Функціонування і розвиток механізмів державного управління

УДК 338.2:351.863

Хряпинський Антон Петрович
кандидат юридичних наук, директор
ТОВ «ХРЯПИНСЬКИЙ І КО»
Khriapynskyi Anton
Candidate of Law Sciences, Director
LTD «Khriapynskyi and partners»
ORCID: 0000-0002-2492-051X

ГІБРИДНИЙ ВПЛИВ І СУЧАСНЕ ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ
HYBRID INFLUENCE AND MODERN INFORMATION ENVIRONMENT

Анотація. *Вступ. Інформаційне середовище та величезний потенціал для його використання у зловмисних діях вже певний час тому привернули значну увагу фахівців у сфері гібридних загроз та гібридної війни. З початку тисячоліття використання операцій впливу як державними, так і недержавними акторами стає все більш очевидним як для тих, хто приймає рішення, так і для пересічного населення. Цифрова революція, що впливає на розповсюдження інформації та соціальний обмін у наших суспільствах і спільнотах, а також посилення зв'язаності ключових суспільних систем та інфраструктури відкрила не лише нові можливості, а також і вразливі місця. Крім того, зміни на ринках праці та у демографічному складі багатьох суспільств розширили можливості та горизонти для частини суспільства, але залишили інших невпевненими у своєму місці чи представленості їхніх інтересів у традиційних ЗМІ чи політичній сфері. Це мало прямий вплив як на національну публічну політику, так і на міжнародні відносини, не в останню чергу пов'язане з*

різними референдумами та виборами.

Мета. Метою даної роботи є повне, всебічне та доктринальне дослідження загальнотеоретичних засад гібридного впливу у контексті визначення та характеристики інформаційного середовища.

Матеріали і методи. В процесі здійснення дослідження було використано наступні наукові методи: емпіричний (для збору та систематизації даних), спостереження (для узагальнення інформації), аналізу та синтезу (для оцінки ситуацій та прикладів до них, а також вжиття необхідних заходів).

Результати. Акцентовано увагу на тому, що комунікаційні стратегії необхідно адаптувати до інформаційного середовища, де кількість каналів для охоплення населення є значно різноманітнішою, ніж лише десять років тому. Це вимагає більших знань щодо ключових цільових аудиторій, розуміння того, які їхні мотивації, занепокоєння та досвід, які канали вони використовують і як мають бути оформлені повідомлення, щоб вони були зрозумілими та ефективними. Іншим ключовим аспектом є впровадження відповідних наборів навичок у служби безпеки та розвідки, оскільки здатність підтримувати ситуаційну обізнаність є ключовою передумовою для кількох інших сфер реагування та стійкості. Оскільки операції впливу можуть бути спрямовані на багато різних ситуацій або акторів у публічному та приватному секторах, також важливо закрити потенційну відповідальність або прогалини у сприйнятті, якими може скористатися опонент. Одним із способів їх зменшення може бути створення організації, яка забезпечує обмін інформацією, навчання та співпрацю для ключових суспільних акторів, а також забезпечує комплексне відстеження загроз, пов'язаних з гібридним впливом, і реалізує механізм раннього попередження. Дану організацію необхідно адаптувати до існуючого законодавства та нинішнього інформаційного середовища, де дані переміщуються вільно, але при цьому стали дуже цінним товаром, який намагаються отримати

багато недоброчесних акторів, починаючи від окремих осіб, закінчуючи державами.

Зосереджено увагу на тому, що операції впливу використовують широкий спектр методологій, технологій та інструментів, але всі вони виграють від великої кількості легкодоступних даних, що дає змогу на відстані дізнатися, як працює чуже інформаційне середовище. Здатність оцінювати та переналаштовувати операції також значно зросла останнім часом. Завдяки швидкості, охопленню та можливостям анонімності в сучасних каналах зв'язку також легше залучати або вилучати акторів у цьому середовищі, не розкриваючи свою особу та справжні мотиви. Науковці та практики в демократичних суспільствах часто розділяють кібероперації та операції впливу.

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на виробленні конкретних методик та показників для протидії внутрішнім загрозам та критеріїв побудови системи їх попередження в контексті інформаційного середовища.

Ключові слова: *управління, гібридні загрози, протидія та превенція, інноваційний розвиток, протидія загрозам, превенція загрозам, гібридні загрози в управлінні.*

Summary. *Introduction. The information environment and the huge potential for its use in malicious actions have already attracted considerable attention from experts in the field of hybrid threats and hybrid warfare. Since the turn of the millennium, the use of influence operations by both state and non-state actors has become increasingly apparent to both decision makers and the public. The digital revolution, affecting the dissemination of information and social exchange in our societies and communities, as well as the increased connectivity of key societal systems and infrastructure, has opened not only new opportunities, but also vulnerabilities. In addition, changes in the labor markets and*

demographics of many societies have expanded opportunities and horizons for some, but left others unsure of their place or the representation of their interests in traditional media or the political sphere. This has had a direct impact on both national public policy and international relations, not least related to various referenda and elections.

Purpose. The purpose of this work is a complete, comprehensive and doctrinal study of the general theoretical foundations of hybrid influence in the context of defining and characterizing the information environment.

Materials and methods. The following scientific methods were used during the research: empirical (to collect and systematize data), observation (to generalize information), analysis and synthesis (to evaluate situations and examples of them, as well as take necessary measures).

Results. Attention is focused on the fact that communication strategies must be adapted to the information environment, where the number of channels for reaching the population is much more diverse than just ten years ago. This requires greater knowledge of key target audiences, understanding what their motivations, concerns and experiences are, what channels they use and how messages should be framed to be understandable and effective. Another key aspect is instilling appropriate skill sets in security and intelligence services, as the ability to maintain situational awareness is a key prerequisite for several other areas of response and resilience. Because influence operations can target many different situations or actors in the public and private sectors, it is also important to close potential liability or perception gaps that an adversary can exploit. One of the ways to reduce them can be to create an organization that provides information exchange, training and cooperation for key societal actors, and also provides comprehensive tracking of threats related to hybrid impacts and implements an early warning mechanism. This organization needs to be adapted to existing legislation and the current information environment, where data moves freely, but at the same time has become a very valuable commodity that many

unscrupulous actors, ranging from individuals to states, are trying to obtain.

The focus is on the fact that influence operations use a wide range of methodologies, technologies and tools, but all of them benefit from a large amount of readily available data, which allows us to learn from a distance how someone else's information environment works. The ability to evaluate and reconfigure operations has also grown significantly in recent times. The speed, reach, and anonymity afforded by today's communication channels also make it easier to recruit or remove actors in this environment without revealing their identity and true motives. Scholars and practitioners in democratic societies often distinguish between cyber operations and influence operations.

Discussion. In further scientific research, it is proposed to focus attention on the development of specific methods and indicators for countering internal threats and criteria for building a system for their prevention in the context of the information environment.

Key words: *management, hybrid threats, counteraction and prevention, innovative development, countermeasures against threats, prevention of threats, hybrid threats in management.*

Постановка проблеми. Інформаційне середовище та величезний потенціал для його використання у зловмисних діях вже певний час тому привернули значну увагу фахівців у сфері гібридних загроз та гібридної війни. З початку тисячоліття використання операцій впливу як державними, так і недержавними акторами стає все більш очевидним як для тих, хто приймає рішення, так і для пересічного населення. Цифрова революція, що впливає на розповсюдження інформації та соціальний обмін у наших суспільствах і спільнотах, а також посилення зв'язаності ключових суспільних систем та інфраструктури відкрила не лише нові можливості, а також і вразливі місця. Крім того, зміни на ринках праці та у демографічному складі багатьох суспільств розширили можливості та

горизонти для частини суспільства, але залишили інших невпевненими у своєму місці чи представленості їхніх інтересів у традиційних ЗМІ чи політичній сфері. Це мало прямий вплив як на національну публічну політику, так і на міжнародні відносини, не в останню чергу пов'язане з різними референдумами та виборами.

Аналіз останніх досліджень і публікацій. Проблематика аналізу та розгляду гібридних загроз та гібридного впливу, в тому числі в інформаційному середовищі, завжди привертала увагу вітчизняних та закордонних науковців, що знайшло своє відображення у працях таких вчених як Л. Акімова – щодо протидії загрозам у економічній сфері та державно-управлінських засадах в цілому [1], Е. Бухвальд – щодо окремих питань макропоказників впливу загроз у державно-управлінських засадах [2], З. Гбур – щодо концептуальних аспектів протидії загрозам [3], В. Ліпкан – щодо сутністних особливостей гібридної війни на прикладі вітчизняного досвіду [4], Є. Магда – щодо загальних характеристик сутності гібридної війни як сутнісного явища [5], В. Мартинюк – щодо загальних характеристик сутності гібридної війни крізь суспільно-економічні показники [6], В. Горбулін – щодо інформаційних характеристик безпеки суспільства як об'єкт впливу гібридних загроз [7], О. Курбан – щодо концепції сучасної системи забезпечення безпеки країни [8], але чимало досліджень все ще перебувають на етапі становлення та осмислення, що свідчить про незавершеність формування наукової думки та усталених постулатів, а відтак, набуває особливої актуальності.

Виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Швидкий розвиток науки та переосмислення існуючих постулатів, а також зміна нормативно-правових засад невпинно змінюють усталені погляди та концепції на явища та процеси, наповнюють їх новим змістом та осмисленням. За даних умов випливає, що поглиблення досліджень у сфері гібридних загроз та

гібридного впливу, в тому числі в інформаційному середовищі має надзвичайно актуальне значення та передбачає ряд систем стримувань та противаг.

Формулювання цілей статті (постановка завдання). Метою даної роботи є повне, всебічне та доктринальне дослідження загальнотеоретичних засад гібридного впливу у контексті визначення та характеристики інформаційного середовища.

Матеріали і методи. В процесі здійснення дослідження було використано наступні наукові методи: емпіричний (для збору та систематизації даних), спостереження (для узагальнення інформації), аналізу та синтезу (для оцінки ситуацій та прикладів до них, а також вжиття необхідних заходів).

Виклад основного матеріалу дослідження. Розглядаючи особливості гібридного впливу на інформаційне середовище, окремі автори використовують поняття «активності щодо інформаційного впливу» для визначення «націлювання на формування громадської думки нелегітимними, хоча й не обов'язково незаконними способами, іноземними суб'єктами або їхніми довіреними особами». Крім того, вони виділяють три терміни, запропоновані шведським урядом, що формують ієрархію активності з впливу: вплив (одноразове використання нелегітимних методів); операції впливу (множинні скоординовані дії); і кампанії впливу (кілька скоординованих операцій у всьому гібридному спектрі) [9, с. 5].

Збільшення уваги до зазначеної проблеми останнім часом може на перший погляд скласти враження, що техніки впливу є дещо новими. Насправді такі дії використовувалися в ситуаціях миру, конфліктів і війн протягом всієї історії. Різниця сьогодні великою мірою залежить від швидкості, з якою може відбуватися розповсюдження повідомлень та інформації, а також від можливості приховати або завуалювати джерело чи відправника повідомлення. Використання автоматизованих облікових

записів і алгоритмів також може допомогти як у зборі даних, пропонуючи більш точний аналіз цільової аудиторії, так і покращити розповсюдження таким чином, щоб здавалось, що інформація поширилась серед більшої групи людей в Інтернеті, ніж це є насправді. Крім того, зловмисники мають ініціативу, а також перевагу в тому, що вони здатні швидко отримувати зворотний зв'язок щодо того, чи отримана інформація.

Таким чином, їхні зусилля можуть бути перенаправлені або відкликані протягом короткого проміжку часу, залежно від того, чи відповідає сприйманий ефект їхнім амбіціям. Доступність цільових аудиторій у сучасному інформаційному середовищі також зменшила витрати на проведення операцій впливу та збільшила потенційні результати, яких можна досягти. Нарешті, такі методи також можна використовувати в поєднанні з іншими можливостями гібридних загроз.

Щоб проілюструвати низку гібридних методів, які використовуються в поточному інформаційному середовищі, у якості головного прикладу агресора будемо розглядати Росію, головним чином тому, що є кілька гучних дій, які ілюструють використання Росією операцій впливу в останні роки. Це жодним чином не означає, що Росія є єдиним актором, який зараз спрямовує значні ресурси на цю мету. Комуністична партія Китаю активно використовувала відповідні стратегії, як зазначено у звіті CSIS за 2018 рік: «Агресивна стратегія спрямована на вплив на прийняття політичних рішень, отримання несправедливих переваг у торгівлі та бізнесі, придушення критики Китаю, сприяння можливостям шпигунства та на посилення впливу закордонних китайських громад» [10, с. 130]. Інші країни, такі як Іран, також проявили себе як такі, що використовують, наприклад, «скоординовану неавтентичну поведінку» через сторінки в соціальних мережах, групи та облікові записи, націлені на політику та вибори в США та Великобританії. Крім того, ряд неурядових організацій доклали значних зусиль для впливу на різні цільові аудиторії, особливо через використання соціальних медіа та

інших веб-каналів комунікації.

Одним із ключових прекурсорів, що дозволяють здійснювати операції впливу, є таргетинг. Як зазначалося раніше, інформаційні технології та велика кількість даних, доступних на платформах соціальних медіа, пропонують нові можливості для визначення цільової аудиторії та найефективнішого способу її охоплення. Справа Cambridge Analytica є одним із яскравих прикладів цього за останній час. 17 березня 2018 року The New York Times разом із The Guardian і The Observer повідомили, що Cambridge Analytica та пов'язана з нею компанія Strategic Communication Laboratories зібрали дані щонайменше 50 мільйонів користувачів Facebook і зберігали їх без згоди платформи [11, с. 244]. Facebook призупинив роботу як Cambridge Analytica, так і Strategic Communication Laboratories, і заявив, що знав про порушення, але отримав юридичні гарантії від компанії, що всі дані були видалені. Ці дані були використані Cambridge Analytica та Strategic Communication Laboratories для проведення політичного таргетування. Точніше, для створення програмного забезпечення для аналізу особистих уподобань виборців для своїх клієнтів, серед яких була команда передвиборчої кампанії Дональда Трампа та, за словами інформатора, переможна команда кампанії Brexit. У липні 2018 року британський член парламенту Деміан Коллінз, який очолював парламентське розслідування щодо фейкових новин, повідомив CNN, що Управління комісара з інформації (ICO) знайшло докази того, що доступ до файлів Cambridge Analytica здійснювався з Росії [12, с. 506].

В той же час, несанкціонований доступ до комп'ютерних систем може сам по собі потенційно вплинути на перспективи певної цільової аудиторії та підірвати довіру до ключових функцій у суспільстві. Він також може служити для отримання даних і розуміння, які сприятимуть таргетингу, розкладу та дизайну операцій впливу. У травні 2016 року, напередодні виборів у США того ж року, систему реєстрації виборців в Арізоні було

виведено з ладу після того, як ФБР попередило про кіберзагрозу. Розслідування показало, що хакери намагалися проникнути в систему, але невдало. Однак штату Іллінойс пощастило менше, і через місяць хакери отримали доступ до 90 000 записів, включаючи імена, дати народження, стать, водійські права та часткові номери соціального страхування зареєстрованих виборців. Після цього вони також намагалися, хоча і безуспішно, маніпулювати частиною отриманої інформації [13, с. 44]. Під час слухань у Сенаті США в червні 2017 року кібердиректор Департаменту внутрішньої безпеки Сем Лайлз заявив, що Росія атакувала системи, пов'язані з виборами, у 21 штаті, включаючи Арізону та Іллінойс. Мета операції була не зовсім зрозумілою, але «кіберзлом інфраструктури, пов'язаної з виборами, такої як системи голосування та бази даних виборців, надав росіянам техніку, матеріали та знайомство з виборчою системою США, які можна застосувати до майбутніх російських кампаній впливу – у США і, можливо, деінде» [14, с. 207]. Однак не лише державні виборчі системи стали мішенню, російських хакерів цікавлять і ЗМІ. У 2015 році група, яка називає себе Кіберхаліфатом, заявила про відповідальність за встановлення шкідливого програмного забезпечення з метою знищення апаратного забезпечення системи передачі для французького каналу TV5 Monde. Дванадцять каналів були вимкнені протягом дев'яти годин, але атака потенційно могла завдати набагато більшої шкоди. Завдяки черговим технікам комп'ютер, який працював як ворота в мережу каналу, був виявлений і відключений від Інтернету [15, с. 53].

Останніми роками хакерські групи, такі як APT 28, розширили свої дії за межі збору розвідданих і шпигунства до операцій з проникненням, які охоплюють ширший спектр цілей, таких як уможливлення майбутніх дій впливу або порушення фізичної інфраструктури. Подібні хакерські атаки яскраво ілюструють дві операції, проведені проти української електромережі у 2015 та 2016 роках. Перша залишила близько 250 000

жителів без світла на кілька годин. Друга призвела до годинного відключення електроенергії в Києві. Кілька розслідувань встановили, що за цими атаками стоїть хакерська група під назвою Sandworm, також відома як Voodoo Bear і Telebots. Організація з кібербезпеки FireEye також виявила зв'язки між Sandworm і Росією на основі російськомовних документів, знайдених на серверах командування та контролю, які використовувала група – зокрема, невирішеної вразливості, яка була представлена на російській хакерській конференції, з явним фокусом на Україні. Як згадувалося раніше, збір великої кількості даних користувачів із ключових платформ може бути дуже корисним для цілей розвідки, а також для планування кампаній впливу. Проте подібна інформація може бути привабливою як для державних суб'єктів, так і для компаній, які шукають короткий шлях для підвищення конкурентоспроможності. Так, у вересні 2018 року Facebook зазнав витоку даних, коли невідомі зловмисники змогли використати основний збій безпеки та завантажити особисті дані приблизно 50 мільйонів користувачів. Викрадені дані включали ім'я користувача, електронну адресу, номер телефону, дату народження та публікації на платформі [16, с. 55]. Коли інформація про злом стала публічною, Facebook на початку жовтня визнав другий великий витік даних. Цього разу російська компанія SocialDataHub і її дочірня компанія Fubutech завантажили таку велику кількість даних з платформи, що в її маркетингових матеріалах стверджувалося, що вона фактично є дзеркалом російської частини Facebook. За оцінкою Facebook, цей витік був частково спричинений потребою російської компанії масово отримувати зображення з Facebook, щоб створити моделі розпізнавання облич, які могли б використовуватися російською владою для цілей стеження [17, с. 80].

Інформація, отримана шляхом злому, іноді доповнена відкритими джерелами, не завжди використовується лише для розвідувальних цілей. Її також можна використовувати для посилення ефекту операцій впливу, за

допомогою яких вибрані частини інформації поширюються переважно через веб-платформи. Ця технологія називається доксінг – практика розкриття та оприлюднення інформації про організацію чи особу, яка є приватною або секретною, щоб публічно присоромити або збентежити ціль. Найвідоміший доксінг, проведений Росією, стався під час підготовки до виборів у США в 2016 році. У березні керівник кампанії Гілларі Клінтон Джон Подеста отримав електронний лист від, здавалося, Google, у якому його просили негайно змінити свій пароль. Повідомлення було розглянуто IT-відділом, але, згідно з пізнішими заявами, було помилково оцінено як «легітимне». Справжнє джерело повідомлення, згідно з розслідуваннями кількох організацій з кібербезпеки, а також розвідувальної служби США, була російська хакерська група APT 28. Коли співробітники Джона Подести змінили пароль електронної пошти, вони надали хакерам доступ до понад 50 000 його електронних листів [17, с. 55]. Через два місяці, наступного дня після того, як Національний комітет Демократичної партії виявив, що їх зламали, анонімний користувач Інтернету а через тиждень і WikiLeaks почали оприлюднювати викрадені дані. Цей процес тривав до виборів 8 листопада.

Кілька разів безперервний доксінг був приурочений до максимального потенційного висвітлення в ЗМІ. Один із прикладів стався після того, як адміністрація Обами оприлюднила заяву 7 жовтня, назвавши російське керівництво відповідальним за кампанію впливу проти виборів у США. Через тридцять хвилин *The Washington Post* оприлюднила записи телешоу «Access Hollywood», де Дональд Трамп робить принизливі заяви про жінок 28. Ще через тридцять хвилин WikiLeaks почав оприлюднювати розмови електронною поштою за участю Подести, вказуючи на зв'язки кандидатки в президенти Клінтон із великими банками (це було питання, яке вже піднімалося проти Клінтон під час попередніх дебатів). Тревертон зазначив, що це «демонструє явну перевагу Кремля щодо кандидата Трампа

та його допомогу у збільшенні шансів Трампа на виборах». У жовтні 2018 року Національний центр кібербезпеки Великобританії опублікував додаткові роз'яснення щодо APT, описавши в «оцінці високої достовірності» ідентифікацію кількох кібератак на політичні інституції, компанії, а також ЗМІ та спортивні організації, організовані російською розвідувальною службою ГРУ. Національний центр кібербезпеки Великобританії також встановив, що серед інших груп APT 28 і його численні псевдоніми, такі як Fancy Bear, Pawnstorm і Cyber Caliphate, пов'язані з ГРУ [17, с. 41].

Операції впливу використовують широкий спектр методологій, технологій та інструментів, але всі вони виграють від великої кількості легкодоступних даних, що дає змогу на відстані дізнатися, як працює чуже інформаційне середовище. Здатність оцінювати та переналаштовувати операції також значно зросла останнім часом. Завдяки швидкості, охопленню та можливостям анонімності в сучасних каналах зв'язку також легше залучати або вилучати акторів у цьому середовищі, не розкриваючи свою особу та справжні мотиви. Науковці та практики в демократичних суспільствах часто розділяють кібероперації та операції впливу. Поширення повідомлень, які підживлюють поляризацію та спотворюють суспільні дебати в іншій країні, також є важливою метою. Якщо в країні виникають внутрішні суперечки, а політики чи громадськість намагаються знайти спільну мову, у них буде менше енергії та зосередженості на стримуванні та протидії стратегіям і діям наступального актора.

У світлі цих викликів виникає закономірне запитання: яким чином ключові актори демократичного суспільства можуть обмежити наслідки операцій шкідливого впливу? Поінформованість громадськості є першою лінією захисту, тому проактивна стратегічна комунікація та прозорість з боку керівництва держави та інших ключових комунікаторів є життєво важливими. Це може зберегти зосередженість на проблемі та мінімізувати

вплив дезінформації, одночасно зберігаючи довіру та забезпечуючи довгострокову комунікацію між особами, які приймають рішення, та населенням.

Висновки з цього дослідження і перспективи подальших розвідок у даному напрямку, таким чином, комунікаційні стратегії необхідно адаптувати до інформаційного середовища, де кількість каналів для охоплення населення є значно різноманітнішою, ніж лише десять років тому. Це вимагає більших знань щодо ключових цільових аудиторій, розуміння того, які їхні мотивації, занепокоєння та досвід, які канали вони використовують і як мають бути оформлені повідомлення, щоб вони були зрозумілими та ефективними. Іншим ключовим аспектом є впровадження відповідних наборів навичок у служби безпеки та розвідки, оскільки здатність підтримувати ситуаційну обізнаність є ключовою передумовою для кількох інших сфер реагування та стійкості. Оскільки операції впливу можуть бути спрямовані на багато різних ситуацій або акторів у публічному та приватному секторах, також важливо закрити потенційну відповідальність або прогалини у сприйнятті, якими може скористатися опонент. Одним із способів їх зменшення може бути створення організації, яка забезпечує обмін інформацією, навчання та співпрацю для ключових суспільних акторів, а також забезпечує комплексне відстеження загроз, пов'язаних з гібридним впливом, і реалізує механізм раннього попередження. Дану організацію необхідно адаптувати до існуючого законодавства та нинішнього інформаційного середовища, де дані переміщуються вільно, але при цьому стали дуже цінним товаром, який намагаються отримати багато недоброчесних акторів, починаючи від окремих осіб, закінчуючи державами.

Література

1. Акімова Л. М. Сутнісна характеристика основних загроз в економічній

безпеці держави. *Державне управління: удосконалення та розвиток*. 2016. № 10. С. 16-28.

2. Бухвальд Є. Макроаспекти економічної безпеки: фактори, критерії та показники. *Питання економіки*. 1994. №12. С. 25-44.
3. Гбур З. В. Актуальні гібридні загрози економічній безпеці України. *Інвестиції: практика та досвід*. 2018. № 7. С. 97-99.
4. Ліпкан В. А. Сутність гібридної війни проти України. *GOAL*. 2015. URL: https://goal-int.org/sutnist-gibridnoi-vijni-proti-ukraini/ (дата звернення: 05.08.2023).
5. Магда Є. Гібридна війна: питання і відповіді. *Інтернет-видання «MEDIASAPIENS»*. 2015. URL: http://ms.detector.media/trends/1411978127/gibridna_viyna_pitannya_i_vidpovidi/ (дата звернення: 05.08.2023).
6. Мартинюк В. Гібридні загрози Україні і суспільна безпека. досвід ЄС і східного партнерства. *Центр глобалістики «Стратегія XXI»*. 2018. С. 106-112.
7. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ : Інтертехнологія, 2012. 360 с.
8. Курбан О. В. Основи сучасної національної інформаційної безпеки країни. *Вісн. ХДАК*. 2017. Вип. 50. С. 55-62.
9. Wanless A., Pamment J. How Do You Define a Problem Like Influence? Journal of Information Warfare. 2019. 18.3. P. 1-14. URL: https://carnegieendowment.org/files/2020-How_do_you_define_a_problem_like_influence.pdf (дата звернення: 06.08.2023).
10. Pascal B. Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. NATO CCD COE. 2016.
11. Canadian Security Intelligence Service, China and the Age of Strategic

Rivalry: Highlights from an Academic Outreach Workshop. URL: https://publications.gc.ca/site/eng/9.867080/publication.html (дата звернення: 06.08.2023).

12. Kanishk K. Facebook Removes Iran-based Assets Again. 2019. URL: https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-f17358ef21f (дата звернення: 06.08.2023).
13. Cohen K., Kaati L. Digital Jihad – Propaganda from the Islamic State. Swedish Defence Research Agency. 2018.
14. Cadwalladr C. Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian*. 2018. P. 32-38.
15. O'Sullivan D. Cambridge Analytica's Facebook Data was Accessed from Russia, MP Says. *CNN*. 2016. № 13. P. 140-142.
16. Cadwalladr C., Graham-Harrison E. Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University. *The Guardian*. 2017. № 17. P. 25-29.
17. Lewis P., Wong J. Facebook Employs Psychologist Whose Firm Sold Data to Cambridge Analytica. *The Guardian*. 2018. № 18. P. 11-14.

References

1. Akimova, L. M. (2016). Sutnisna kharakterystyka osnovnykh zaghroz v ekonomichnij bezpeci derzhavy [Essential characteristics of the main threats to the economic security of the state] // *Public administration: improvement and development*, № 10, pp. 342-344 [in Ukrainian].
2. Buchvald, E. (1994). Makroaspekty ekonomichnoji bezpeky: faktory, kryteriji ta pokaznyky [Macroeconomic aspects of economic security: factors, criteria, and indicators] // *Putanya ekonomyky*, № 12, pp. 25-44 [in Ukrainian].
3. Hbur, Z. (2018). Aktualjni ghibrydni zaghrozy ekonomichnij bezpeci Ukrajiny [Actual hybrid threats to Ukraine's economic security] // *Investytsii: praktyka ta dosvid*, № 7, pp. 97-99 [in Ukrainian].

4. Lipkan, V. A. (2015). Sutnistj ghibrydnoji vijny proty Ukrajiny [The essence of the hybrid war against Ukraine]. URL: http://goal-int.org/ sutnist-gibridnoi-vijni-proti-ukraini/ [in Ukrainian].
5. Magda E. (2015). Ghibrydna vijna: pytannja i vidpovidi [Hybrid war: questions and answers]. URL: http://ms.detector. media/trends/1411978127/gibridna_viyna _pitannya_i_vidpovidi/ [in Ukrainian].
6. Martyniuk,V. (2018). Ghibrydni zaghrozy Ukrajini i suspiljna bezpeka. dosvid ES i skhidnogho partnerstva [Hybrid threats to Ukraine and public safety. Experience of the EU and the Eastern Partnership] // *Tsentr hlobalistyky "Stratehiia KhKhI",* pp.106 [in Ukrainian].
7. Gorbulin V. P. (2012). Informacijni operaciji ta bezpeka suspiljstva: zaghrozy, protydija, modeljuvannja [Information operations and social security: threats, countermeasures, modeling]. Kyiv, 360 p. [in Ukrainian].
8. Kurban O. V. (2017). Osnovy suchasnoji nacionaljnoji informacijnoji bezpeky krajiny [Fundamentals of modern national information security of the country] //*Visn. KhDAK* 2017. № 50. pp. 55-62 [in Ukrainian].
9. Pamment, James. How Do You Define a Problem Like Influence?' URL: https://carnegieendowment.org/files/2020-How_do_you_define_a_problem_like_influence.pdf [in English].
10. Brangetto, Pascal (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. NATO CCD COE. [in English].
11. Canadian Security Intelligence Service, China and the Age of Strategic Rivalry: Highlights from an Academic Outreach Workshop. URL: https://publications.gc.ca/site/eng/9.867080/publication.html. [in English].
12. Kanishk Karan. Facebook Removes Iran-based Assets Again. URL: https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-f17358ef21f. [in English].

13. Cohen, Katie & Kaati, Lisa (2018). Digital Jihad – Propaganda from the Islamic State. Swedish Defence Research Agency [in English].
14. Cadwalladr, Carole (2018). Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian*. pp. 32-38 [in English].
15. Donie, O'Sullivan (2016). Cambridge Analytica's Facebook Data was Accessed from Russia, MP Says. *CNN*. № 13, pp. 140-142 [in English].
16. Cadwalladr, Carole & Graham-Harrison, Emma (2017). Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University. *The Guardian*, № 17, pp. 25-29 [in English].
17. Lewis, Paul & Wong, Julia (2018). Facebook Employs Psychologist Whose Firm Sold Data to Cambridge Analytica, *The Guardian*, № 18, pp. 11-14 [in English].