DOI: 10.15421/152031 УДК: 004.49+316.772.5

Віктор Бондаренко
Дніпропетровський регіональний інститут державного управління
Національної академії державного управління при Президентові України

Кібербезпека: роль держави у захисті суспільства та окремої особистості у збереженні міжетнічного миру

Кібербезпека, кібервійни, інформаційні війни, кіберзахист, кіберпростір – поняття, які останнім часом все більше заполоняють простір навколо кожної людини. Усе частіше ми чуємо ці слова, усе частіше вони відіграють важливу роль. Зростає й роль держави у захисті національного суспільного простору, захисті окремої людини у цьому інформаційному протистоянні. Не менш важливою стає в нашому швидкоплинному світі все більш зростаюча проблема захисту міжетнічного миру в країні, а особливо в таких поліетнічних державах як Україна. У наш час навіть відносно моноетнічні держави через активні міграційні процеси й значні економічні зміни повинні займатись питаннями безпеки міжетнічного простору. Адже безпека інформаційного простору – тепер, безперечно, це теж безпека держави.

Ключові слова: *інформаційна війна, кібербезпека, кібервійна, кіберзахист, кіберпростір, етнос, етносоціологія, синтез наук, соціальна структуризація, соціоетнологія, соціологія, суспільство*

Cyber security: the role of the state in protecting society and individual personality in maintaining interethnic peace

Viktor Bondarenko, Dnipropetrovsk Regional Institute for Public Administration National Academy for Public Administration under the President of Ukraine

Cybersecurity, cyberwarfare, information wars, cyber defense, cyberspace - concepts that have recently increasingly filled the space around everyone. More and more often we hear these words, more and more often they play an important role. The role of the state in the protection of the national social space, the protection of the individual in this information confrontation is also growing. Equally important in our fleeting world is the growing problem of protecting interethnic peace in the country, and especially in such polyethnic states as Ukraine. Nowadays, even relatively mono-ethnic states, due to active migration processes and significant economic changes, have to deal with the security of the interethnic space. After all, the security of the information space is now, without a doubt, also the security of the state.

Keywords: *information war, cybersecurity, cyberwar, cyber defense, cyberspace, ethnos, ethnosociology, synthesis of sciences, social structuring, socioethnology, sociology, society*

Аналіз ролі держави у захисті суспільства та окремої особистості, а також у збереженні етнічного миру в державі, у галузі кібернетичної безпеки заслуговує особливої уваги. Тим більш у часи, коли в світі постійно обговорюють питання кібервійн. Одні кажуть, що вони вже йдуть, інші – що наступна світова війна почнеться й буде вестись значною мірою в кіберпросторі як кіберзіткнення, а дехто – що наступна світова війна й буде Світовою Кібервійною.

Як там буде далі – це питання аналітиків політики, але вже у 2014 році стало зрозуміло, що Україна була раніше й лишається жертвою кібератак (і не тільки кібер-) з боку Росії як агресора, що поставило країну на грань втрати державності чи, як мінімум, створило серйозніші загрози безпеці країни. От саме наш досвід і свідчить про те, що кібербезпека грає значну роль у захисті суспільства та окремої людини, а також і в збереженні етнічного миру у поліетнічній державі.

Головним підґрунтям для функціонування й розвитку будь-якої сфери є законодавча база. У наші часи багато країн світу вже ухвалили кіберзаконодавство. В Україні теж є Закон України «Про основні засади

забезпечення кібербезпеки України», який «визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки» (Про основні засади забезпечення кібербезпеки України, 2017).

Отже, вже зрозуміло, що тільки становлення інформаційного суспільства сприяє створенню ефективного та успішного суспільства і, одночасно, надаючи нових імпульсів загрозам безпеки держави та створюючи нові складнощі для системи національної безпеки, формує умови задля пошуку нових можливостей забезпечення безпеки держави з огляду на нове поле протиборства – кіберпростор (Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка).

На підтвердження цього можна згадати про підписання під час зустрічі на вищому рівні глав держав та голів урядів країн-учасниць НАТО, яка проходила у Варшаві у 2016 році, першого в історії договору між ЄС та НАТО про співпрацю у сфері безпеки, зокрема в питаннях гібридних війн та кібератак. Кіберпростір, разом із землею, повітрям, морем і космосом, визнано новим простором можливих зіткнень, а кібероперації – частиною реальної гібридної війни (Кібербезпека як важлива складова всієї системи захисту держави, 2018).

Європейський Союз взагалі постійно є одним з лідерів створення умов для мережевої та інформаційної безпеки. Ще у 2004 році в ЄС у зв'язку з розумінням важливості проблеми кібербезпеки було створено Європейське агентство з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security), яке з часом перетворилось на центр експертизи щодо отримання консультацій з питань, пов'язаних із мережевою та інформаційною безпекою, для держав-членів ЄС й її інституцій. Завдяки цьому кроку у більшості країн-членів було створено національні стратегії кібербезпеки та національні плани із захисту інформаційної інфраструктури. У 2013 році відбулося логічне завершення процесу відкритого, надійного і безпечного кіберпростору з ухваленням Стратегії кібербезпеки Євросоюзу (Кібербезпека як важлива складова всієї системи захисту держави, 2018).

Що ж стосується країн НАТО, то кіберзахист є тут зараз основним аспектом оновлення Альянсу та його адаптації до нових загроз. Після ухвалення на саміті в Лісабоні в листопаді 2010 року нової стратегічної концепції організація 28 червня 2011 року затвердила політику НАТО щодо кіберзахисту, а у вересні 2014 року під час саміту у Ньюпорті (Уельс) її було розширено (Хлапонін, Кондакова, Шабала, Юрчук, & Демянчук, 2019, с. 8).

Провідні інформаційні країни світу по різному ставляться до кібербезпеки й до формування своєї політики щодо цієї сфери (Ліпкан, & Діордіца, 2017, с. 177–178). Японія, Південна Корея і Великобританія ретельно відстежують ситуацію й роблять важливі кроки щодо захисту своїх суспільств від кіберагресій. Китай же, виходячи з цілей захисту суверенітету свого простору й збереження наявного державного ладу, має великі можливості проводити свої великі кібератаки під прикриттям у політичних чи економічних цілях (Хлапонін, Кондакова, Шабала, Юрчук, & Демянчук, 2019, с. 8–11).

І за кордоном, і в Україні особливою темою є інноваційна стратегія регіонів. За останні десятиліття накопичені різні підходи до її побудови. Спосіб побудови інноваційної стратегії розвитку регіону та спосіб здійснення втручання (інтервенції) мають важливі наслідки для всього процесу перетворень у регіоні. Задля результативної політики кібербезпеки стосовно захисту безпеки держави й безпеки її регіонів.

Впровадження такої політики передбачає, що через взаємодію з мережами організацій усередині регіону ініціюється процес постійного вивчення результатів перетворень, відбувається апробація запропонованої парадигми, що значно підвищує інноваційність, власне, самих учасників цього процесу і окремих особистостей (Квітка, & Соколовська, 2013, с. 90–91).

З урахуванням того, що головною тенденцією розвитку сучасної міжнародної системи права стало зміцнення поваги до прав людини, захисту людської особистості, так звана гуманізація, це обумовлювало й рух до збереження міжетнічного миру в державі як одного з його аспектів (Молдавчук, 2016, с. 19–21).

Порівнюючи гібридну війну зі звичайною, де вирішуються міжетнічні конфлікти, – відрізняють в них лише цілі та інструменти. Дуже важливо вчасно визначити, коли саме тиск у кіберпросторі у прийнятних межах перетворюється безпосередньо на дестабілізацію країни. На прикладі України можна побачити, яким чином відбулася інтеграція всіх інструментів гібридної війни – це і довгострокова підготовка в кіберпросторі, це і дії, націлені на місцеві етнічні групи населення, у першу чергу, на етнічних росіян і російськомовних. Багаторічна координація з інформаційної кампанії створила уяву, що йдеться не про анексію, а про мирне «перейняття», яке було ініційовано в самій Україні. І Росії це вдалося, не дивлячись на представлення безлічі доказів того, що гібридна атака й кібервійна легальними не були і бути не могли (Трутненко, & Стеценко, 2018).

Аналіз загальних моделей дозволив зробити висновки, що в процесі націєтворення міжетнічна сумісність виявляється під загрозою й створює конфліктногенні й деформовані зони. Найбільш же етноконфліктогенними виявляються перехідні періоди, коли суспільства індустріально-громадянського типу і міжетнічної сумісності переходять від старого до нового етапу утворення націй, коли відмирають аграрно-станові типи соціоетнічних ролей, статусів і відносин і переростають у нові, індустріально-громадянські типи.

Сьогодні людство живе в інформаційному суспільстві. Інформація – є рушійною силою перетворень та розвитку людства, а запорукою його процвітання є людська інтелектуальна творчість. Отже, головним об'єктом, на якому концентрується безпосередній інформаційний деструктивний вплив у межах інформаційної війни, стали громадська думка та свідомість окремої людини. Саме тому духовні, культурні, історичні, етнічні й загальнонаціональні цінності, традиції, надбання держави стають полем кібербитви, адже це той простір, де дуже багато вразливих й чутливих рецепторів суспільства.

Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Водночас руйнування, яких завдають інформаційні війни у суспільній психології, психологічній етнічній атмосфері, психології особи, за масштабами і за значенням цілком співмірні, а часом і перевищують наслідки збройних воєн. Дестабілізація міжетнічних відносин, розбурхування напруження між етнічними об'єднаннями й рухами з метою провокації конфліктів, розпалювання міжетнічної недовіри, підозрілості, що напевно призводить до загострення політичної боротьби, провокування репресій і навіть може спровокувати громадянську війну – от цілі гібридних і кібервійн у міжетнічній сфері (Малик, 2015).

Підсумовуючи висловлене, можна стверджувати, що в період інформаційної війни ворог може маніпулювати свідомістю для широкомасштабної експансії і загрожує національній безпеці. Кіберзахист – це єдине, що може запобігти втратам інформації та втручанню одних країн в безпеку інших. Тому держава повинна розвивати свою кібербезпеку, що дозволить захистити суспільство загалом та окрему особистість і зберегти етнічний мир у кожній країні.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Бойко, В. Д., Василенко, М. Д., & Кухаренко, С. В. *Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення*. Відновлено з http://academy.ssu.gov.ua/ua/page/page_1581426437.htm

Про основні засади забезпечення кібербезпеки України. № 2163-VIII. (2015). Відновлено з https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Квітка, С. А., & Соколовська, О. О. (2013). Розробка інноваційних стратегій та їх впровадження в соціально-економічну структуру регіону. *Аспекти публічного управління*, *1 (2)*, 90–93.

Кібербезпека як важлива складова всієї системи захисту держави. (2018). *Офіційний веб сайт Міністерства оборони України*. Відновлено з https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

Ліпкан, В., & Діордіца, І. (2017). Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право,* 5, 174–180.

Малик, І. (2016). Інформаційна безпека суспільства та інформаційні війни: співвідношення понять. *Актуальні проблеми міжнародних відносин та зовнішньої політики.* Матеріали ІІІ Регіональної науково-теоретичної конференції (Львів, 24 березня 2016 р.). (с. 126). Львів: НУ ЛП.

Малик, Я. (2015). Інформаційна війна і Україна. Демократичне врядування. *Науковий вісник*, 15.

Молдавчук, М. (2016). Проблема гуманітарної інтервенції у сучасній міжнародній політиці. А*ктуальні проблеми міжнародних відносин та зовнішньої політики. Матеріали ІІІ Регіональної науково-теоретичної конференції* (Львів, 24 березня 2016 р.). (с. 126). Львів: НУ ЛП.

Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. *Національний інститут стратегічних досліджень*. Відновлено з http://old2.niss.gov.ua/articles/294/

Тимофєєва І. Б. (Укл.). (2017). *Кібербезпека та системи захисту інформації: виклики сьогодення:* збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня 2017 р. Маріупольський державний університет; Кафедра математичних методів та системного аналізу. Маріуполь: МДУ.

Трутненко, І., & Стеценко, С. (2018, 14 грудня). «Найяскравішим прикладом гібридної війни 21-го століття є війна в Україні» – чеський генерал. *Радіо Свобода*. Відновлено з https://www.radiosvoboda.org/a/29656992.html

Хлапонін, Ю. І., Кондакова, С. В., Шабала, Є. Є., Юрчук, Л. П., & Демянчук, П. С. (2019). Аналіз стану кібербезпеки в провідних країнах світу. *Кібербезпека: освіта, наука, техніка*, 4 (4), 6–13.