УДК 343.2

КІБЕРЗАГРОЗИ ДЛЯ УКРАЇНИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

CYBER THREATS FOR UKRAINE IN THE INFORMATION SPACE

Тронько О.В.,
кандидат юридичних наук,
провідний науковий співробітник відділу
з вивчення проблем протидії організованій
злочинності у сфері державної безпеки
Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою
злочинністю при Раді національної безпеки і оборони України

Довгаль Ю.С.,
молодший науковий співробітник відділу
з вивчення проблем забезпечення інформаційної
та кібернетичної безпеки, захисту
вітчизняного інформаційного простору
Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою
злочинністю при Раді національної безпеки і оборони України

У статті розкриваються проблеми кібербезпеки України. Звертається увага на наукове осмислення термінів «кіберпростір», «кібербезпека». Вказано, що дотепер немає чітко визначеного змісту зазначених термінів, що ускладнює наукове осмислення та подальше практичне подолання тих проблем і викликів, які постають у кіберпросторі. Актуалізується питання кібермогутності держави. Описано основні загрози кібербезпеці України і контексті російської інформаційної війни та кіберагресії.
Ключові слова: кібертероризм, кіберзагроза, кібератака, інформаційна війна, боротьба з кібертероризмом.

В статье раскрываются проблемы кибербезопасности Украины. Обращается внимание на научное осмысление терминов «киберпространство», «кибербезопасность». Указано, что до сих пор еще не существует четко определенного содержания указанных сроков, что затрудняет научное осмысление и дальнейшее практичное преодоление тех проблем и вызовов, стоящих в киберпространстве. Актуализируется вопрос кибермогущества государства. Описаны основные угрозы кибербезопасности Украины в контексте российской информационной войны и киберагресии.
Ключевые слова: кибертерроризм, киберугрозы, кибератака, информационная война, борьба с кибертерроризмом.

The article reveals the problems of cybersecurity in Ukraine. Attention is paid to the scientific understanding of the terms “cyberspace”, “cybersecurity”. It is indicated that there is still no clearly defined content of these terms, which complicates scientific comprehension and further more practical overcoming of those problems and challenges that arise in cyberspace. The issue of cyber-power of the state is underway. The main threats to the cybersecurity of Ukraine and the context of the Russian information and cyber-revolution are described.
Key words: cyber terrorism, cyber threats, cyber attack, information war, fight against cyber terrorism.

Виклад основного матеріалу. 2018 р. став роком позитивних кроків у питанні утвердження інформаційної безпеки та інформаційного суверенітету держави. Прийняття у 2017 р. Доктрини інформаційної безпеки України стало фундаментом, на якому держава змогла почати перебудовувати свою діяльність у цій царині на базі підпорядкованості єдиному стратегічному задуму та узгодженості дій різних органів державної влади. Водночас залишається значна кількість стратегічних викликів та загроз у сфері інформаційної безпеки, які потребують першочергового вирішення.

Завдяки системним зусиллям українських державних структур упродовж 2014–2018 рр. вдалося істотно зменшити спроможності РФ щодо поширення на території України власних деструктивних наративів. Цьому сприяло обмеження мовлення російських телеканалів та російського медіа-продукту (телесеріалів, кінофільмів), посилення контролю за друкованою літературою, яка містить висловлювання та наративи, що становлять загрозу національній безпеці, запровадження економічних санкцій (що дало змогу додатково обмежити діяльність частини російських соціальних мереж), точкове висилання з території держави співробітників російських пропагандистських медіа та ін.

Однак ключовою проблемою все ще лишаються стратегічні дезінформаційні кампанії, що реалізуються агресором із залученням усього доступного йому арсеналу прийомів та засобів ведення інформаційної війни.

Останні сформовані РФ у чітку пропагандистську систему, яка спрямовується такою ж чіткою політичною волею керівництва Росії. Ключові цілі таких кампаній відомі і мало змінилися протягом цих років – дискредитація української влади, сіяння розбрату між владою та громадянами як начебто антагоністичних суб’єктів, дискредитація України на міжнародній арені, легітимація анексії АР Криму та терористичних утворень на сході України, інспірування внутрішньополітичного вибуху (в т. ч. використовуючи протиріччя між Україною та деякими сусідніми державами).

При цьому агресор шукає різноманітні шляхи впливу на український медіапростір, використовуючи для цього мережі агентів впливу з числа представників політичної еліти, медіа сфери, церковних структур, псевдонеурядових організацій та окремих публічних осіб. Усі вони активно задіяні у спробах протидіяти становленню України як єдиної, незалежної, суверенної держави. Варто зазначити, що пошук ефективних інструментів протидії дезінформаційним кампаніям має не лише внутрішньоукраїнський, але й більш загальний вимір. Якщо трендом «холодної війни» було засекречування, приховування інформації, то сучасний тренд полягає більше в розкритті та поширенні інформації. При цьому закритість лише збільшує простір для маніпуляцій, у чому дорікають, зокрема, Б. Обамі, який, не поділившись інформацією американської розвідки щодо винуватців катастрофи МН17, надав мовчазну згоду на поширення російської дезінформації та пропаганди [1].

Отже, небажання ***«загострювати»*** ситуацію чіткими та зрозумілими заявами може призводити до зростання

стратегічної переваги агресора у світовому інформаційному просторі. Так само агресор продовжує активно використовувати мережеві інформаційні ресурси, або фінансуючи чинні (шукаючи нові шляхи для цього), або створюючи нові. Справа К. Вишинського та ***«РИА Новости Украина»*** свідчить про те, що ця діяльність не припиняється, однак розслідувати такі справи ще досить складно, у тому числі через недосконаліть українського законодавства.

З аналогічними проблемами стикаються і країни Заходу, які вживають дедалі активніших кроків щодо реформуванням свого нормативно-правового поля з метою недопущення використання мережевих інформаційних ресурсів чи нових медіа з деструктивною метою. Такі ініціативи, як новий закон Німеччини проти використання соціальних мереж для поширення мови ненависті чи французький закон із недопущення використання соціальних медіа з метою дезінформації під час виборів, є тими пріоритетами демократичних практик, на які орієнтується й Україна. Значною мірою проблеми деструктивного використання інтернет-сервісів пов'язані із невизначеністю юридичного статусу інтернет-ЗМІ в Україні та обмеженими можливостями України вплинути на тих інформаційних суб'єктів, що ведуть свою діяльність із території інших країн. Українське законодавство в цій сфері є чи не найбільш ліберальним з усіх європейських держав, що подекуди ставить під загрозу суспільну злагоду та національну безпеку нашої країни.

Водночас ситуація із розслідуваннями США та ЄС щодо окремих соціальних сервісів (соціальних мереж) та ті проблеми, з якими вони стикаються на цьому шляху (в тому числі пошук шляхів правозастосування прийнятих рішень щодо цих сервісів) свідчить про те, що нормативно-правове поле у сфері регулювання інтернету є вкрай [2] недосконалим не тільки в Україні й потребує істотного реформування. При цьому спостерігається брак діалогу між державою та власниками соціальних сервісів, що ускладнює пошук рішення в цій царині.

Варто констатувати, що дедалі більше деструктивних інформаційних впливів в Україні здійснюються на регіональному рівні, причому це характерно не лише для територій, які традиційно є зонами пріоритетного інформаційного впливу російської пропаганди, а й для західних регіонів України, де, крім російського, посилюється інформаційний вплив і сусідніх держав. Питання історичної пам'яті, регіональної політики, забезпечення прав національних меншин дедалі частіше стають предметом маніпуляцій із боку інших держав, але так само і РФ, яка намагається їх використати у власних інтересах. Активізують не завжди дружню інформаційну діяльність у прикордонних регіонах й інші сусідні держави, загострюючи ситуацію в регіоні [3].

Загрозою залишається інформаційне домінування держави-агресора на тимчасово окупованих територіях Криму та Донбасу. Незважаючи на поступово відновлювану мережу теле- та радіомовлення для донесення українських новин на ці території, саме російські наративи здебільшого формують світосприйняття мешканців окупованих територій України. Серед причин такого явища – неповна сформованість державної політики щодо окупованих територій, що ускладнює вироблення спеціалізованого контенту для їх мешканців та протидію російському деструктивному впливу в інформаційній сфері. Водночас з українського боку здійснюються заходи недопущення реалізацій спроб РФ та підконтрольних їй терористичних угруповань поширювати інформаційну агресію на контрольовану Україною територію [4].

Зокрема, у 2018 р. було запущено комплексну систему протидії антиукраїнському мовленню в зоні проведення операції Об'єднаних сил, Луганській та Донецькій областях. За допомогою спеціальних технічних рішень зазначена система не дає змоги поширювати сигнал телевізійного мовлення держави-агресора та підконтрольних їй утворень на території Донецької та Луганської областей (що здійснюється за допомогою неправомірного використання захоплених передавачів українських телерадіокомпаній та радіочастотного ресурсу України). Таке мовлення агресора поширює відверту антиукраїнську пропаганду, яка завдає шкоди національним інтересам та порушує інформаційний суверенітет країни. Значною мірою маніпулятивні впливи з боку агресора стають наслідком усе ще несистемних зусиль із впровадженням медіа грамотності в Україні та слабкими освітніми програмами щодо виховання критичного мислення. Ще однією ареною інформаційного протиборства з агресором залишається кіберпростір.

У 2017 р. у рамках російських кампаній зі знищення української державності здійснено низку кібернетичних операцій проти України, основними з яких були:

«BugDrop» (червень 2016 – березень 2017 рр.);

«WannaCry» (відома як ***«WannaCwt»***, червень 2017 р.);

«NotPetya» (відома також як ***«Petya.A»***, ***«Petya»***, 27–30 червня 2017 р.).

Цілями цих кібероперацій були: добування конфіденційної інформації щодо діяльності об'єктів критичної інфраструктури, органів державного управління, офісів міжнародних, у т. ч. правозахисних, організацій (у т. ч. на тимчасово окупованих територіях Донецької та Луганської областей і в Криму), політичних партій, впливових ЗМІ; перешкоджання роботі систем управління великих компаній, об'єктів енергетичної і транспортної інфраструктури, банківських установ для послаблення української економіки.

За оцінками експертів американської науково-дослідної компанії з кібербезпеки ***«CyberX»,*** внаслідок операції ***«BugDrop»*** підконтрольні Кремлю хакерські угруповання проникали в мережі і системи офісів міжнародних (зокрема правозахисних) організацій, які діяли у т. ч. на тимчасово окупованих територіях Донецької й Луганської областей, об'єктів енергетичної інфраструктури, науково-дослідних установах, деяких впливових ЗМІ, використанні ***«нетипових»*** методів проникнення в обчислювальні мережі для заволодіння конфіденційною інформацією, що циркулює в органах державного управління, на об'єктах критичної, у т. ч. енергетичної, інфраструктури, впливових ЗМІ. Результатом кібероперації ***«WannaCry»*** стало ураження і виведення з ладу близько 300 тис. комп'ютерів у близько 150 країнах, а хакерським угрупованням вдалося шахрайським способом заволодіти коштами, за різними оцінками, у розмірі від 1 до 4 млрд дол. США. Західні експертні установи відповідальність за кібероперацію ***«WannaCray»*** покладають на РФ та КНДР [5].

Спрямовано антиукраїнською була й кібероперація ***«NotPetya»*** 27–30 червня 2017 р. Нині західні уряди публічно визнають, що за цією атакою стояла Російська Федерація. І остання не збирається обмежувати свою протиправну діяльність у кіберпросторі – у 2017 р. вона так само намагалась атакувати енергетичну інфраструктуру США [6] та Великобританії, а у 2018 р. постійно розширювала як географію, так і характер кібератак на західні уряди, охопивши такою діяльністю США [7], Німеччину [8], Великобританію [9], Нідерланди [10]. Потужна кібератака, яку було завчасно викрито, готувалась і проти України – міжнародні дослідницькі структури та українські правоохоронні органи спільно викрили масштабне зараження мережевих пристроїв за допомогою шкідливого програмного забезпечення ***VPNFilter***. На думку СБУ, ця атака готувалася для проведення як кіберрозвідувальної діяльності, так і кібердиверсій (у тому числі проти об'єктів національної критичної інфраструктури). Виявлення та попередження цієї атаки стало можливим завдяки тій роботі, що були здійснена за рік у сфері кібербезпеки України, у тому числі – з допомогою НАТО. У 2017 р. було успішно звершено перший етап Трастового фонду НАТО,

принциповим організаційним та технічним задумом якого була розбудова мережі ситуаційних центрів кібербезпеки [11]. У межах цього етапу в структурі суб'єктів національної системи кібербезпеки такі центри було відкрито в СБУ (Ситуаційний центр забезпечення кібернетичної безпеки) [12], Національному банку України ***(CERT)*** [13] та Державній службі спеціального зв'язку та захисту інформації (Центр реагування на кіберзагрози) [14]. На черзі відкриття ***CERT-ів*** у складі інших суб'єктів національної системи України. Про успішне завершення першого етапу Трастового фонду Україна – НАТО з питань кібербезпеки свідчить і спільна заява Голови СБУ В. Грицака, заступника Генерального секретаря НАТО С. Дукару та заступника директора Румунської служби інформації К. Бізадя, зроблена 4 липня 2017 р. [15]. При цьому сторонами досягнуто домовленостей щодо започаткування другого етапу Трастового фонду Україна – НАТО з питань кібербезпеки, оскільки розроблення та вдосконалення механізмів захисту об'єктів критичної інфраструктури від зовнішніх посягань є критично важливим питанням в умовах сьогодення. У подальшому до спільного контуру безпеки планується включити всі важливі для держави й суспільства об'єкти сектору безпеки та оборони, охорони правопорядку та галузеві об'єкти критичної інформаційної інфраструктури держави [16]. У рамках подальшої реалізації проектів Трастового фонду передбачається створення на базі Головного об'єднаного центру захисту інформації та кібернетичної безпеки в ***ІТС*** Збройних сил України міжвідомчого Центр ситуаційного моделювання систем кіберзахисту у сфері безпеки та оборони.

Завдяки Закону України ***«Про санкції»*** вдалось обмежити поширення на території України програмних продуктів, які могли використовуватись агресором задля збору розвідувальної інформації або шпигування за користувачами таких систем.

У 2018 р. повноцінно запрацювали Стратегія кібербезпеки України і прийнятий у 2017 р. Закон України ***«Про основи кібербезпеки України»*** – державні органи активно здійснюють їх реалізацію. Розвивається міжнародна співпраця України у сфері кібербезпеки. Один із ключових партнерів України з цього питання – США, який надає значну допомогу Україні для розвитку кіберспроможностей українських безпекових органів. Прийнятий у 2018 р. Палатою представників Конгресу США ***«Закон про співпрацю з Україною з питань кібербезпеки»*** дасть змогу додатково систематизувати цю співпрацю. Крім того, цей закон має і важливе політичне значення, засвідчуючи системну підтримку України з боку США у питаннях захисту її кібербезпеки та державного суверенітету.

Однак, незважаючи на докладені зусилля, досі є значна кількість стратегічних проблем у сфері кібербезпеки, які потребують вирішення. Ключовим викликом найближчого часу стане убезпечення демократичного виборчого процесу (на всіх етапах) від кібервтручань із боку РФ. Перші результати розслідування втручання РФ у президентську виборчу кампанію у США 2016 р. вкотре засвідчили масштаби загроз від можливих кібератак контрольованих РФ хакерських угруповань об'єктам критичної інфраструктури будь-якої країни.

У травні 2017 р. президент США призначив екскерівника ФБР США Р. Мюллера керівником незалежної спеціальної групи з розслідування ймовірного втручання РФ у президентську виборчу кампанію США 2016 р. Зважаючи на це, а також на заплановані на 2019 р. президентські та парламентські вибори в Україні, міжнародні експерти, зокрема представники Національного центру кіберзахисту Міністерства національної оборони Литви, прогнозують, що у 2018 р. РФ може розпочати масштабну інформаційну операцію з метою впливу на результати цих виборів. При цьому кібернетичному складнику згаданої інформаційної операції буде відведено ключову роль. Особливості цієї інформаційної операції, найімовірніше, будуть такими: зосередження спеціальними службами РФ основних зусиль на маніпулюванні суспільними настроями та моделюванні поведінки потенційного виборця; ***«комплексний підхід»*** до планування операції із забезпечення необхідних для РФ змін політичного курсу країни.

РФ буде розглядати підсумки голосування тільки як ***«проміжний»*** результат операції, тому після завершення виборчих кампаній втручання Кремля у внутрішні процеси України не припиняться. Україна завчасно готується до такого розвитку подій, напрацьовуючи превентивні рішення в межах завдань Ради національної безпеки й оборони України [17].

Безпека виборів буде істотно ускладнена без ефективної реалізації Стратегії кібербезпеки України, що неможливо без проведення оцінки ефективності її виконання. Введена в дію у 2016 р. вона активно реалізується суб'єктами національної системи кібербезпеки. Однак і до цього часу відсутня комплексна система оцінки її виконання, що робить неможливим оцінити ефективність докладених зусиль, зрозуміти, які проблеми виникають на шляху реалізації. Через те незрозумілим є, наскільки ефективно органи державної влади діють у цій сфері та чи потребує зазначена стратегія корегування. Досі невирішеним залишається питання осучаснення системи ***КСЗІ*** або її заміна на інші системи захисту. Сама ідея, внутрішня структура й модель впровадження ***КСЗІ*** здебільшого не відповідають вимогам сучасного кіберзахисту (особливо в недержавному секторі, надто ж у бізнесі). Це стає причиною перманентної гострої критики у вітчизняних експертних та бізнесових колах, яка зосереджується на статичності системи, її громіздкості та обмеженості в можливості масштабування.

Крім того, Закон України ***«Про основні засади забезпечення кібербезпеки України»*** вимагає проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО, відповідна нормативна база нині активно напрацьовується.

Об'єкти критичної інфраструктури та їх захист також є однією з важливих проблем сфери кібербезпеки, що має бути вирішена найближчим часом. На жаль, досі не було створено реєстру об'єктів критичної інформаційної інфраструктури, що мав бути затверджений Кабінетом Міністрів України ***(водночас із 2016 р. діє Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений Постановою КМУ № 563 від 23 серпня 2016 р.)***. Відсутність такого реєстру створює проблеми у формуванні єдиної політики їх захисту, а тому ускладнює реалізацію державної політики щодо сфери кібербезпеки.

Водночас суб'єкти національної системи кібербезпеки намагаються здійснювати безпекову політику в цій царині й на поточному етапі. Зокрема, Службою безпеки України спільно з розпорядниками окремих об'єктів критичної інфраструктури досягнуто попередніх домовленостей щодо надання доступу до інформаційної системи Malware Information Sharing Platform and Threat Sharing ***«Ukrainian Advantage»*** з метою обміну ідентифікаторами компрометації, що використовувались у цільових кібератаках. Крім того, Державним центром кіберзахисту та протидії кіберзагрозам Держспецзв'язку було розроблено проект Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також усунення їхніх наслідків.

Останнє ставить питання про більш інтенсивний розвиток сфери кібербезпекового державно-приватного партнерства, а в більш загальному сенсі – побудови довгострокових

довірчих відносин між урядовими та бізнес структурами у сфері забезпечення кібербезпеки. Брак довіри між сторонами робить практично неможливою розбудову справді ефективної загальнодержавної системи кібербезпеки, особливо зважаючи на те, що значна кількість об'єктів критичної інфраструктури перебуває у приватній власності. Розбудова такої довіри має базуватися на основі передбачуваності дій сторін, розуміння мотивів прийняття рішень та наявності спільно реалізованих проектів у сфері кібербезпеки.

Висновки. З метою посилення захисту вітчизняного інформаційного простору видається необхідним посилити спроможності та активізувати взаємодію компетентних правоохоронних органів за такими напрямами:

– виявлення, попередження та локалізація (припинення) спеціальних інформаційних операцій із боку країни-агресора проти України;

– виявлення фактів та намагань маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації, нагнітання панічних настроїв у засобах масової інформації, у тому числі у мережі Інтернет;

– моніторинг впливу на вітчизняний медіа-ринок процесів, що відбуваються в інформаційній, політичній, економічній, соціальній та інших сферах, із метою прогнозування змін, які відбуваються в них, потенційних загроз інформаційній безпеці та своєчасного реагування;

– посилення контролю за діяльністю закордонних інформаційних структур та їх функціонерів, насамперед РФ, вжиття дієвих заходів щодо недопущення з їх боку здійснення антиукраїнської інформаційної діяльності;

– вжиття додаткових заходів, спрямованих на блокування поширення в ЗМІ та інтернет-просторі матеріалів, що містять заклики до посягання на державний суверенітет, територіальну цілісність України, розпалювання міжнаціональних, міжконфесійних конфліктів, пропаганду війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Eight EU countries oppose construction of Nord Stream-2. URL: https://www.ukrinform.net/rubric-economy/1983580-eight-eu-countries-oppose-construction-of-nord-stream2.html.

2. U.S. Says Planned Russian Pipeline Would Threaten European Energy Security. URL: https://money.usnews.com/investing/news/articles/2018-01-27/uss-tillerson-says-nord-stream-2-pipeline-would-undermine-europes-energy-security.

3. Робимо все, щоб донести об'єктивну картину і не дати Росії використовувати «Північний потік – 2» як елемент гібридної агресії – Президент. / Офіційний сайт Президента України. URL: http://www.president.gov.ua/videos/robimo-vse-shob-donesti-obyektivnu-kartinu-i-nedati-rosiyi-566.

4. Secretariat transfers complaint against Nord Stream 2 project to European Commission. URL: https://www.energy-community.org/news/Energy-Community-News/2016/01/05.html.

5. The Top Secret Scandal Behind the Kremlin's MH17 Massacre. URL: http://observer.com/2018/05/kremlin-responds-to-netherlands-australia-blame-russia-for-mh17-crash/.

6. США заявляють про кібератаки на комп'ютерні системи своїх АЕС. *Радіо Свобода.* 8 липня 2017. URL: https://www.radiosvoboda.org/a/news/28602970.html.

7. ЗМІ: адміністрація Трампа звинуватила РФ в кібератаках на енергосистему США. *Українська правда.* 15 березня 2018. URL: https://www.eurointegration.com.ua/news/2018/03/15/7078844/.

8 Глава розвідки Німеччини: Москва, дуже ймовірно, стоїть за кібератакою на німецький уряд. *Українська правда.* 11 квітня 2018. URL: https://www.eurointegration.com.ua/news/2018/04/11/7080217/.

9 США і Великобритания застерігають світ щодо кібератаки з боку Росії. DW. 17.04.2018. URL: https://tinyurl.com/yah848aq.

10. У Нідерландах заявили про кібератаки на великі банки – ЗМІ. *Укрінформ.* 29.01.2018. URL: https://www.ukrinform.ua/rubric-world/2392133-u-niderlandah-zaavili-pro-kiberataki-na-veliki-banki-zmi.html.

11. Петров В.*В*. Співробітництво України з НАТО щодо забезпечення кібербезпеки. *Міжнародні відносини. Серія політичні науки.* 2018. № 18. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3384.

12. Голова СБУ відкрив Ситуаційний центр забезпечення кібернетичної безпеки. Служба безпеки України. 25.01.2018. URL: https://ssu.gov.ua/ua/news/1/category/21/view/4318#.QU9ehlwS.dpbs.

13. При НБУ создали Центр киберзащиты. Банкам уже передали список сайтов-взломщиков. Вот он. *Інше ТВ*. 01.02.2018. URL: https://inshe.tv/economics/2018-02-01/304057/.

14. Відкриття Центру реагування на кіберзагрози. CERT-UA. URL: https://cert.gov.ua/news/25.

15. У СБУ відбулася церемонія завершення першого етапу Трастового фонду НАТО зі сприяння Україні в зміцненні кіберзахисту. URL: https://www.ssu.gov.ua/ua/news/1/category/2/view/3668#.dnBn8P1V.dpbs.

16. Петров В.В. Співробітництво України з НАТО щодо забезпечення кібербезпеки. *Міжнародні відносини. Серія політичні науки.* 2018. № 18. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3384.

17. Офіційний Twitter-акаунт Президента України. URL: https://twitter.com/poroshenko/status/1026717307198947328.