного поступу, а саме інструментів моделювання, прогнозування та аналітики, через котрі б проходили системи перед запуском. Тому технології раннього виявлення загроз, мережева опірність, а також механізми відновлення даних документом визначені як сфери досліджень, на яких потрібно сконцентруватись [89].

Загалом ж документ декларує наміри Пентагону грати першу скрипку в галузі національної кібернетичної безпеки і демонструє спроможність вести як оборонну, так і розвідувальну та наступальну діяльність в цифровому просторі.

На додачу, за час головування Обами було створено дієвий механізм стримування ймовірних кібернетичних загроз економіці та обороноздатності Сполучених Штатів – указ президента «Про арешт власності осіб, причетних до серйозних протиправних дій у кіберпросторі» від 1 квітня 2015 р.. Документ надав право американському уряду накладати санкції на фізичних та юридичних осіб, винних у кібератаках на комп'ютерні мережі об'єктів критичної інфраструктури та привласненні шляхом скоєння кіберзлочинів фінансів чи інших активів (комерційних секретів американських компаній і організацій чи персональних даних). Саме завдяки механізмам, закладеним у цьому нормативно-правовому акті, в грудні 2016 р. було прийнято санкції проти Російської Федерації [26].

Отож кожна наступна стратегія закономірно спирається на попередню. Втім, Барак Обама почав створення механізму наступальних операцій в кіберпросторі, а значить – застосування інформаційних технологій як зброї у веденні гібридного протистояння. Іншим суттєвим напрацюванням Обами варто виокремити «Про арешт власності осіб, причетних до серйозних протиправних дій у кіберпросторі» – інструмент притягнення до

відповідальності фізичних та юридичних осіб, винних у скоєнні кіберзлочинів.

2.2.Пріоритети адміністрації Дональда Трампа у кіберполітиці США та перспективи подальшого розвитку

Питання інформаційної, зокрема кібернетичної, безпеки для Сполучених Штатів Америки загострилось під час передвиборної кампанії 2016 р.: унаслідок кібератаки на штаб Демократичної партії та активності в мережі Ольгінської «фабрики тролів».

В липні 2016 р. унаслідок фішингової атаки на Демократичну партію США та Гілларі Клінтон на ресурсі WikiLeaks оприлюднили 20 тисяч мейлів, зміст яких компрометував кандидатку в президенти, та призвів до розслідування ФБР проти неї. [41] Відповідальність за атаку покладають на хакерів, підконтрольних Генеральному штабу Збройних сил Російської Федерації: 13 липня 2018 р. Міністерство юстиції Сполучених Штатів опублікувало обвинувальний акт 12 громадянам Росії за федеральні злочини з метою перешкодити виборам президента США через атаки на «комп'ютерні мережі Національного комітету Демократичної партії та оприлюднення отриманої інформації в Інтернеті під іменами «DCLeaks», «Guccifer 2.0» [57].

Ймовірно так російський уряд вирішив посприяти приходу до влади Дональда Трампа, який під час кампанії називав Владіміра Путіна «великим лідером», на противагу порівняння його з Гітлером та осудом анексії Кримського півострова, які Гілларі Клінтон висловила ще в 2014 р.

Кремль використав соціальні кібератаки – крадіжки даних із політичним підґрунтям задля впливу на електоральну думку (в даному випадку – створивши негативний імідж Клінтон). Хакери опосередковано сприяли падінню її рейтингу: за тиждень після заяви директора ФБР Джеймса Комі щодо розслідування справи Клінтон розрив між кандидатами скоротився з 12% до 1% [31].

В остаточній версії доповіді Комітету із розвідки Сенату США щодо російського втручання в американські вибори 2016 р., яку представили у серпні 2020 р., зазначається, що наміром Москви було «нашкодити кампанії Гілларі Клінтон, очорнити її потенційну президентську адміністрацію та

допомогти кампанії Дональда Трампа після того, як Трамп став ймовірним кандидатом від республіканців, похитнути демократичний процес у Сполучених Штатах Америки» [29].

Відтак 45-й президент демонстрував діаметрально протилежне ставлення до держав, чиї хакери атакували американські мережі: різка критика Китаю протиставлялася фактичному ігноруванню втручань Кремля, в той час, як конгресмени обох парій вважали російських хакерів серйознішою загрозою та назвали інцидент із хакерами Fancy Bear – «нападом на американську демократію». Дональд Трамп неодноразово висміював спроби розвідувального співтовариства покласти провину на режим Владіміра Путіна, одного разу навіть заявивши, що хакерами, які зламали системи Демократичної партії, міг бути хто завгодно, «хтось на дивані вагою 400 фунтів».

Отож, зокрема, через суттєву розбіжність поглядів на роль Російської Федерації між очільником Білого дому та фахівцями з кібербезпеки, однією з характерних рис кіберполітики адміністрації Трампа став експертний вакуум, а сам президент відзначився «чистками», що в підсумку позначилось на неготовності американських мереж протистояти хакерам (як-от атака на трубопровід Colonial Pipeline) та призвело до критики 45-го президента з боку експертів.

Вісім членів Національної консультативної ради з питань інфраструктури (NIAC) подали у відставку в 2017 р., вказавши серед низки причин у листі, отриманому NextGov, що дії президента загрожують безпеці батьківщини, а адміністрація Дональда Трампа приділяє недостатню увагу кібербезпековим загрозам для США, що зростають [84].

Крім того, Дональд Трамп скасував при Білому домі позицію кіберкоординатора, звільнивши тим самим Роба Джойса, скоротив крило Державного департаменту з питань кібердипломатії та звільнив керівника Агенства з кібербезпеки та безпеки інфраструктури США (CISA) Кріса

Кребса, після визнання Агентством заяви президента-республіканця про шахрайство під час виборів безпідставними.

Відтак 71% респондентів опитування The cybersecurity 202 Network, експертної групи з цифрової безпеки, визначили, що адміністрація Дональда Трампа скерувала державну кіберполітику в неправильному напрямку, а 29% – проголосували за правильність курсу. Однак варто зазначити, що респонденти високо оцінили роботу урядовців, як-то вже згаданих Роба Джойса і Кріса Кребса, а не самого Трампа [81], на що вказують коментарі фахівців кіберсектору для The Washington Post:

«Скасування ролі кіберкоординатора Білого дому стало кроком у неправильному напрямку», – зазначила Дебора Планкетт, колишня керівна особа Агентства національної безпеки, наразі – старша наукова співробітниця Гарвардського університету в Центрі Белфер. Інший колишній посадовець АНБ, Стів Раян вважає, що «з точки зору політики та операцій у сфері кібербезпеки, звільнення Кріса Кребса, Тома Боссерта та Роб Джойса поставили країну в небезпеку в час, коли кіберзахист найбільше потрібен». За словами Джейсон Хілі, колишнього офіцера з кібербезпеки Білого дому та чинного старшого наукового співробітника Школи міжнародних та громадських справ Колумбійського університету: «Більшість успіхів у кібербезпеці за останні чотири роки досягла не адміністрація Трампа, а урядові чиновники, які працюють проти чи незважаючи на цю адміністрацію». Стів Гробман, головний технологічний директор McAfee, американської компанії-розробника систем захисту і аналізу шкідливого програмного забезпечення, вважає, що «адміністрація Трампа досягла значних успіхів щодо кібербезпеки у таких сферах, як створення Агентства з кібербезпеки та безпеки інфраструктури (CISA) та послаблення обмежень щодо кіберкомандування США», втім «скасування ролі координатора з кібербезпеки Білого дому та звільнення директора CISA Крістофера Кребса» називає провальним рішенням» [67].

Однак діяльність Дональда Трампа в напрямку посилення кібернетичних можливостей США мала й позитивні зрушення. «Основна заслуга Білого дому під його керівництвом у цифровому просторі спирається на Національну стратегію кібербезпеки США 2018 р., яка, на відміну від попередньої, не обмежується превентивними заходами, роблячи ставку на наступальні операції, та скасування PPD-20 – президентської директиви Барака Обами, яка затверджувала обов'язкове обговорення на високому рівні між багатьма відомствами, перш ніж військові зможуть проводити значні кібероперації. Таким чином президент-республіканець поставив кібератаки в один ряд з кінетичними операціями, тобто військовими діями, що не потребують схвалення на високому рівні або міжвідомчих дискусій» [28].

Посилаючись на оцінку ризиків, тенденцій та потенціалу, серед яких: посилення впливу кіберпростору на всі сфери суспільного життя, зокрема політичне та економічне, та визнання фактів використання опонентами та конкурентами переваг мережі для заподіяння шкоди економічним, військовим та політичним інтересам США та їхніх партнерів, у вересні 2018 р. адміністрація Трампа представила оновлене бачення політики захисту кіберпростору в Національній кіберстратегії Сполучених Штатів Америки, яка спирається на Виконавче розпорядження «Зміцнення федеральних мереж та критичної інфраструктури» та Стратегію національної безпеки США від 2017 р. [11]. Структурно документ поділяється на 4 принципи, кожен з яких визначає сфери функціонування, об'єкти та пріоритетні дії:

1. «Захист американського народу, Батьківщини та способу життя Америки» – тобто керування ризиками кібербезпеки задля підвищення безпеки та стійкості нації. Даний принцип має три підрозділи:

1.1. Захист федеральних мереж та інформації, що визначає такі пріоритетні дії, як:

- подальше централізоване управління та нагляд за федеральної цивільною кібербезпекою;

- узгодження активності з управління ризиками та діяльності в галузі інформаційних технологій;
- покращення федерального управління ризиками у ланцюжку поставок.

Тобто, прослідковується тенденція розвитку системи управління ризиками на федеральному рівні, що полягає, перш за все, у визначенні чітких повноважень щодо виключення (у деяких випадках) із процесу постачання та закупівель ризикованих постачальників продуктів та послуг. Як приклад варто виокремити інформаційну кампанію проти китайського виробника обладнання Supermicro: за даними звіту Bloomberg Businessweek, уряд Китаю впроваджував апаратних закладок на сервери, якими користуються багато компаній США, зокрема Amazon та Apple [56]. Мікросхеми закладок встановили під час виробництва на заводах Supermicro агенти з Народно-визвольної армії Китайської Народної Республіки.

1.2. Надійна критична інфраструктура, що передбачає:

- визначення пріоритетності дій відповідно до національних ризиків;
- підтримку кібербезпеки з боку постачальників інформаційних та комунікаційних технологій;
- захист демократії;
- стимулювання інвестицій у кібербезпековий сектор;
- надання пріоритетності національним інвестиціям у дослідження та розвиток.

1.3. Боротьба з кіберзлочинністю та покращення повідомлень про інциденти, де пріоритетними цілями є:

- швидкий обмін інформацією про інциденти та реагування на них;
- модернізація електронного спостереження та законодавства;
- зменшення загроз із боку транснаціональних злочинних організацій у кіберпросторі;

- посилення спроможності правоохоронних органів країн-партнерів проти кіберзлочинців.

Удосконалення законодавства про комп'ютерну злочинність передбачає розширення можливостей правоохоронних органів щодо законного збору фактів злочинної діяльності та подальшого здійснення судових проваджень, а також збір необхідної інформації за межами США. Раніше така діяльність спиралась на угоди про правову допомогу, що реалізовувалась, у тому числі в рамках Будапештської конвенції про кіберзлочинність, тоді як прийнятий «Закон CLOUD» S2383 («Роз'яснення законності», від 2018 р.) надає правоохоронним органам значні повноваження щодо отримання інформації, яка зберігається на серверах компаній Сполучених Штатів, розташованих за межами США [14]. Тож укладення угод та відповідне інформування держав про проведення слідчих заходів на їхніх території більше не потрібні.

2. «Сприяння процвітанню Америки» – другий принцип, який в свою чергу теж поділяється на три підрозділи:

2.1. Формування стійкої цифрової економіки, де ключовими заходами визначено:

- стимулювання адаптивного ринку технологій; пріоритетність інновацій;
- інвестування в інфраструктуру нового покоління; сприяння вільному кроскордонному обігу даних;
- збереження лідерства США у розвитку нових технологій.

Останній із заходів – збереження лідерства Сполучених Штатів в IT-секторі передбачає просування у світі інновацій із кібербезпеки, зокрема, шляхом подолання перешкод для створення єдиного глобального ринку кібербезпеки.

2.2. Стимулювання та захист винахідливості США через:

- оновлення механізмів перегляду іноземних інвестицій та діяльності в Америці;
- зміцнення системи захисту інтелектуальної власності;
- захист конфіденційності та цілісності американських ідей.

2.3. Розвиток найвищого рівня кібербезпеки зі ставкою на людський потенціал, тобто шляхом підтримки талантів та розширення можливостей підвищення кваліфікації американських працівників;

3. «Збереження миру силовими методами» – принцип, націлений ідентифікувати, протистояти та стримувати ту поведінку в кіберпросторі, яка дестабілізує та суперечить національним інтересам, та складається з двох підрозділів:

3.1. Підвищення кіберстабільності за допомогою відповідальної поведінки держави через заохочення загального дотримання кібернорм.

3.2. Атрибутизація та стримування неприйнятної поведінки у кіберпросторі шляхом розвідки і подальшої протидії злочинному кібервпливу та інформаційним операціям.

4. «Просування американського впливу», що також об’єднує два підрозділи:

4.1. Сприяння відкритому, надійному та безпечному Інтернету, що передбачає реалізацію шляхом співпраці з державами-партнерами, промисловими та академічними колами, а також громадянським суспільством; просування багатосторонньої моделі управління Інтернетом – прозорої та рівної участі державного, приватного, наукового, технологічного та громадянського секторів; розбудова сумісної та надійної комунікаційної інфраструктури. Принцип свободи Інтернету, що лежить в основі Кіберстратегії США намірені просувати як міжнародний стандарт, тож спроба інших держав обмежити цю

свободу, навіть під гаслами боротьби з тероризмом, визнається політичною загрозою та ознака авторитаризму.

4.2. Нарощення міжнародного кіберпотенціалу, тобто посилення кіберспроможностей через покращення координації зусиль, аналітичного та технічного обміну, зокрема, акцент робиться на зменшенні рівня впливу транснаціональної кіберзлочинності та терористичної діяльності.

Зазначені вище основи розкривають завдання у сфері кіберзахисту, які поставив перед собою Білий дім під керівництвом Дональда Трампа:

1. Захист батьківщини, захищаючи мережі, системи, функції та дані;
2. Сприяння процвітанню Америки шляхом розвитку безпечної, цифрової економіки та сприяння вітчизняним інноваціям;
3. Збереження миру і безпеки через зміцнення здатності Сполучених Штатів разом з партнерами стримувати зловмисників у кіберпросторі;
4. Розширення впливу Сполучених Штатів за кордоном задля просування фундаментальних принципів відкритого, надійного та безпечного Інтернету [11, с. 18]

У 2018 р. кібернетичний підрозділ Пентагону отримав статус незалежної командної одиниці: Кіберкомандування прирівняли до 9 інших бойових підрозділів Сполучених Штатів, а кібератаки визнали повноцінними бойовими діями. Вже незабаром, у червні 2019 р., Кіберкомандування продемонструвало свою ефективність: Трамп схвалив наступальну операцію на іранські комп’ютерні системи для планування нападів на нафтові танкери в Перській затоці. Ймовірно, кібернапад став відповіддю Сполучених Штатів на збиття американського безпілотника [61]. Інцидент став свідченням реалізації принципу «defend forward», тобто превентивного захисту кіберпростору поза американськими мережами, прописаного в Національній стратегії.

Із затвердженням стратегії видатки на кібероборону зросли. До прикладу, фінансування 2020 р. на 5% більше, ніж було у 2019 р. Втім, про пріоритети і настрої в кіберсекторі найкраще говорить бюджетне розподілення між військовими та цивільними структурами: бюджет Міністерства оборони на кіберпромисловість перевищував загальний обсяг усіх цивільних відомств, включно з департаментом нацбезпеки, казначейства та енергетики, на майже 25% – 9,6 млрд дол. США проти 7,8 млрд [53]. А видатки на кібернетичні операції співвідносяться з бюджетами Федерального бюро розслідувань, Агентства з кібербезпеки та безпеки інфраструктури та Відділу національної безпеки міністерства юстиції разом як 3,7 млрд дол. США проти 2,21 млрд [53].

Чергові президентські вибори в Сполучених Штатах, які не минули без кіберінцидентів, привели до Білого дому нового керівника – Джозефа Байдена. У 2019 р. серії атак зазнала українська газова компанія Burisma, в якій працював син ексвіцепрезидента, а на той час – кандидата від Демократичної партії, Хантер Байден, ймовірно, з боку вже відомих подібними злочинами Fancy Bear. В американській службі безпеки заявили, що хакери націлювались на мейли, юридичні документи та фінансові звіти, які потенційно могли б скомпрометувати Джозефа Байдена [27]. Ще одним об’єктом атак Fancy Bear стала SKDKnickerbocker – фірма, що спеціалізується на консультаціях та розробці стратегій для американських демократів (працювала із шістьма президентськими виборчими кампаніями та низкою губернаторських), і яка, зокрема, співпрацювала із Джозефом Байденом. Хоч хакери не змогли отримати доступ до мережі, атака продемонструвала інтерес до пов’язаних із Байденом конфіденційних матеріалів, який лідирував у передвиборній гонці. Показово, що полювання за чорним досьє на Байдена співпали в часі з порушеними питаннями щодо імпічменту Трампа. Проте, і службовці адміністрації чинного на той момент очільника Білого дому, кандидата від Республіканської партії, зазнали низки атак з травня по червень 2020 р. від іранських хакерів – Phosphorus [37].

Отож питання зміцнення інформаційно-комунікаційних мереж за час каденції лише актуалізувалось для новообраного Джозефа Байдена, який за адміністрації Барака Обами займався питаннями кібербезпеки (на той момент офіційний Вашингтон зіткнувся з проблемою посилення кібершпигунства з боку Китайської Народної Республіки та вже звичним втручанням у демократичні процеси в США Російської Федерації).

Першим фактичним кроком кіберполітики Джозефа Байдена стало формування команди – те, за що попередник зазнав неабиякої критики, а саме:

- призначення керівницею CISA Джен Істерлі;
- Кріса Інгліса як національного кібердиректора (заміщення створеної наприкінці минулого року посади при Білому домі для контролю за оборонними та кібербезпековими бюджетами цивільних агентств);
- Майкл Сулмаєр посів крісло директора з питань кіберпромисловості;
- Анна Нойбергер стала заступницею радника з питань національної безпеки;
- Роберт Сілверс отримав посаду заступника міністра з питань стратегії, політики та планів;
- Русс Треверс – новий заступник радника з питань внутрішньої безпеки; а Елізабет Шервуд-Рендалл тепер радниця з питань нацбезпеки – усі посадовці раніше обіймали керівні посади в секторі нацбезпеки, спеціалізуючись на питаннях кіберстійкості [28].

Тим самим Байден з перших днів показав серйозність намірів щодо посилення безпеки мереж американських відомств та компаній. Аналізуючи призначення, варто також зазначити, що оновлену кіберкоманду складають спеціалісти з держсектору, при тому що переважна більшість інтернет-інфраструктури Сполучених Штатів розміщена в приватному полі, отож потенційно потерпає координованість зусиль.

Першим юридичним кроком президента-демократа стало підписання 12 травня 2021 р. Указ президента про підвищення рівня кібрбезпеки Сполучених Штатів Америки [4] як реакція на кібератаку, в результаті якої обмежили роботу на майже 9 км дистанції трубопроводу Colonial Pipeline, який забезпечує приблизно 45% дизельного пального і бензину на східному узбережжі США [19].

Указ президента, серед усього, спонукає федеральні відомства співпрацювати з приватним сектором через обмін інформацією та застосовування технологій, здатних підвищити стійкість до кібернападів. Втім, ключовим елементом наказу став SBOM – Software Bill of Materials – технічний набір матеріалів, який називають «аналогічним переліку інгредієнтів на упаковці харчових продуктів», що сприятиме аналізу факторів вразливості програмного забезпечення для управління ризиками, адже знатись на програмних компонентах у складі продуктів означає швидше реагувати на інциденти [4].

Даний виконавчий наказ став послідовним і рішучим кроком вперед, змінивши рекомендаційний характер щодо надання інформації про мережеві загрози на обов'язковий. Прийнятий у 2015 р. Закон про обмін інформацією про кібербезпеку заохочував приватні компанії звітувати, втім не зобов'язував [44]. Наступним кроком, ймовірно, буде встановлення часових рамок: робота ведеться над законопроєктом, згідно з яким державні та приватні організацій будуть змушені попереджати уряд про порушення безпеки кіберпросторі протягом однієї доби [28].

Розуміння адміністрації Байдена ризиків і можливостей, пов'язаних з кіберпростором, чітко прослідковується у фінансуванні сектору:

1. «Американський план порятунку» на посилення кібербезпеки виділяє 1,65 млрд дол.: 1 млрд для Фонду модернізації технологій федерального уряду, тобто на оновлення системи безпеки та перехід до захищеної хмарної інфраструктури, та 650 млн для CISA, тобто на

розширення можливостей реагування та посилення спроможності підтримувати проєкти безпеки у федеральних департаментах [50];

2. Згідно з планом бюджету на 2022 рік фінансування CISA збільшено на 110 млн у порівнянні з минулорічним – 2,1 млрд дол [50].

Отже, ліквідація посад та суб'єктивні звільнення кіберспеціалістів, як-от Кріса Кребса, Дональдом Трампом негативно позначилась на політиці захисту інформаційно-комунікаційних мереж як державного, так і приватного типу. Разом з тим, варто відзначити, що саме адміністрація Трампа дала потужний імпульс нарощенню потенціалу Сполучених Штатів Америки в кіберпросторі. По-перше, завдяки можливості здійснення наступальних операцій у кіберпросторі, яка закріплена в Національній стратегії кібербезпеки від 2018 р.. По-друге, завдяки визнанню Кіберкомандування як повноправної військової одиниці та скасуванню Директиви Барака Обами про обов'язкове обговорення потенційних кібероперацій на високому рівні.

Чинний президент Джозеф Байден певною мірою дотримується курсу попередника – за Кіберкомандуванням залишено право здійснювати операції без попереднього обговорення. Але відмінність політики полягає, зокрема, у формуванні команди – фахівців, які вже зарекомендували себе в секторі захисту інформаційно-комунікаційних мереж. До того ж, президентське розпорядження посилює координацію зусиль між державним та приватним секторами, що потенційно мало зміцнити американський кіберпростір, але слабкою ланкою в цьому ланцюжку на сьогодні є відсутність в оновленій кіберкоманді спеціалістів приватного поля.

Аналізуючи формування кіберполітики Сполучених Штатів з початку XX століття, варто зазначити, що Білий дім слідує вектору, який задав ще Джордж Буш-молодший, а кожна з наступних стратегій спитається на основні положення попередньої, що свідчить про розуміння проблеми і бачення можливостей її розв'язань.

Втім, кожна з адміністрацій зробила свій внесок у сферу. Джордж Буш-молодший визнав кіберпростір ареною протиборства та заклав основи безпеки кіберпростору не лише в урядовому секторі, але й в об'єктах критичної інфраструктури приватного поля.

Чи не найбільшого впливу на розвиток політики в кіберпросторі завдав за дві каденції Барак Обама. Його діяльність сфокусувалась на двох основних аспектах. По-перше, з огляду на глобальний контекст кібернетичних загроз, які, відповідно, потребують колегіальної реакції, адміністрація Барака Обами в низці документів (Стратегії національної безпеки 2010 р., Міжнародній стратегії для кіберпростору від 2011 р. та Стратегії Міністерства оборони для операцій у кіберпросторі) закцентувала увагу на ролі міжнародної співпраці. По-друге, Сполучені Штати за Обами розробили типологію джерел загроз і виокремили Російську Федерацію та Китайську Народну Республіку як основні загрози національним інтересам США. До того ж, саме указ Барака Обами «Про арешт власності осіб, причетних до серйозних протиправних дій у кіберпросторі» від 2015 р. уможливив політику санкцій проти Російської Федерації за втручання у вибори 2016 р.

Хоч наступальні операції згадувались ще в PPD-20 – директиві Обами, найбільшої уваги їм приділив Дональд Трамп, як юридично (прирівнявши Кіберкомандування до бойового підрозділу та скасувавши PPD-20, яка передбачала погодження потенційних операцій на високому рівні), так фінансово (бюджетне розподілення демонструвало ставку на наступальні операції, а не захист інформаційно-комунікаційної інфраструктури).

Політика нинішнього президента Джозефа Байдена контрастує з баченням попередника. Вступивши на посаду, Байден почав з роботи над помилками Трампа: зібрав команду фахівців, котрі працювали в урядовому кіберсекторі за адміністрації Обами. На відміну від Трампа, адміністрація Байдена збільшила фінасування CISA – цивільного відомства. Втім, хоч виконавчий наказ Байдена спонукає федеральні установи співпрацювати з

приватними колами, в кіберкоманді, яку він сформував, не вистачає спеціалістів приватного поля!

РОЗДІЛ ІІІ. РОЛЬ ТА МІСЦЕ КІБЕРБЕЗПЕКОВИХ ПИТАНЬ У ЗОВНІШНІЙ ПОЛІТИЦІ США: ПРОБЛЕМИ ТА ШЛЯХИ РОЗВ'ЯЗАННЯ

3.1. Кризові аспекти безпекової політики США під впливом хакерських атак РФ

Неодноразово під час Холодної війни Радянський Союз використовував розвідку та пропаганду для впливу на політичний процес Сполучених Штатів Америки, зокрема під час виборів. Ще в 1960-х рр. КДБ працював проти кандидата-республіканця Баррі Голвотера, який був антикомуністом. Чеська розвідка надрукувала та відправила дипломатичною поштою до США тисячі листівок пропагандистського змісту про расистські погляди Голдвотера, які потрапили до виборців разом із кореспонденцією. В результаті радянського втручання Баррі Голдвотер програв Ліндону Джонсону. Незабаром, у 70-х рр., співробітники КДБ вербували американських службовців для збору інформації про тодішнього кандидата у президенти Джиммі Картера, а згодом – взялись за імідж Рональда Рейгана, називаючи його «корумпованим чиновником» та популяризуючи гасло «Рейган означає війна».

Технологічний прогрес, помножений на успадкований від Радянського Союзу інструментарій впливу, надав Кремлю можливість ще легше та швидше отримувати та поширювати «необхідну» інформацію. Замість службовців КДБ шпигунством на благо держави тепер займаються хакери-службовці ГРУ, замість листівок – пости у соціальних мережах.

Вплив Кремля на вибори президента Сполучених Штатів 2016 р. продемонстрував безпекову кризу Америки, вказавши на вразливість інформаційно-комунікаційних мереж. Відтак, дезінформаційна кампанія фабрики тролів з Ольгіна та атаки на інформаційно-комунікаційні мережі хакерів-службовців ГРУ з мінімальними витратами сколихнули політичну стабільність одного з найвпливовіших гравців на міжнародній арені.

У 2016 р. громадяни Сполучених Штатів постали перед вибором нового очільника Білого дому. Барак Обама, який керував державою впродовж двох термінів, відходив від справ, а демократів натомість представила жінка. Рейтинг Гілларі Клінтон впродовж кампанії демонстрував високий вотум довіри американців. Втім, їй не довіряв Владімір Путін, якого демократка різко критикувала, на відміну від республіканця-Трампа.

Ще навесні 2011 р. Путін сказав, що Клінтон, як тодішня головна дипломатка США, допомогла організувати щось на кшталт «середньовічного заклику до хрестового походу». Він мав на увазі прийняття резолюції ООН щодо військової інтервенції в Лівії, щоб зашкодити режиму Муаммара Кадаффі масово обстріляти повстанців. Роль Гілларі Клінтон і Барака Обами тоді полягала у переконанні Дмітрія Мєдвєдєва не ветувати домовленості в Раді Безпеки ООН [79].

Наступна сутичка спалахнула в грудні того ж 2011 р. Держсекретарка США Гілларі Клінтон підтримала масові протести в Москві через сфальсифіковані результати виборів на користь Путіна, зазначивши: «російський народ, як і люди в усьому світі, заслуговує на право, щоб їхні голоси були почуті, а їхні голоси підраховані» [63]. Російський президент назвав заяву маніпуляцією, сигналом для демонстрантів, щоб підірвати його владу.

На додачу, у 2014 р. за анексію Кримського півострова Гілларі Клінтон порівняла риторику Владіміра Путіна про захист свого народу з висловлюваннями нацистів у 1930-х рр., а самого очільника Кремля – з Гітлером. Клінтон зазначила також, що спробами «ресовєтізувати» периферію Росії Путін лише розтрачує потенціал нації і «загрожує нестабільності і навіть миру Європи» [58].

На противагу критиці з боку Клінтон, коментарі Трампа щодо Путіна носили виключно позитивний характер і visa versa – російський президент називав кандидата-республіканця «яскравим і талановитим» і «абсолютним лідером президентських перегонів» [46]. Тож, на фоні тривалої конфронтації

з Гілларі Клінтон та взаємної приязні з Дональдом Трампом саме на республіканця зробив ставку Кремль.

Відтак, в оприлюдненому 6 січня 2017 р. звіті розвідувального співтовариства США (ЦРУ, ФБР та АНБ) «Оцінка діяльності і намірів Росії в ході нещодавніх виборів США» йдеться про те, що «президент Росії Владімір Путін у 2016 р. наказав провести кампанію впливу, націлену на президентські вибори у Сполучених Штатах. Мета Росії полягала в тому, щоб підірвати віру громадськості в демократичний процес США, очорнити репутацію Гілларі Клінтон і зашкодити її передвиборчій кампанії. Путін і російський уряд чітко надали перевагу вже обраному президенту Трампу та прагнули допомогти йому, дискредитуючи Клінтон» [2, с. 7].

«Тролі з Ольгіна» або АІД, тобто Агентство інтернет досліджень, – адепти інформаційних війн, які переважно зосередженні на атак на опозицію Путіна та «Єдиної Росії». Опис організації робочого процесу фабрики російською опозиційною журналісткою Людмилою Савчук, яка певний час працювала «тролем» під прикриттям нагадує Міністерство Правди Орвелла: «Усередині ферми на кожному поверсі стояли суцільні щільні ряди комп'ютерів, за якими безперервно працювали кілька робочих змін. Працівники заходили за перепустками, якими відзначали час прибуття та закінчення роботи. Навіть перекуси були за розкладом» [102, с. 41.]. Саме так, зусиллями тролів, створювалась фейкова реальність.

Однак «слави» тролі набули через участь в американській виборчій кампанії. На початку 2018 р. спеціальний прокурор США в ході розслідування з'ясував, що діяльність «ольгінських тролів» вийшла за межі Російської Федерації, дійшовши до Сполучених Штатів. «Ферма» створила тисячі фейкових аккаунтів начебто від імені американців (праворадикалів, активістів за права чорношкірих, прихильників Трампа), чиї месседжі можна поділити на три типи:

- агітація афроамериканського сегменту електорату бойкотували вибори або дотримувалися неправильної процедури голосування;
- спонукання праворадикалів до активнішої конфронтації;
- поширення конспірологічних теорій і дезінформації.

В межах дезінформаційної кампанії тролі використовували хештеги, які демонстрували підтримку Трапма і зневагу до Клінтон, як-то: #TrumpTrain, #IWontProtectHillary, #BlacksAgainstHillary, #Hillary4Prison, та фейсбук-аккаунти під назвами “Clinton FRAUDation” and “Trumpsters United”.

Примітно, що хвилі активізації АІД в соціальних мережах збігалися в часі з важливими політичними подіями Сполучених Штатів:

- Розпал президентських праймеріз (кінець 2015 р.,);
- Дебати демократів і дебати республіканців (січень 2016 р.);
- Після проголошення Трампа офіційним кандидатом від Республіканської партії (липень 2016 р.);
- Дебати між Гілларі Клінтон і Дональдом Трампом (осінь 2016 р.);
- 8 листопада 2016 р. – день голосування;
- дати розслідування стосовно хакерських атак Кремля після виборів (29 і 30 грудня 2016 р.).

Варто зазначити, що «тролям» вдалось вийти не лише далеко за межжі власних аккаунтів, а й за межі соціальних мереж взагалі. Твіти з 2752 фейкових аккаунтів Агенства інтернет-досліджень у Twitter потрапили на сайти таких популярних медіа-ресурсів, як-то: The Washington Post, Miami Herald, InfoWars та місцевих станцій ABC [75].

Втім, насправді, активність Агентства Інтернет-досліджень не обмежилась кампанією 2016 р. – тролі намагались посіяти розбрат між громадянами Сполучених Штатів до і після виборів. У період з 2013 по 2018 рр. кампанії тролів у соціальних мережах Facebook, Instagram та Twitter охопили десятки мільйонів користувачів у Сполучених Штатах. В результаті тридцять мільйонів американців за два роки, з 2015 по 2017 рр., поширювали

такий контент між своїми рідними та друзями та популяризували лайками, реакціями та коментарями [59, с. 3].

Отож, діяльність «Ольгінських тролів» свідчить про перманентні намагання Кремля підірвати американську демократію. Значний вплив тролів на громадян Сполучених Штатів пояснюється місцем соцмереж у їхньому житті – 85% дорослого населення США регулярно користується Інтернетом, 80% з клієнти Facebook [59, с. 39]. Агентство Інтернет-досліджень маніпулювало громадською думкою американців через використання найпопулярніших соціальних мереж, як-от Facebook, Instagram та Twitter (станом на 2 квартал 2016 р. користувачі проводили в цих мережах 128 хв, 173 хв та 159 хв відповідно) [33]. До того ж, для політичних акторів ці платформи є привабливими через можливість сегментувати аудиторію та швидко й дешево поширювати контент. Попри спрямування дезінформаційних месседжів на широке коло громадян, цільовою аудиторією Кремля були консерватори та активісти за права афроамериканців, а дискусії розгортались навколо расових та міграційних питань.

Особливу активність «тролі з Ольгіна» проявили під час виборів президента, позначаючи пости хештегами, зміст яких підтримував Дональда Трампа та створював негативний імідж Гілларі Клінтон. Річард Кларк, американський політик, аналітик та публіцист, який спеціалізується на боротьбі з тероризмом назвав проникнення тролів у соціальні мережі «переможною психологічною війною широкого масштабу» [103, с. 24]. Відтак, соцмережі стали інструментом політичного впливу, а фабрика тролів з Ольгіна – солдатами Кремля в руйнуванні західної демократії.

Російська Федерація як спадкоємиця Радянського Союзу веде пропаганду, як і в XX ст., – всеосяжно. Арсенал зброї Кремля у веденні Post-Cold War не обмежується творцями фейків – на службі державних інтересів стоять ще й хакери. Проблема вразливості американського кіберпростору загострилась у 2015-2016 рр. – атаками російських хакерів на кандидатку в президенти.

Група хакерів, що пов'язані з ГРУ з липня 2016 р. до червня 2016 р., отримали несанкціонований доступ до електронних листів, даних і меморандумів Національного комітету Демократичної партії. Викрадений контент спершу публікували через Guccifer 2.0 і DCLeaks.com, а згодом – на WikiLeaks. У січні 2017 р. розвідувальні служби США заявили, що «відомості, здобуті від Національного комітету Демократичної партії, ГРУ передало WikiLeaks». Таким чином, викрадені та оприлюднені Кремлем дані призвели до судового розслідування проти Гілларі Клінтон та змінили адженду ЗМІ.

Рупором кремлівської пропаганди традиційно стало медіа Russia Today, на поширення програм якого Росія щорічно витрачає 190 млн. дол. Згідно з дослідженням Nielsen – компанії, яка аналізує медійний ринок, – у 2012 р. RT здійснила найбільший ріст в порівнянні з іншими міжнародними новинними каналами: аудиторія в Нью-Йорку збільшилась втричі, у Вашингтоні – на 60% [2, с. 20].

У 2016 р. Russia Today англійською мовою активно транслювала попередньо «злитий» у WikiLeaks контент та стверджував, що Клінтон має проблеми зі здоров'ям і фінансується прихильниками ІДІЛу [86]. Примітно, що інтерв'ю з засновником ресурсу Джуліаном Асанджем, опубліковане за кілька днів до виборів під заголовком «Ассандж: Клінтон та ІДІЛ фінансуються за ті ж гроші, Трампу не дозволять перемогти» зібрало 2,2 млн переглядів та 115 тис лайків у Facebook [32]. А найпопулярніше серед громадськості відео RT з назвою «Як 100% «благодійності» Клінтонів пішла…собі ж» зібрало 9 млн. переглядів на платформах даного медіа [2, с. 14].

Джонатан Олбрарйт, дослідник соціальних медіа Колумбійського університету, проаналізував 36 тис твітів російських аккаунтів та виокремив 25 сайтів, на які здебільшого посилались тролі – RT посіла 19 сходинку [85]. Три облікові записи, що належать Russia Today та мали близько 6 млн.

підписників, витратили 274 100 дол. США на просування твітів у 2016 році [103, с. 85].

Значну лепту в поширення російських фейків внесли й провідні американські ЗМІ. Приміром, за 6 днів напередодні виборів в The New York Times кількість публікацій про е-мейли Клінтон прирівнялась до числа новин про всі політичні питання за попередні 69 днів. Дослідники Дункан Уоттс та Девід Ротшильд, проаналізувавши контент, створений «переважно професійними журналістами New York Times, Washington Post та Wall Street Journal» з'ясували, що скандали, пов'язані з Клінтон, згадуються значно частіше, ніж ті, що пов'язані з Трампом – 65 тис проти 40 тис. Показовим також є той факт, що ЗМІ в чотири рази більше писали про скандали з Клінтон, ніж про її політику, а у випадку з Трампом – месседжі про політику в півтора рази перевищували згадки про скандали [87].

В підтвердження факту впливу російських хакерів на адженду американських ЗМІ виступають заголовки, якими рясніли медіа напередодні виборів. Зокрема, варто виокремити деякі заголовки в New York Times за жовтень, як-то:

- «Уривки промов, що протікають, показують, як Гілларі Клінтон спокійно спілкується з Волл-стріт» (7 жовтня 2016 р.) [65];
- «Помічники Гілларі Клінтон тримали де Блазіо на відстані витягнутої руки, WikiLeaks показали електронні листи» (10 жовтня 2016 р.) [55];
- Основні моменти з електронних листів кампанії Клінтон: як боротися з

Сандерс і Байден» (10 жовтня 2016 р.) [54];

- «Дональд Трамп знайшов неймовірного союзника у WikiLeaks» (12 жовтня 2016 р.) [47];
- «Електронний лист про пропозицію Катару показує гострі етичні проблеми Фонду Клінтона» (15 жовтня 2016 р.) [49];

- «Урок WikiLeaks для місіс Клінтон» (21 жовтня 2016 р.) [34];
- «Пожертви для Фонду викликали роздратування помічників Гілларі Клінтон як показують електронні листи» (26 жовтня 2016 р.) [48];
- Розчарування та відданість Челсі Клінтон, показані у викрадених хакерами електронних листах» (27 жовтня 2016 р) [40];
- «CNN розлучається з Донною Бразиле, прихильницею Гілларі Клінтон» (31 жовтня 2016 р.) [42].

Крім того, значною мірою сама кампанія Дональда Трампа спиралась на викрадену Кремлем інформацію та фейки, що, радше, нагадувало танці на кістках, ніж політичну конкуренцію. Приміром, Трамп за підрахунками PolitiFact в інтерв'ю, промовах та виступах на дебатах в період з 10 жовтня по 8 листопада (останній місяць передвиборчої кампанії) згадав WikiLeaks та опубліковані там е-мейли Національного комітету Демократичної партії і Клінтон 164 рази [81]. На додачу, 14 жовтня старший син опублікував твіт зі змістом: «Для тих, хто має час прочитати про всю корупцію та лицемірство, е-мейли @wikileaks доступні тут: : http://wlsearch.tk/» [103, с. 168].

Найкраще вплив такої дезінформаційної кампанії прослідковується у коливанні вотуму довіри до кожного з кандидатів. Наприкінці жовтня Джеймс Комі, директор ФБР, заявив про поновлення розслідування у справі Клінтон, яке закрили в липні. За даними Центру публічної політики США, в період з 27 вересня по 2 жовтня 59% дорослого населення вважали, надавали перевагу у виборчій гонці Гілларі Клінтон. Втім, з 20 по 25 жовтня прослідковується різке падіння електоральних симпатій – на 11 пунктів, до 48%. Рейтинг Трампа в той час зріс з 27% до 35% [103, с. 175].

Таким чином, Кремль провів потужну інформаційну кампанію проти кандидатки в президенти Гілларі Клінтон, що стала можливою завдяки кіберзлочину – втручання хакерів в мережі Національного комітету Демократичної партії. Колишній спеціальний прокурор США Роберта Мюллера у звіті щодо втручання РФ у президентські вибори 2016 р. визначив

відповідальною в атак хакерську групу Fancy Bear, яка працює на ГРУ [13, с. 42]. Цей інцидент став одним з найгучніших, втім, не єдиним.

Крайня передвиборча гонка між Трампом та Байденом теж не обійшлась без уваги кремлівських хакерів.

На початку вересня у Microsoft заявили про низку кібератак, які спрямовувались на вибори, з боку груп, що пов'язують з Росією, Китаєм та Іраном. Зокрема, Strontium, відомий також як Fancy Bear задля збору розвідувальної інформації з вересня 2019 по вересень 2020 р. атакував понад 200 цілей, серед яких:

- Партії;
- Політичні консультанти, які співпрацювали як з республіканцями, так і з демократами;
- Аналітичні центри, як-то The German Marshall Fund of the United States, та правозахисні організації;
- Компанії, що надають фінансові послуги, та підприємства в сфері розваг та безпеки.

Показово, що у порівняні з атаками 2016 р. хакери дещо змінили тактику, розвинувши методику приховання операцій. На відміну від спір-фішингу, застосованому в 2016 р., тепер хакери використали атаки грубої сили, зокрема «розпилення паролів», що автоматизувало процес, та для маскування діяли через понад 1000 IP-адрес, деякі з яких пов'язані зі службою анонімізації Tor [37].

Крім того, починаючи з листопада 2019 р. серії кібератак піддалась українська газова компанія Burisma, в які працював син Джозефа Байдена Хантер. Вже в січні 2020 р. Fancy Bear, використовуючи фейкові вебсайти, які імітували сторінки входу дочірніх компаній, та фішинг, отримали доступ до мережі.

Варто зауважити три моменти, які вкотре підтверджують спробу Росії вплинути на політичну ситуацію в Сполучених Штатах. По-перше,

кібератаки на Burisma збіглися в часі з питанням про імпічмент Трампа. По-друге, несанкціонований доступ до сервера компанії хакери отримали незадовго до чергових виборів. По-третє, як зазначили працівники органів безпеки Сполучених Штатів, кіберзлочинці полювали за юридичними документами та фінансовими звітами [27].

Втім, кремлівські хакери піддають атакам американські державні та приватні мережі і поза електоральними процесами. Відтак, в грудні 2020 р. виявили кібератаку, здійснену через злам програмного забезпечення SolarWinds – «найбільшою і найвитонченішою, яку коли-небудь бачив світ», згідно з оцінкою Бреда Стім, президента Microsoft [80].

Зокрема атака поширилась на приблизно сотню американських компаній і дев'ять федеральних агентств, серед яких Міністерства юстиції, енергетики, фінансів, безпеки, торгівлі США, а також Пентагон та Національне агентство з ядерної безпеки. У спільній заяві Федерального бюро розслідувань (ФБР), Агентства кібербезпеки та безпеки інфраструктури (CISA), Офісу директора національної розвідки (ODNI) та Агентства національної безпеки (АНБ) від 5 січня 2021 р. йдеться про ймовірну відповідальність Росії за атаку, від якої постраждали 18 тисяч державних та приватних організацій у світі [10].

Вже на початку жовтня 2021 р. Reuters повідомило, що «підозрювані хакери з Росії, використовуючи програмне забезпечення SolarWinds та Microsoft для проникнення у федеральні агентства США, отримали доступ до інформації про розслідування контррозвідки, політику санкцій проти росіян, а також реагування США на COVID-19». Саме доступ до справ контррозвідки проти Росії назвали найбільшою втратою від даного кібернападу [68].

7 травня 2021 р. про атаку повідомила компанія Colonial Pipeline, трубопровід якої забезпечує дизелем та паливом 18 штатів Східного берега США на 45%. В результаті нападу компанія тимчасово призупинила роботу на 9 км дистанції. ФБР 9 травня підтвердило причетність до кіберзлочину

російської хакерської групи DarkSide [52]. Однак Colonial Pipeline постраждала від програми-вимагача, тобто хакери діяли з фінансових мотивів, тож компанія сплатила злочинцям 4,4 млн. дол. [25]. Через місяць після атаки, в червні, ФБР змогло конфіскувати кошти, сплачені хакерам, із віртуального гаманця. Проте, через падіння курсу біткоїна, компанія отримала лише 2,3 млн. дол [45].

Наприкінці травня, група Nobelium, яка ймовірно стоїть за атаками з використанням SolarWinds, отримавши доступ до американського агенстства з міжнародного розвитку через фішинг атакувала приблизно 3 тис облікових записів у 150 організаціях у 24 країнах, серед яких державні агентства, науково-дослідні інститути, консалтингові фірми та некомерційні організації. Втім, за словами Тома Берта віце-президента Microsoft з питань безпеки, найбільша частка атак припала на компанії Сполучених Штатів [70]

2 липня 2021 р. «колосальної і руйнівної» хакерської, за оцінкою фахівця з кібербезпеки Джона Гемонда, зазнала американська компанія-розробник програмного забезпечення для керування мережевою інфраструктурою Kaseya. Злочин із використанням програми-вимагача призупинив роботу принаймні 200 компаній в Сполучених Штатах, які користуються продуктами Kaseya, та вийшов за межі держави. До прикладу, атака паралізувала роботу 500 швецьких супермаркетів Coop [36].

Про протистояння на кібернетичному фронті свідчить також активність Сполучених Штатів проти Росії. Ще в жовтні 2018 р. Кіберкомандування США були здійснені наступальні операції щодо Агентства Інтернет-досліджень, більш відомого як «Тролі з Ольгіна». Таким чином, інцидент став свідченням реалізації принципу «defend forward», тобто превентивного захисту кіберпростору поза американськими мережами, прописаного в Національній стратегії – Америка «вдарила» по «тролях з Ольгіна» за втручання у вибори в 2016 р.

Отже, протистояння між Сполученими Штатами та Росією, початок якого сягає Холодної війни, набуло гібридного характеру поширилось на

інформаційний, зокрема кібернетичний фронт. Москва, притримуючись радянського стилю двосторонніх відносин з Вашингтоном, продовжує втручатись в хід американських виборів, проводячи дезінформаційні кампанії. Втім, звичну розвідку змінило кібершпигунство, яке здійснюють хакери-службовці ГРУ. Ефективність втручання кремлівських хакерів підтверджена перемогою Дональда Трампа у 2016 р. Однак, за 4 роки американські відомства дещо зміцнили свої інформаційно-комунікаційні системи, а громадяни – підвищили рівень критичного сприйняття інформації, тож кібератаки 2019-2020 рр. не посприяли переобранню одіозного кандидата-республіканця. Проте, криза безпекової політики у сфері кібернетичного захисту Сполучених Штатів не вирішена, що чітко прослідковується в кількості масштабах атак російських хакерських груп, що діють з метою отримання інформації чи викупу протягом крайніх двох років.

3.2. Основні напрямки зовнішньополітичної стратегії США в кібербезпековій політиці у відносинах з Росією, Україною та ЄС

Проблема загроз у кіберпросторі не обмежена кордонами, а відповідно її розв'язання потребує кооперації зусиль міжнародної співпраці. Показово, що Вашингтон приділяє особливу увагу ролі кібербезпекових питань у двосторонніх та багатосторонніх відносинах. Про це свідчать положення низки стратегій, прийнятих за різних адміністрацій:

- Приміром, Стратегія національної безпеки від 2010 р. задекларувала необхідність розробки міжнародних стандартів та норм поведінки державних акторів у кіберпросторі;
- Міжнародна стратегія для кіберпростору від 2011 р. [9] виокремила дипломатію як важливий інструмент забезпечення глобальної інформаційної безпеки та вказала на потребу розробки норм міжнародного права в сфері забезпечення інформаційної безпеки. Фактично цим документом Сполучені Штати підтвердили свою готовність адаптуватись до викликів сучасності, де серед усього вибудовувалась поліцентрична система міжнародних відносин, у якій Америка як держава з потужним інформаційним потенціалом виступає центральним гравцем;
- У Стратегії міністерства оборони для операцій у кіберпросторі від 2011 [3] зазначено, що розбудова міцних відносин з союзниками США та міжнародними партнерами є механізмом зміцнення колективної кібербезпеки;
- Автори Національної кіберстратегії Сполучених Штатів Америки від 2018 р. [11] приділили увагу перспективам нарощення міжнародного кіберпотенціалу шляхом покращення координації зусиль, аналітичного та технічного обміну, зокрема, акцентується на зменшенні рівня впливу транснаціональної кіберзлочинності та терористичної діяльності.

Окремо варто розглянути проєкт Закону про кібердипломатію від 2017 р., переданий Комітету з міжнародних справ у січні 2018 р. [7]. Законопроект

передбачає створення в межах Державного департаменту «Управління з питань кібернетики» та затвердженої Сенатом посади очільника з посольським рангом. До компетенції Офісу увійде координація дипломатичних зусиль Держдепартаменту в кіберпросторі, а також розв'язання проблем цифрової економіки та Інтернету. Крім того, Управління консультуватиме держсекретаря та вищих посадових осіб з питань даного спектру.

Отож, Сполучені Штати належним чином оцінюють роль міжнародного співробітництва, як для управління ризиками, так і для застосування економічних і соціальних можливостей, які надає кіберпростір. До того ж, такі зусилля передбачають комплексний підхід, адже безпека, економіка та захист прав людини у кіберпросторі взаємопов'язані. Відтак, з урахуванням американських потенціалу та амбіцій, Вашингтон намагається займати лідерську позицію в системі забезпечення міжнародної кібернетичної безпеки.

З огляду на використання державами наступальних операцій, нарощення кіберспроможностей та відсутність чіткого консенсусу про прийнятну поведінку в кіберпросторі, на початку століття світ постав перед значними ризиками. Сполучені Штати Америки, дотримуючись задекларованих положень, очолили розробку та впровадження стратегічної основи кіберстабільності, яка передбачала:

- Глобальне підтвердження застосування міжнародного права до діяльності держав у кіберпросторі;
- Вироблення добровільних норм прийнятної поведінки держави в мирний час;
- Застосування практичних заходів зміцнення довіри для зниження ризику помилкового сприйняття та ескалації у кіберпросторі [72].

Відтак Сполучені Штати долучились до розробки міжнародних галузевих документів [20, с. 47]. До таких належать:

- Конвенція з кіберзлочинності Ради Європи 2001 р., яка включає керівні принципи як для національних законодавств, так і для міждержавного співробітництва;
- «Керівні принципи щодо безпеки інформаційних систем і мереж» Організації економічного співробітництва та розвитку 2002 р., в які прописують механізми протидії кібертероризму та хакерам;
- «Всеосяжна Міжамериканська стратегія кібербезпеки: багатовекторний і комплексний підхід до створення кібербезпеки» Організації Американських Держав (ОАД) 2004 р. Документ є зобов'язанням держав-членів ОАД зміцнювати кібербезпеку, захищати об'єкти критичної інфраструктури та протидіяти кіберзагрозам.

Білий дім неодноразово вносив питання зміцнення міжнародної безпеки до порядку денного на світових форумах. До прикладу, у 2013 р. низка держав, серед яких США, КНР та РФ, дійшла консенсусу щодо того, що міжнародне право, зокрема Статут ООН, застосовується у кіберпросторі. Тобто, мається на увазі, що кіберпростір не є зоною «вільного вогню», а передбачає дотримання таких самих правил, що й фізичний світ. Згодом, у 2015 р. звіт Групи урядових експертів ООН з розробок у сфері інформації та телекомунікацій у контексті міжнародної безпеки (UN GGE) заклав основу для міжнародно визнаного урядового кодексу поведінки в кіберпрограмі. Документ GGE окреслив наявні та потенційні загрози в кіберпросторі, запропонував основні норми, правила та принципи відповідальної поведінки держав, а також заходи міжнародного партнерства та зміцнення довіри [6].

Таким чином, можна відзначити внесок Сполучених Штатів у формування фундаменту глобальної взаємодії в кіберсекторі. Втім, з розвитком інформаційно-комунікаційних технологій модернізуються і загрози національній, зокрема кібернетичній безпеці, а кіберполітика стала повноцінною галуззю двосторонніх відносин. Отож, варто розглянути як

Сполучені Штати співпрацюють з партнерами на прикладі конкретних держав.

Кібербезпека протягом багатьох років є одним з наріжних каменів американсько-російських двосторонніх відносин, отож особливої уваги заслуговує взаємодія Вашингтону та Москви в даній галузі. Цікаво, що 25 вересня 2020 р., незадовго до виборів і після кібератак хакерів, які вкотре намагались вплинути на електоральний процес, на офіційному сайті президента Росії Владіміра Путіна з'явилась заява про комплексну програму заходів з відновлення російсько-американської співпраці в галузі міжнародної інформаційної безпеки. Очільник Кремля звернувся до Сполучених Штатів з пропозицією схвалити ініціативу перезавантаження відносин в сфері використання інформаційно-комунікаційних технологій, яка передбачала чотири кроки:

1. Відновлення повномасштабного двостороннього регулярного міжвідомчого діалогу з питань забезпечення міжнародної інформаційної безпеки;

2. Підтримка безперервної ефективної роботи каналів зв'язку між компетентними установами обох держав по лінії центрів зменшення ядерної небезпеки, груп оперативного реагування на комп'ютерні інциденти та посадових осіб високого рівня, що займаються проблематикою міжнародної інформаційної безпеки;

3. Спільна розробка та укладання двосторонньої міжурядової угоди про запобігання інцидентам в інформаційному просторі за аналогією з радянсько-американською Угодою про запобігання інцидентам у відкритому морі та повітряному просторі над ним від 25 травня 1972 року;

4. Обмін гарантіями невтручання у внутрішні справи одне одного, зокрема у виборчі процеси, в тому числі з використанням ІКТ та високотехнологічних методів [90].

Втім, фактичне обговорення перспектив співпраці чи навпаки – конфронтації – в кіберпросторі між Джозефом Байденом та Владіміром

Путіним відбулось під час Женевського саміту. До того ж, розмова видалась аж надто прицільною: президент США передав очільнику Кремля перелік 16 секторів критичної інфраструктури, на яку заборонено спрямовувати хакерські атаки, інакше – Росія отримає контрудар. До списку, серед усього, увійшли сфери телекомунікації, охорони здоров'я та енергетики. Однак, доцільність та ефективність такого кроку сумнівна. По-перше, Путін отримав перелік найбільш вразливих та значущих для Сполучених Штатів зон. По-друге, Кремль отримав широке поле для маневрів, адже під забороною мали б бути усі державні та приватні організації.

Як стало відомо на початку листопада від New York Times, Женевська зустріч започаткувала низку секретних зустрічей між Сполученими Штатами та Росією, як-то три візити до Москви посадовців адміністрації Джозефа Байдена та бесіди з посадовцями адміністрації Путіна у Швейцарії та Фінляндії. Зокрема, приділили увагу питанням кібербезпеки: Енн Нойбергер, головна радниця Білого дому з кіберпитань та новітніх технологій провела серію онлайн-зустрічей з російською стороною. Як зазначає медіа, після тривалих дебатів в американському розвідувальному співтоваристві, розкрито імена кількох хакерів, які активно атакують США. Тож Сполучені Штати прагнуть пересвідчитись, чи дана інформація призведе до арештів відповідальних за злочини осіб, тобто, наскільки серйозною є позиція Путіна щодо сприяння в боротьбі з програмами-вимагачами та іншими кіберзлочинами [74].

Тобто, нова американська адміністрація прагне дійти певного консенсусу щодо застосування кіберзброї як з політичними, так і з фінансовими мотивами. Втім, як демонструє історія Радянського Союзу та сучасної Росії, вірити обіцянкам Путіна не варто. Тож Сполучені Штати зміцнюють власні інформаційно-комунікаційні системи та налагоджують співпрацю з міжнародними партнерами.

Одним з найбільш релевантних в даному випадку партнерів виступає Україна – держава, що початком гібридної російсько-української війни

фактично стала «випробувальним майданчиком». Хакерських атак зазнали приватні компанії та державні установи, серед яких ЦВК, Міністерство фінансів, «Укртелеком», «Ощадбанк», аеропорти «Бориспіль» та «Жуляни», та навіть об'єкт життєзабезпечення населення – «Прикарпаньяобленерго».

Відтак, зважаючи на досвід протистояння російській агресії у кіберпросторі, Сполученим Штатам є чому повчитись в України, і visa versa – враховуючи кібернечний потенціал офіційного Вашингтона, у такій співпраці зацікавлений і Київ.

Партнерство активізувалось з приходом до влади Джозефа Байдена. Приміром, 31 серпня 2021 року міністрами оборони обох держав Андрієм Тараном та Ллойдом Остіном підписано Стратегічну оборонну програму США та України. Документ, серед усього, охоплює і кібернетичну складову національної безпеки. Тобто, передбачає посилення співробітництва з питань кібербезпеки для стримування зловмисної кібердіяльності та ефективного захисту від супротивників [82].

Вже на початку осені, 3 вересня 2021 р., пройшла зустріч між представниками Адміністрації Державної служби спеціального зв'язку та захисту інформації України і Агентства кібербезпеки та безпеки інфраструктури США (CISA), за підсумками якої до кінця року планується підписання угоди про співпрацю між двома структурами, яка передбачає:

1. Обмін досвідом та інформацією щодо протидії агресії Російської Федерації у кіберпросторі, а також розробку спільних протоколів дій;
2. Формування платформи для обміну інформацією про кіберінциденти в інтересах системи управління інцидентами та відновлення після них;
3. Спільні дії щодо захисту критичної інформаційної інфраструктури та надання партнерам актуальної інформації для вдосконалення системи реагування на кіберінциденти;
4. Обмін досвідом в рамках системи управління ризиками, що забезпечить національну стабільність України;

5. Використання досвіду США в організації співпраці у сфері кібербезпеки з приватним сектором;

6. Реалізація конкретних проєктів міжнародної технічної допомоги щодо побудови мережі галузевих та регіональних операційних центрів безпеки (Security Operation Center) та груп реагування (CSIRT), які передбачені Стратегією кібербезпеки України;

7. Формування за сприяння США кадрового потенціалу з питань кібербезпеки шляхом проведення навчальних курсів на базі CISA, тренінгів [30].

Трохи згодом, 29 жовтня 2021 р. відбувся четвертий американсько-український кібердіалог, покликаний зміцнити двостороннє партнерство з питань кібербезпеки для подолання загроз, зокрема на фоні кібератак хакерськими групами, що пов’язані з Росією проти України та США.

Варто нагадати, що перші два пройшли у 2017 та 2018 рр. Ще тоді представники Києва та Вашингтона обговорили прогрес національних галузевих політик, крайні кіберінциденти та тенденції посилення загроз, а також окреслили вектор майбутньої співпраці. Крім того, сторони підтвердили готовність дотримуватися норм відповідальної поведінки держав в кіберпросторі, відповідно до норм міжнародного права. Результатом такої співпраці стало отримання українською стороною 10 млн. дол. на реалізацію проєктів з посилення кібербезпеки ОКР та виборчих систем [22].

Делегації розглянули ініціативи допомоги Україні з боку Сполучених Штатів, розроблені зі стейкхолдерами. Проєкти спиралися на реалізацію низки завдань в українському кіберсекторі, як-от:

1. Посилення кібербезпеки виборчих систем та критичної інфраструктури;

2. Підтримка впровадження національної кіберстратегії України;

3. Підвищення потенціалу кіберзахисту та реагування на інциденти;

4. Підвищення обізнаності щодо кібербезпеки;

5. Проведення тренінгів для спеціалістів з кібербезпеки та цифрової криміналістики [22].

Під час третьої зустрічі мова йшла про питання реагування на серйозні кіберінциденти, зміцнення критично важливої інфраструктури та безпеку мережі 5G. До того ж, увагу приділили міжнародній кіберполітиці та перспективам нарощення кіберпотенціалу. За підсумками даного кібердіалогу, що відбувся в березні 2020 р., Україна отримала 8 млн. дол. та чотирирічне фінансування на реформи в кіберсекторі від USAID загальним обсягом до 38 млн. дол. [43]. Обіцянка Сполучених Штатів фінансово допомогти Україні стала реакцією на запит української влади до ФБР за підтримкою в розслідуванні кібератаки на українську газову компанію Burisma. Виділені кошти спрямують, зокрема, на розвиток потенціалу працівників кіберсектору, а також підтримку реформи нормативно-правового забезпечення. Ефективність співпраці підтверджена цифрами: в період з січня по квітень 2021 р. СБУ разом із американськими спецслужбами запобігла 350 кібератакам від хакерів, що працюють на російську розвідку [78].

Відтак, проведення діалогів з кібербезпеки та супутня фінансова підтримка Вашингтону підтверджує спільну для двох сторін візію щодо забезпечення відкритого і надійного кіберпростору, в межах якого всі держави демонструють відповідальну поведінку.

Крім того, Сполучені Штати підтримали розвиток нормативно-правового забезпечення України в сфері кіберпростору та здійснили зустрічний крок – Конгрес США в лютому 2018 р. схвалив законопроєкт про співпрацю з Україною в кіберсфері. Документ націлений на сприяння Україні вдосконалити стратегію кібербезпеки. До того ж, передбачається посилення захисту комп'ютерних мереж та забезпечення ширших перспектив для міжнародного інформаційного обміну. Варто наголосити, що цим Законом для Україна разом зі США виконуватиме лідерську роль в посиленні

кібербезпеки Центральної і Східної Європи. Наразі законопроєкт переданий до комітету з міжнародних відносин [8].

Отож рівень кіберзагроз, що зростає, додає питання координації зусиль в сфері захисту кіберпростору до пріоритетних завдань двосторонніх відносин. В контексті американсько-української співпраці необхідність ведення кібердіалогу зумовлена наявністю спільного ворога – Кремля, а його ефективність підтверджена здатністю спецслужб протистояти хакерам.

Вже згаданий Законопроєкт про співпрацю з Україною має на меті підвищення рівня захисту кіберпростору Європи. Втім, партнерство в даній сфері з ЄС почалось ще в 2010 р. – згідно з домовленостями саміту Сполученими Штатами та Євросоюзом лідери створили Робочу групу з кібербезпеки та кіберзлочинності як основу трансатлантичних кіберпрограм. Робоча група структурно функціонує за чотирма експертними підгрупами, які сфокусовані на:

1. управлінні кіберінцидентами;
2. партнерстві між державним та приватним секторами;
3. підвищенні обізнаності;
4. кіберзлочинністю.

Фактичними проявами такої співпраці стали, приміром, теоретично-тренувальні заходи з протидії кіберінцидентів між партнерами у 2011 р., робочі наради за участі представників державного та приватного секторів щодо промислових систем управління та інтелектуальних мереж та діяльність, спрямована на посилення безпеки доменних імен. Крім того, варто виокремити запущений у грудні 2012 р. Глобальний альянс проти сексуального насильства в Інтернеті на основі спільної ініціативи комісара Мальмстрьом та генерального прокурора Холдера після діалогу в Робочій групі ЄС-США. Таким чином, 53 держави зобов’язались боротись з сексуальним насильством над дітьми в мережі: виявляти, захищати та підтримувати жертв, переслідувати злочинців та підвищувати обізнаність [51].

В контексті співпраці між США та ЄС також створено діалог інформаційного суспільства для вирішення питань, пов'язаних з інформаційно-комунікаційними технологіями та управління Інтернетом. Деякі з питань виносяться на обговорення на Трансатлантичній економічній раді.

Ріст рівня загроз зумовив потребу тіснішої співпраці – вкотре питання підняли на Брюсельському саміті 26 березня 2014 р. Наразі пріоритетними напрямами роботи залишаються: підвищення обізнаності щодо потенційних кіберзагроз та шляхів протидії, розробка стандартів управління ризиками, протидія атакам та просування норм Будапештської конвенції про кіберзлочинність.

Крім того, співпраця між США та ЄС реалізовується на базі таких платформ, як-от AEGIS та DISCOVERY.

AEGIS – ініціатива, націлена на сприяння кооперації зусиль щодо досліджень та інновацій у сфері кібербезпеки та конфіденційності між Євросоюзом та Америкою [95]. Для реалізації поставлених завдань AEGIS проводить міжнародні семінари, підготує звіти про ландшафт кібербезпеки та рекомендації для подальшого розвитку та зміцнення інформаційно-комунікаційних систем. Консорціум проєкту складають провідні європейські та американські експерти сектору. Зокрема, в межах ініціативи Представництво ЄС в США та Інститут Брукінгса 8-9 липня 2020 р. провели Вашингтонський форум з питань оборони ЄС. Одним з питань порядку денного стало обговорення технологій 5G, Штучного Інтелекту, а також співробітництва між США, ЄС та НАТО.

Інша ініціатива, DISCOVERY – Трансатлантичний ІКТ Форум, в межах якого над співпрацею між ЄС, США та Канадою в галузі забезпечення безпеки інформаційно-комунікаційних систем працює Робоча група з кібербезпеки [96]. Однак, остання активність була в січні 2017 р. – Форум «Бачення Європи цифрової трансформації».

За час каденції Дональда Трампа підходи до кіберполітики Сполучених Штатів Америки та Європейського Союзу дещо розійшлись. Сполучені Штати здійснили стратегічний відхід до постійної конкуренції в кіберпросторі, спираючись на наступальний кіберпотенціал. Європейський Союз – зосередився на спільних дипломатичних превентивних заходах в запобіганні конфліктів. Розбіжність у підходах чітко проглядається в сконцентрованості Сполучених Штатів на принципі «defend forward» та, відповідно, незгоді з деякими нормами відповідальної поведінки держав в кіберпросторі. Однією з таких є положення про захист публічного ядра Інтернету, згідно з яким «державні та недержавні суб'єкти не повинні ні здійснювати, ні свідомо допускати діяльність, яка навмисно та істотно завдає шкоди загальній доступності чи цілісності публічного ядра Інтернету» [1, с. 30]. Дану норму підтримують країни-члени Євросоюзу, зокрема через ініціативи, до яких США за адміністрації Трампа не доєднались, – Паризький заклик щодо довіри та безпеки в кіберпросторі та Глобальна комісія зі стабільності в кіберпросторі. Крайніми роками аналітичні центри розглядали можливості посилення партнерства, зокрема німецький фонд «Нова відповідальність» розробив «Ініціативу досліджень трансатлантичної кіберполітики», втім, зближення не відбулось [77].

Крім того, EU Cyber Direct – ініціатива ЄС з кібердипломатії, метою якої є визначення можливостей для конвергенції між ЄС та іншими зацікавленими сторонами щодо застосування наявних та розробки нових норм міжнародного права в кіберпросторі – визначила ключові позиції співпраці між США та ЄС в кіберсекторі:

- взаємодопомога в підвищенні стійкості
- досягнення спільного розуміння загроз і можливостей
- покращення потенціалу кіберфахівців [76].

Натомість Джозеф Байден встиг пообіцяти «врятувати зовнішню політику після Дональда Трампа», а саме «побудувати і підтримувати

відносини, визначивши точки перетину інтересів в управлінні конфліктами». Така позиція вказує на перспективи подальшої співпраці в галузі кібербезпеки. Деякі зрушення вже відбулись – приміром, в листопаді 2021 р. Сполучені Штати доєднались до Паризького заклику [97].

Отож, після чотирирічного послаблення відносин між ЄС та США, зокрема в питаннях кіберзлочинності, адміністрація Джозефа Байдена дає надію на зміцнення співпраці, адже, попри різні стратегії, спільними є загрози, а відповідно – потреба колективного захисту та протидії.

Підсумовуючи, варто ще раз зауважити: Сполучені Штати Америки, спираючись на внутрішнє законодавство, зробили чималий внесок в розбудову міжнародної співпраці з питань захисту кіберпростору та безпеки Інтернету. Проте, очевидно, що значну роль в екосистемі глобальної кібернетичної безпеки та дипломатії відіграють двосторонні відносини між Сполученими Штатами Америки та Російською Федерацією – одними з найбільш розвинених кібердержав. Останніми роками діяльність двох акторів в кіберпросторі радше нагадувала конфронтацію, ніж співпрацю. Однак, зі вступом на посаду Джозеф Байден активізував діалог з Владіміром Путіним щодо невтручання в інформаційно-комунікаційні мережі об’єктів критичної інфраструктури. Звісно, виокремлення 16 заборонених для атак цілей викликає деякі питання до Білого Дому, однак суттєво, що кіберполітика займає чільне місце в американсько-російському дискурсі.

Щодо України – заданий Трампом вектор двосторонньої співпраці шляхом проведення діалогів з кібербезпеки з подальшим фінансуванням української сторони продовжує реалізовуватись адміністрацією Джозефа Байдена. Ефективність партнерства вже підтверджена здатністю українських спецслужб протистояти атакам. Втім, суттєвим зрушенням стане прийняття закону про співпрацю з Україною в кіберсекторі. По-перше, нормативно-правовий акт закріпить за Києвом та Вашингтоном лідерські ролі в зміцненні кіберпростору Європи. По-друге, документ стане першим законом США, де «Україна» винесена в назву.

Аналіз трансатлантичної співпраці демонструє деякий застій в період президентства Дональда Трампа через розбіжності в стратегіях та візіях кіберполітики: поки ЄС прагнув захисти свій кіберпростір, США робили ставку на наступальні операції. Втім, обидва гравці мають спільний фундамент та спільні загрози, отож прихід до влади Джозефа Байдена відновлює перспективи координації зусиль між Європейським Союзом та Сполученими Штатами Америки.

ВИСНОВКИ

Ввійшовши в XXI століття, світ постав перед новими можливостями з одного боку та викликами і загрозами – з іншого. До першої категорії належить онлайн-освіта, Інтернет-банкінг та необмежена кордонами комунікація для громадян, автоматизовані системи управління для корпорацій, цифрова дипломатія та електронне врядування для урядів. До другої – крадіжки грошей і конфіденційних даних, відмова в обслуговуванні та кібершпигунство.

Кіберпростір – стратегічний об’єкт держави та п’ятий фронт для ведення гібридних протиборств. Тож очевидно, що екосистема кібернетичного простору позначається на внутрішній та зовнішній політиці держави, а також впливає на її рівень на міжнародній арені. Відтак потреба формування галузевої політики обґрунтована.

Теракти 11 вересня 2001 р. фактично продемонстрували незахищеність навіть наддержав перед транскордонними загрозами та вказали на потребу формування політики захисту. Розуміючи, що наступний інцидент може трапитися з використанням інформаційно-комунікаційних технологій, тобто у кіберпросторі, Сполучені Штати взялися за розробку політики кібербезпеки.

Процес становлення кіберполітики Сполучених Штатів Америки розпочав 43-й президент, Джордж Буш-молодший. У 2003 р. була прийнята перша та основоположна Стратегія кібербезпеки США. Вагомо, що саме Буш визнав кіберпростір – ареною протиборства, а також почав розробку політики безпеки не лише в урядовому секторі, але й в об’єктах критичної інфраструктури приватного поля. Кожна наступна законодавча ініціатива спитається на положення та норми, які задекларував Білий дім під керівництвом Джорджа Буша.

Поступ у галузі відбувся при кожній з чотирьох досліджуваних адміністрацій. Втім, найбільший внесок за дві каденції здійснив 44-й президент США.

По-перше, Барак Обама «Президентською політичною директивою», більш відомою як PPD-20, розпочав створення механізму наступальних операцій у кіберпросторі, тобто – застосування інформаційних технологій як зброї у веденні гібридного протистояння.

По-друге, значну увагу адміністрація Барака Обами приділяла міжнародній співпраці. Зокрема, під його керівництвом вийшла низка документів, які наголошували на глобальному контексті кіберзагроз та, відповідно, обґрунтували потребу колегіальної реакції міжнародної спільноти, – Стратегія національної безпеки 2010 р., Міжнародна стратегія для кіберпростору від 2011 р. та Стратегія Міністерства оборони для операцій у кіберпросторі. Таким чином Білий дім підтвердив лідерські амбіції на міжнародній арені, зокрема в кризовому менеджменті.

По-третє, Сполучені Штати за Барака Обами розробили типологію джерел загроз і виокремили Російську Федерацію та Китайську Народну Республіку як основні загрози національним інтересам США. Наступним суттєвим напрацюванням адміністрації Барака Обами став указ «Про арешт власності осіб, причетних до серйозних протиправних дій у кіберпросторі». Даний документ надав право уряду Сполучених Штатів накладати санкції на фізичних та юридичних осіб, винних у скоєнні кібератак на об’єкти критичної інфраструктури та присвоєнні в результаті коштів або інших активів. Завдяки механізмам, закладеним у цьому нормативно-правовому акті, в грудні 2016 р. було прийнято санкції проти Російської Федерації.

Чергове загострення проблеми вразливості кіберпростору як складової інформаційної, зокрема кібернетичної, безпеки для Сполучених Штатів Америки відбулось під час передвиборної кампанії 2016 р. Кремль провів успішну комплексну дезінформаційну кампанію, яку розпочали хакери Fancy Bear, продовжили «Тролі з Ольгіна», а завершили американські журналісти.

Метою Росії була негативізація іміджу Гілларі Клінтон та, відповідно, сприяння кампанії Дональда Трампа.

Показово, що Москва, притримуючись радянського стилю двосторонніх відносин з Вашингтоном, продовжує втручатись у хід американських виборів, проводячи дезінформаційні кампанії. Втім, звичну розвідку змінило кібершпигунство, яке здійснюють хакери-службовці ГРУ. Таким чином кіберпростір було використано як арену глобального протиборства.

Отож, і американців, і міжнародну спільноту цікавило, якою буде кіберполітика Дональда Трампа, адже його перемозі посприяла Росія саме з використанням кібератак.

Аналізуючи галузеву діяльність Дональда Трампа, варто виокремити моменти спірного прогресу та регресу. Перший полягає у продовженні політики Барака Обами щодо наступальних операцій. Дональд Трамп прирівняв Кіберкомандування до бойового підрозділу та скасував PPD-20, яка передбачала погодження потенційних операцій на високому рівні. Крім того, розподілення бюджетних коштів при адміністрації Дональда Трампа надавало пріоритет наступальних операції, а не захисту інформаційно-комунікаційної інфраструктури.

Другий, тобто регрес, спричинений суб'єктивними звільненнями кіберфахівців, як-от Кріса Кребса, керівника Агенства з кібербезпеки та безпеки інфраструктури США (CISA) за визнання Агентством заяви президента-республіканця про шахрайство під час виборів безпідставними. Вагомо, що при президентстві Дональда Трампа прослідковується певна стагнація міжнародної співпраці, зокрема щодо партнерства з Європейським Союзом.

Політика нинішнього президента, Джозефа Байдена, контрастує з баченням попередника та, певно мірою, нагадує діяльність адміністрації Барака Обами, в якій Байден серед усього займався питаннями кібербезпеки. Першим кроком чинного президента стало формування команди фахівців.

Однак, слабким місцем такої кіберкоманди є відсутність спеціалістів приватного поля – новопризначені обіймали релевантні посади в адміністрації Барака Обами, тобто належали до урядового сектору.

З огляду на місце Сполучених Штатів Америки в сучасній системі міжнародних відносин та інформаційно-комунікаційний потенціал держави, Білий дім з початку століття демонструє лідерські амбіції у формуванні політики глобальної кібербезпеки. Відтак офіційний Вашингтон здійснив чималий вклад у розбудову міжнародної співпраці з питань захисту кіберпростору та безпеки Інтернету, зокрема у розробку міжнародних галузевих документів, як-от: Конвенція з кіберзлочинності Ради Європи 2001 р. та Керівні принципи щодо безпеки інформаційних систем і мереж 2002 р.

Проте, очевидно, що значну роль в екосистемі глобальної кібернетичної безпеки та дипломатії відіграють двосторонні відносини між Сполученими Штатами Америки та Російською Федерацією – держав з потужним кіберпотенціалом. Крайніми роками взаємодія двох акторів в кіберпросторі радше нагадувала конфронтацію, ніж співпрацю. Втім, вже на початку каденції Джозеф Байден активізував діалог з Владіміром Путіним щодо невтручання в інформаційно-комунікаційні мережі об’єктів критичної інфраструктури. Отож питання кіберполітики наразі набуло пріоритетного значення в американсько-російському дискурсі.

Аналізуючи двосторонню американсько-українську співпрацю, варто наголосити на зацікавленості у ній обох держав, адже і Україна, і Сполучені Штати мають досвід протидії спільному кіберворогу – Кремлю. Відтак, Білий дім під керівництвом Джозефа Байдена рухається в напрямі, який задав Дональд Трамп, та продовжує проводити кібердіалоги з подальшим фінансуванням української сторони. Ефективність партнерства вже підтверджена здатністю українських спецслужб протистояти атакам. Прогресом для офіційного Києва стане прийняття закону про співпрацю з Україною в кіберсекторі, адже по-перше, нормативно-правовий акт закріпить

за сторонами лідерські ролі в зміцненні кіберпростору Європи. По-друге, документ стане першим законом США, де «Україна» винесена в назву.

Аналіз трансатлантичної співпраці демонструє деякий застій у період президентства Дональда Трампа через розбіжності в баченні кіберполітики: поки Європейський Союз прагнув захистити свій кіберпростір, Сполучені Штати Америки робили ставку на наступальні операції. Однак обидва гравці мають спільний фундамент та спільні загрози, отож прихід до влади Джозефа Байдена відновлює перспективи координації зусиль між ЄС та США.

Отже, кіберпростір – середовище можливостей для реалізації державних інтересів, як і середовище загроз для національної і міжнародної безпеки. Білий дім при чотирьох президентах протягом 20 років зумів визначити джерела загроз, визначити пріоритети, розробити механізми оборони і контрнаступу та взяти участь у зміцненні глобальної безпеки шляхом реалізації двосторонньої та багатосторонньої співпраці, а також у рамках міжнародних організацій. Втім, разом із розвитком інформаційно-комунікаційних технологій, модернізується інструментарій злочинців, отож Сполучені Штати змушені і надалі зміцнювати мережі та швидко виявляти, реагувати на загрози та ліквідовувати наслідки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Нормативно-правові документи

1. Advancing cyberstability final report november 2019. Global commission on the stability of cyberspacy. 2019. P. 52. URL: https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf (Last accessed: 5.10.2021)

2. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. Office of the Director of National Intelligence. 2017. P. 25. URL: ICA_2017_01.pdf (dni.gov) (Last accessed: 15.10.2021)

3. Department of Defense Strategy for Operating in Cyberspace. Department of Defense. 2011. P.19. URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (Last accessed: 5.08.2021)

4. Executive Order on Improving the Nation's Cybersecurity. The White House. 2021. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (Last accessed: 15.09.2021)

5. Presidential Policy Directive/PPD-20. 2012. P.18. URL: https://irp.fas.org/offdocs/ppd/ppd-20.pdf (Last accessed: 15.09.2021)

6. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly of the United Nations. 2015. P. 17. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (Last accessed: 15.10.2021)

7. H.R.3776 – Cyber Diplomacy Act of 2018. URL: https://www.congress.gov/bill/115th-congress/house-bill/3776/text?q=%7B%22search%22%3A%5B%22cyber+diplomacy+act%22%5D%7D&r=1 (Last accessed: 18.10.2021)

8. H.R.1997 – Ukraine Cybersecurity Cooperation Act of 2017. URL: https://www.congress.gov/bill/115th-congress/house-bill/1997 (Last accessed: 18.10.2020)

9. International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World. The White House. P. 30. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Last accessed: 12.09.2021)

10. Joint statement by The Federal Bureau of Investigation (FBI), The Cybersecurity and Infrastructure Security Agency (CISA), The Office of the Director of National Intelligence (ODNI), and The National Security Agency (NSA). CISA. 2021. URL: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure (Last accessed: 10.10.2021)

11. National Cyber Strategy. The White House. 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Last accessed: 8.09.2021)

12. National Plan for Information Systems Protection. The White House. 2000. P. 199. URL: https://irp.fas.org/offdocs/pdd/CIP-plan.pdf (Last accessed: 17.10.2021)

13. Report On The Investigation Into Russian Interference In The 2016 Presidential Election. U.S. Department of Justice. 2019. P. 448. URL: https://www.justice.gov/archives/sco/file/1373816/download (Last accessed: 2.10.2021)

14. S.2383 - CLOUD Act. 2018. URL: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text (Last accessed: 2.10.2021)

15. The National Strategy to Secure Cyberspace. The White House. 2003. URL: https://georgewbush-whitehouse.archives.gov/pcipb/ (Last accessed: 3.08.2021)

16. The Comprehensive National Cybersecurity Initiative. Executive office of the president of the USA. 2008. P.5 URL: https://breakinggov.sites.breakingmedia.com/wp-content/uploads/sites/4/2012/05/cybersecurity.pdf (Last accessed: 5.08.2021)

17. The DoD Cyber Strategy. Department of Defense. 2015. P.42. URL: 764848 (1).pdf (Last accessed: 22.09.2021)

18. The Global Risks Report 2020/ World Economic Forum. 2020. P.102. URL: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (Last accessed: 27.09.2021)

Інтернет-ресурси

19. Американський трубопровід відновлює роботу після кібератаки. Економічна правда. 2021. URL: https://www.epravda.com.ua/news/2021/05/13/673816/ (дата звернення: 11.11.2021)

20. Бережна М.С. Розвиток інформаційної безпеки США: практичні кроки Барака Обами. Вісник Східноукраїнського Національного Університету ім. В. Даля №8(197). 2013. С. 46-52. URL: http://dspace.snu.edu.ua:8080/jspui/bitstream/123456789/3316/1/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA_8%28197%29_2_2013.pdf#page=46 (дата звернення: 2.09.2021)

21. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник. Київ. 2015. 288 с. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf (дата звернення: 18.11.2021)

22. Другий американсько-український діалог з кібербезпеки. Посольство США в Україні. 2018. URL: https://ua.usembassy.gov/uk/cybersecurity-bilat/ (дата звернення: 9.11.2021)

23. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. Монографія. Київ. 2014. 328 с. URL:

http://old2.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf (дата звернення: 16.11.2021)

24. Зернецька О. В. Глобальна комунікація. Наукова думка. Київ, 2017. 352 с. URL: https://ivinas.gov.ua/publikatsiji/novi-vydannia-instytutu/zernetska-ov-hlobalna-komunikatsiia.html (дата звернення: 5.10.2021)

25. Павлюк О. США повернули частину викупу, який Colonial Pipeline заплатила хакерам. Але через падіння біткоїна він вартує ще менше. Громадське. 2021. URL:https://hromadske.ua/posts/ssha-povernuli-chastinu-vikupu-yakij-colonial-pipeline-zaplatila-hakeram-ale-cherez-padinnya-bitkoyina-vin-vartuye-she-menshe (дата звернення: 8.11.2021)

26. Полтавець Ю. Інформаційно-технологічні атаки і способи захисту кіберпростору: новітні тактики гібридних війн. Навчальний посібник «Гібридна війна і журналістика проблеми інформаційної безпеки». Вид-во НПУ імені М. П. Драгоманова. Київ. 2018. С.246-263. URL: http://enpuir.npu.edu.ua/bitstream/handle/123456789/22257/Poltavets%20246-263.pdf;jsessionid=FE30C195A57B6BD65268DC98A8FE6C54?sequence=4 (дата звернення: 16.11.2021)

27. Прищепа Я. Російські хакери зламали сервери 95 кварталу та Burisma – NYT. Суспільне.Новини. 2020. URL: https://suspilne.media/8798-rosijski-hakeri-zlamali-serveri-95-kvartalu-ta-burisma---nyt/ (дата звернення: 8.11.2021)

28. Садомська Б. Кіберполітика Сполучених Штатів: успадкована від Трампа й скерована Байденом. Аналітичний центр ADASTRA. 2021. URL: https://adastra.org.ua/blog/kiberpolitika-spoluchenih-shtativ-uspadkovana-vid-trampa-j-skerovana-bajdenom (дата звернення: 5.10.2021)

29. Садомська Б. Сполучені Штати напередодні виборів: кібератаки набирають обертів. Аналітичний центр ADASTRA. 2020. URL: https://adastra.org.ua/blog/spolucheni-shtati-naperedodni-viboriv-kiberataki-nabirayut-obertiv (дата звернення: 5.10.2021)

30. Розпочинаємо співпрацю з Агентством з кібербезпеки та безпеки інфраструктури Держдепу США, - Держспецзв'язку. Урядовий портал. 2021. URL: https://www.kmu.gov.ua/en/news/rozpochinayemo-spivpracyu-z-agentstvom-z-kiberbezpeki-ta-bezpeki-infrastrukturi-derzhdepu-ssha-derzhspeczvyazku (дата звернення: 8.11.2021)

31. ABC News/Washington Post poll: 2016 election tracking no. 9. 2016. URL: https://www.langerresearch.com/wp-content/uploads/1184a92016ElectionTrackingNo9.pdf (Last accessed: 15.10.2021)

32. Assange: Clinton & ISIS funded by same money, Trump won't be allowed to win. RT World News. 2016. URL: https://www.rt.com/news/365299-assange-pilger-saudi-clinton/ (Last accessed: 29.10.2021)

33. Average daily time spent with selected social networks among selected social media users worldwide as of 2nd quarter 2016. Statista. 2016. URL: https://www.statista.com/statistics/267043/daily-usage-per-social-network/ (Last accessed: 15.10.2020)

34. A WikiLeaks Lesson for Mrs. Clinton. The New York Times. 2016. URL: https://www.nytimes.com/2016/10/22/opinion/a-wikileaks-lesson-for-mrs-clinton.html (Last accessed: 29.10.2021)

35. Beidleman, S. Defining and deterring cyber war. U.S. Army War College. 2009. P.40. URL: https://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf (Last accessed: 15.11.2021)

36. Bajak, F., Tucker, E., O'brien, M. Ransomware hits hundreds of US companies, security firm says. AP News. 2021. URL: https://apnews.com/article/business-technology-3011c6037bda9ac11b1249a4beb13b06 (Last accessed: 5.10.2021)

37. Burt, T. New cyberattacks targeting U.S. elections. Microsoft. 2020. URL: https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/ (Last accessed: 5.09.2021)

38. Cambridge Advanced Learner's Dictionary. URL: https://dictionary.cambridge.org/rucyber?q=cyber- (Last accessed: 15.11.2021)

39. Cavelty, M. Cyberwar: concept, status quo, and limitations. Center for Security Studies ETH Zurich. 2010. P. 3. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-71.pdf (Last accessed: 15.11.2021)

40. Chelsea Clinton's Frustrations and Devotion Shown in Hacked Emails. The New York Times. 2016. URL: https://www.nytimes.com/2016/10/28/us/politics/bill-chelsea-clinton-foundation.html (Last accessed: 29.10.2021)

41. Cheney, K., Wheaton S. The most revealing Clinton campaign emails in WikiLeaks release. Politico. 2016. URL: https://www.politico.com/story/2016/10/john-podesta-wikileaks-hacked-emails-229304 (Last accessed: 29.10.2021)

42. CNN Parts Ways with Donna Brazile, a Hillary Clinton Supporter. The New York Times. 2016. URL: https://www.nytimes.com/2016/11/01/us/politics/donna-brazile-wikileaks-cnn.html (Last accessed: 29.10.2021)

43. Coble, S. US to Give Ukraine $8m for Cybersecurity. Infosecurity. 2020. URL: https://www.infosecurity-magazine.com/news/us-to-give-ukraine-8m-for/ (Last accessed: 5.11.2021)

44. Cybersecurity information sharing act of 2015 procedures and guidance. CISA. 2020. URL: https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance (Last accessed: 9.09.2021)

45. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside. Department of Justice. 2021. URL: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (Last accessed: 5.11.2021)

46. Diamond, J. Donald Trump lavishes praise on 'leader' Putin. CNN. URL: https://edition.cnn.com/2015/12/18/politics/donald-trump-praises-defends-vladimir-putin/ (Last accessed: 29.10.2021)

47. Donald Trump Finds Improbable Ally in WikiLeaks. The New York Times. 2016. URL:https://www.nytimes.com/2016/10/13/us/politics/wikileaks-hillary-clinton-emails.html (Last accessed: 29.10.2021)

48. Donations to Foundation Vexed Hillary Clinton's Aides, Emails Show. The New York Times. 2016. URL:https://www.nytimes.com/2016/10/27/us/politics/bill-hillary-clinton-foundation-wikileaks.html (Last accessed: 29.10.2021)

49. Email about Qatari Offer Shows Thorny Ethical Issues Clinton Foundation Faced. The New York Times. 2016. URL: https://www.nytimes.com/2016/10/16/us/politics/wikileaks-bill-clinton-foundation.html (Last accessed: 29.10.2021)

50. Epstein, J., Mehrotra, K. Biden Proposes Billions for Cybersecurity After Wave of Attacks. Bloomberg. 2021. URL: https://www.bloomberg.com/news/articles/2021-05-18/biden-proposes-billions-for-cybersecurity-after-wave-of-attacks (Last accessed: 15.09.2021)

51. EU-US Cooperation on Cyber Security & Cyberspace. The European American Chamber of Commerce. 2020. URL: https://eaccny.com/news/eu-us-cooperation-on-cyber-security-cyberspace/ (Last accessed: 11.11.2021)

52. FBI Statement on Network Disruption at Colonial Pipeline. FBI National Press Office. 2021. URL: https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline (Last accessed: 20.10.2021)

53. Healey, J.The Cyber Budget Shows What the U.S. Values—And It Isn't Defense. Law Fare. 2020. URL: https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense (Last accessed: 9.09.2021)

54. Highlights from the Clinton Campaign Emails: How to Deal with Sanders and Biden. The New York Times. 2016. URL:

https://www.nytimes.com/2016/10/10/us/politics/hillary-clinton-emails-wikileaks.html (Last accessed: 29.10.2021)

55. Hillary Clinton Aides Kept de Blasio at Arm's Length, WikiLeaks Emails Show. The New York Times. 2016. URL:https://www.nytimes.com/2016/10/11/nyregion/clinton-aides-kept-de-blasio-at-arms-length-wikileaks-emails-show.html (Last accessed: 29.10.2021)

56. Gibbs, S. China planted chips in Apple and Amazon servers, report claims. The Guardian. 2018. URL: https://www.theguardian.com/technology/2018/oct/04/china-planted-chips-on-apple-and-amazon-servers-report-claims (Last accessed: 25.09.2021)

57. Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election. Department of Justice. 2018. URL: https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election (Last accessed: 25.10.2021)

58. Hillary Clinton says Vladimir Putin's Crimea occupation echoes Hitler. The Guardian. 2014. URL: https://www.theguardian.com/world/2014/mar/06/hillary-clinton-says-vladimir-putins-crimea-occupation-echoes-hitler (Last accessed: 29.10.2021)

59. Howard, P., Ganesh, B., Liotsiou D., Kelly, J., François, C. The IRA, Social Media and Political Polarization in the United States, 2012-2018. 2019. P.48. URL: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs (Last accessed: 28.10.2021)

60. ITU Toolkit For Cybercrime Legislation. ITU. ITU. Committed to connecting the world. 2009. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx (Last accessed: 16.11.2021)

61. Kannan, V. What Really Happened in the Cyber Command Action Against Iran? Law Fare. 2019. URL: https://www.lawfareblog.com/what-really-happened-cyber-command-action-against-iran (Last accessed: 25.09.2021)

62. Kramer, F., Wentz, L. Cyber Influence and International Security. Chapter 14. National Defense University Press. 2008. P. 16. URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-14.pdf?ver=2017-06-16-115054-273 (Last accessed: 16.11.2021)

63. Labott, E. Clinton cites 'serious concerns' about Russian election. CNN. 2011. URL: https://edition.cnn.com/2011/12/06/world/europe/russia-elections-clinton/ (Last accessed: 29.10.2021)

64. Langevin, J., McCaul, M. Securing Cyberspace for the 44th Presidency. Semantic Scholar. 2008. URL: https://www.semanticscholar.org/paper/Securing-Cyberspace-for-the-44th-Presidency-Langevin-McCaul/59b999548bacbb8345dc6a720a9562e83d33ef51 (Last accessed: 21.08.2021)

65. Leaked Speech Excerpts Show a Hillary Clinton at Ease with Wall Street. The New York Times. 2016. URL:https://www.nytimes.com/2016/10/08/us/politics/hillary-clinton-speeches-wikileaks.html (Last accessed: 29.10.2021)

66. Lord, K., Sharp, T. America's Cyber Future Security and Prosperity in the Information Age. Volume I. Centre for American Security. P. 64. URL: https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238&focal=none (Last accessed: 16.11.2021)

67. Marks, J. The Cybersecurity 202: Trump took the nation in the wrong direction on cybersecurity, experts say. The Washington Post. 2020. URL: https://www.washingtonpost.com/politics/2020/12/15/cybersecurity-202-trump-took-nation-wrong-direction-cybersecurity-experts-say/ (Last accessed: `15.11.2021)

68. Menn, J., Bin, C. Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes. Reuters. 2021. URL:

https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07/ (Last accessed: 21.10.2021)

69. Morgan, S. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. 2020. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Last accessed: 21.10.2021)

70. New sophisticated email-based attack from NOBELIUM. Microsoft. 2021. URL: https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/ (Last accessed: 21.10.2021)

71. Oxford English Dictionary. URL: https://www.oxfordlearnersdictionaries.com/definition/english/cyber?q=cyber- (Last accessed: 15.11.2021)

72. Painter, C. The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. American Foreign Service Association. 2018. URL: https://afsa.org/diplomacy-cyberspace (Last accessed: 17.11.2021)

73. Remarks by The President on securing our Nation's Cyber Infrastructure. The White House. 2009. URL: http://www.whitehouse.gov/the_press_office/Remarks-bythe-President-on-Securing-Our-Nations-CyberInfrastructure/ (Last accessed: 9.09.2021)

74. Rivals on World Stage, Russia and U.S. Quietly Seek Areas of Accord. The New York Times. 2021. URL: https://lb.ua/go.php?url=aHR0cHM6Ly93d3cubnl0aW1lcy5jb20vMjAyMS8xMC8zMS93b3JsZC9ldXJvcGUvYmlkZW4tcHV0aW4tcnVzc2lhLXVuaXRlZC1zdGF0ZXMuaHRtbA (Last accessed: 5.11.2021)

75. Romm, T., Molla, R. Here's a longer list of news organizations that cited Russia-linked Twitter accounts. Vox. URL: https://www.vox.com/2017/11/4/16606188/twitter-russia-troll-news-citation-list (Last accessed: 29.10.2021)

76. Schuetze, J. EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals. EU Cyber Direct. 2020. URL: https://eucyberdirect.eu/content_research/eu-us-cybersecurity-policy-coming-together-recommendations-for-instruments-to-accomplish-joint-strategic-goals/ (Last accessed: 5.11.2021)

77. Schuetze, J. How to Operationalise a Transatlantic Cyber Policy Research Initiative (TCPRI). Stiftung Neue Verantwortung. 2019. P.18. URL: https://www.stiftung-nv.de/sites/default/files/schutze_rif-forpublication.pdf (Last accessed: 5.11.2021)

78. Shnikman, P. Russia Ramps Up Cyberattacks in Ukraine Amid Fears of War. U.S.News. 2021. https://www.usnews.com/news/world-report/articles/2021-04-20/us-helping-ukraine-foil-russian-cyberattacks-as-hacking-spikes-sources (Last accessed: 5.11.2021)

79. Shuster, S. Vladimir Putin's Bad Blood with Hillary Clinton. Time. 2016. URL: https://time.com/4422723/putin-russia-hillary-clinton/ (Last accessed: 29.10.2021)

80. SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president. Reuters. 2021. URL: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R (Last accessed: 22.10.2021)

81. Speier, J. Says President Donald Trump as a candidate mentioned WikiLeaks "over 160 times in speeches" in the last month of the campaign. PolitiFact. 2017. URL: https://www.politifact.com/factchecks/2017/apr/21/jackie-speier/did-trump-really-mention-wikileaks-over-160-times-/ (Last accessed: 29.10.2021)

82. The U.S.-Ukraine Strategic Defence Framework signed in Washington. Ministry of Defence of Ukraine. 2021. URL: https://www.mil.gov.ua/en/news/2021/08/31/the-u-s-ukraine-strategic-defence-framework-signed-in-washington/ (Last accessed: 5.11.2021)

83. Threats Posed by the Internet. The Threat Working Group of the CSIS Commission in Cybersecurity for the 44th Presidency. 2009. URL: https://csis-

website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081028_threats_working_group.pdf (Last accessed: 9.09.2021)

84. Toor A. Members of Trump's cybersecurity council resign in protest. The verge. 2017. URL: https://www.theverge.com/2017/8/28/16213464/trump-cybersecurity-council-resign-protest-niac (Last accessed: 12.09.2021)

85. TOP-25 News Sources. Count of linked sources in Tweets. URL: top 25 news links overview graph.png (2144×1424) (dwcontent.com) (Last accessed: 29.10.2021)

86. US media accused of burying concerns over Clinton health. RT YouTube. 2016. URL: https://www.youtube.com/watch?v=hjATqbDcvFY (Last accessed: 29.10.2021)

87. Watts, D., Rothschild, D. Don't blame the election on fake news. Blame it on the media. Columbia Journalism Review. 2017. URL: https://www.cjr.org/analysis/fake-news-media-election-trump.php (Last accessed: 30.10.2021)

88. Wilson, C. Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. The Library of Congress. 2003. P. 35. URL: https://irp.fas.org/crs/RL32114.pdf (Last accessed: 16.11.2021)

89. Бакиров Р. Р., Цветкова Н. А. Политика кибербезопасности США - эволюция, угрозы и оппоненты, 1990-2010-е гг. Международные отношения. 2019. №4. URL: https://cyberleninka.ru/article/n/politika-kiberbezopasnosti-ssha-evolyutsiya-ugrozy-i-opponenty-1990-2010-e-gg (дата обращения: 17.11.2021)

90. Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности. Президент России. 2020. URL: http://kremlin.ru/events/president/transcripts/64086#sel=6:11:9,6:11 (дата обращения: 3.11.2021)

91. Карасев П.А. Новые информационные технологии во внешней политике США. Мировая экономика и международные отношения, 2014, № 5, сс. 53-62. URL: https://doi.org/10.20542/0131-2227-2014-5-53-62 (Дата обращения: 22.09.2021)

92. Карасев П.А. Стратегия информационной (кибер)безопасности сша в XXI веке // Вестник Московского университета. Серия 12. Политические науки. 2013. №2. URL: https://cyberleninka.ru/article/n/strategiya-informatsionnoy-kiber-bezopasnosti-ssha-v-xxi-veke (дата обращения: 22.09.2021

93. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza(дата обращения: 17.11.2021).

94. Осипенко Анатолий Леонидович Организованная преступность в сети Интернет. Вестник ВИ МВД России. 2012. №3. URL: https://cyberleninka.ru/article/n/organizovannaya-prestupnost-v-seti-internet(дата обращения: 17.11.2021).

Веб-сайти

95. AEGIS. URL: https://aegis-project.org/ (Last accessed: 7.11.2021)

96. DISCOVERY. URL: https://discoveryproject.eu/discovery-input-papers-policy-briefs/ (Last accessed: 7.11.2021)

97. Paris Call. URL: https://pariscall.international/ (Last accessed: 5.11.2021)

98. U.S. Cyber Command. URL: https://www.cybercom.mil/About/History/ (Last accessed: 09.09.2021)

Книги

99. Лисиченко Г. В., Забулов Ю. Л., Хміль Г. А. Природний, техногенний та екологічний ризики: аналіз, оцінка, управління. Київ : Наук. думка, 2008. 544 с.

100. Манжай О. В. Використання кіберпростору в оперативнорозшуковій діяльності. Право і безпека. 2009. № 4. С. 142–149.

101. Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки. Зб. наук. праць Військового ін-ту КНУ ім. Тараса Шевченка. 2011. № 30. С. 159–165.

102. Померанцев П. Це не пропаганда. Подорож на війну проти реальності. / пер. з англ О. Форостина. Київ : Yakaboo Publishing, 2020. 288 с.

103. Jamieson K. Cyberwar: How Russian Hackers and Trolls Helped Elect a President. Oxford University Press, 2018. 337 p.

104. Janczewski L., Colarik M. Cyber Warfare and Cyber Terrorism. Information Science Reference, 2008. 532 p.

105. Kramer F., Starr S., Wentz L. Cyberpower and National Security. Washington, D.C.: Potomac Books. 2009. 642 p.

SUMMARY

Entering the 21st century, the world faces new opportunities on the one hand when challenges and threats on the other. The first category includes online education, Internet banking, and unrestricted communication for citizens, automated management systems for corporations, digital diplomacy, and e-government for governments. The second one comprises the theft of money and confidential data, denial of service, and cyber espionage. Subsequently, the notion of cyberspace has become a strategic object of the state and the fifth front for hybrid confrontations. Therefore, it is obvious that the ecosystem of cyberspace affects the domestic and foreign policies of the state, as well as affects its level in the international arena. Accordingly, the need for sectoral policy has been justified.

The terrorist attacks of September 11, 2001, demonstrated the vulnerability of even superpowers to cross-border threats and pointed to the need to formulate protection policies. Therefore, realizing that the next incident could happen with the use of information and communication technologies, that is, in cyberspace, the United States has begun to develop a cybersecurity policy.

The 43rd President, George W. Bush, has begun the process of shaping the cyber policy of the United States. In 2003, the first and fundamental US Cyber Security Strategy was adopted. Significantly, Bush recognized cyberspace as an arena of confrontation and began developing security policies not only in the government sector but also in critical private infrastructure. Each subsequent legislative initiative will ask for the provisions and norms declared by the White House under George W. Bush.

Progress in the industry has taken place in each of the four administrations surveyed. However, the largest contribution in two terms was made by the 44th President of the United States.

First, with the Presidential Political Directive, better known as the PPD-20, Barack Obama began creating a mechanism for offensive operations in cyberspace.

Second, the Barack Obama administration has paid close attention to international cooperation, so the White House has reaffirmed its leadership

ambitions in the international arena, particularly in crisis management. Finally, under Barack Obama, the United States developed a typology of threat sources and singled out Russia and China as major threats to US national interests.

Another exacerbation of the vulnerability of cyberspace as a component of information, including cyber, security for the United States took place during the 2016 election campaign. Russia's goal was to denigrate Hillary Clinton's image and, consequently, to promote Donald Trump's campaign. It`s significant that Moscow, adhering to the Soviet-style of bilateral relations with Washington, continues to interfere in the course of the American elections, conducting disinformation campaigns. However, the usual intelligence has been replaced by cyber espionage carried out by hackers serving in the GRU. Thus, cyberspace was used as an arena of global confrontation. So, both the Americans and the international community were interested in what Donald Trump's cyber policy should be because Russia contributed to his victory through the use of cyberattacks.

Analyzing the industry activities of Donald Trump, it is worth highlighting the moments of controversial progress and regress. The first is to continue Barack Obama's policy of offensive operations. Donald Trump equated Cyber Command with a combat unit and abolished the PPD-20, which provided for the coordination of potential high-level operations. In addition, the distribution of budget funds under the Donald Trump administration gave priority to offensive operations over the protection of information and communication infrastructure. The second is the regression caused by the subjective dismissals of cyber experts, such as Chris Krebs, head of the US Cybersecurity and Infrastructure Security Agency, for declaring the Republican president's allegations of election fraud unfounded. Significantly, Donald Trump's presidency has been seen a stagnation in international cooperation, particularly in the partnership with the European Union.

The policies of the current president, Joseph Biden, contrast with the vision of his predecessor. The first step of the incumbent president was to form a team of specialists. However, the weak point of such a cyber team is the lack of private

field specialists – the recruits held relevant positions in the Barack Obama administration, so they belong to the government sector. Given the place of the United States in the modern system of international relations and the information and communication potential of the state, the White House since the beginning of the century demonstrates leadership ambitions in shaping global cybersecurity policy. As a result, Washington has made significant contributions to international cooperation on cyberspace protection and Internet security, including the development of international sectoral instruments such as the 2001 Council of Europe Convention on Cybercrime and the 2002 Guiding Principles on Security of Information Systems and Networks.

However, it is clear that bilateral relations between the United States and the Russian Federation, two states with strong cyber potential, play a significant role in the ecosystem of global cybersecurity and diplomacy. In recent years, the interaction of two actors in cyberspace has resembled confrontation rather than cooperation. However, at the beginning of his term, Joseph Biden intensified his dialogue with Vladimir Putin on non-interference in information and communication networks of critical infrastructure. Thus, the issue of cyber politics has now become a priority in American-Russian discourse.

Analyzing the bilateral American-Ukrainian cooperation, it is worth emphasizing the interest of both states in it, as both Ukraine and the United States have experience in counteracting the common cyber enemy - the Kremlin. Thus, the White House under the leadership of Joseph Biden is moving in the direction set by Donald Trump and continues to conduct cyber dialogues with further funding from the Ukrainian side. The effectiveness of the partnership has already been confirmed by the ability of Ukrainian special services to resist attacks. Progress for official Kyiv will be the adoption of a law on cooperation with Ukraine in the cyber sector. Firstly, the legal act will consolidate the parties' leadership roles in strengthening the cyberspace of Europe. Secondly, the document will be the first US law with the Ukraine mentioned in its name.

An analysis of transatlantic cooperation shows some stagnation during Donald Trump's presidency due to differences in cyber policy: while the European Union sought to protect its cyberspace, the United States relied on offensive operations. However, both players have a common foundation and common threats, so the coming to power of Joseph Biden restores the prospect of coordination between the EU and the United States.

Thus, cyberspace is an environment of opportunities for the realization of state interests, as well as an environment of threats to national and international security. For 20 years, the White House has managed to identify sources of threat, highlight priorities, develop defense and counter-offensive mechanisms, and participate in strengthening global security through bilateral and multilateral cooperation, as well as within international organizations. However, with the development of information and communication technologies, the tools of criminals are being modernized, so the United States is forced to continue to strengthen networks and quickly detect, respond to threats and eliminate consequences.