УДК 32.019.51.004.738.5:061-1 ЄС
DOI: 10.31673/2409-7292.2019.023741

Т.М. Мужанова, Ю.М. Якименко

ДОСВІД ЄВРОПЕЙСЬКОГО СОЮЗУ З ПРОТИДІЇ ДЕСТРУКТИВНІЙ ІНФОРМАЦІЙНІЙ ДІЯЛЬНОСТІ В МЕРЕЖІ ІНТЕРНЕТ

У статті окреслено передумови розширення масштабів деструктивної інформаційної діяльності в мережі Інтернет, розглянуто сутність та види заходів інформаційно-психологічного впливу в Інтернеті. Автори проаналізували діяльність Європейського Союзу зі стратегічних комунікацій (2015-2019 рр.), спрямовану на запобігання та протидію небезпечному для ЄС інформаційно-психологічному впливу у всесвітній мережі.

***Ключові слова**:* деструктивна інформаційна діяльність у мережі Інтернет, пропаганда, дезінформування, стратегічні комунікації.

Вступ

В умовах функціонування глобальної мережі Інтернет геополітична боротьба між державами та іншими суб'єктами поступово переходить у інформаційну сферу. З огляду на те, що можливості Інтернету дозволяють вплинути на величезні, різноманітні, а часто й фізично важко досяжні аудиторії з використанням відносно незначних ресурсів, більшість провідних держав переорієнтували свою політику на здобуття й утримання інформаційної переваги на просторах всесвітньої мережі.

Статистика свідчить, що кількість користувачів мережі Інтернет постійно зростає: у жовтні 2018 року у світі налічувалося майже 4,2 мільярда користувачів Інтернету, що становить 55% всього населення планети і у порівнянні з попереднім роком цей показник зріс на 7%. Найбільше охоплення Інтернетом спостерігається у Північній Америці (90%) та Європі (85%). В Україні кількість користувачів становить 25,6 млн. осіб (58% від усього населення [6].

Безсумнівними є такі переваги Інтернету як доступність, швидкість і анонімність, що також сприяє зростанню кількості його користувачів. Крім того, все більше громадян, не довіряючи традиційним ЗМІ, звертаються до альтернативних джерел в Інтернеті у пошуках об'єктивної інформації.

У комплексі зазначені чинники сприяють посиленню тенденції щодо використання геополітичними суб'єктами Інтернет-ресурсів та соціальних мереж для здійснення деструктивного інформаційно-психологічного впливу, зокрема дезінформування та пропаганди, і відкривають широкі можливості впливу на багатомільярдну аудиторію.

Внаслідок цього виникають серйозні загрози безпеці глобального інформаційного простору загалом і безпеці окремих його суб'єктів, у нашому випадку – держав, зокрема. Отже, запобігання й протидія деструктивним інформаційним діям у мережі Інтернет є першочерговим завданням кожної держави, яка дбає про захищеність свого інформаційного простору від зовнішніх впливів та прагне протидіяти загрозам інформаційній безпеці. Відповідно дослідження зазначених актуальних проблем сприятиме науковому обґрунтуванню шляхів їх вирішення.

Основна частина

Характеризуючи інформаційні заходи геополітичних Інтернет-гравців, варто відзначити, що вони можуть бути спрямовані як на все населення держави, жителів окремих регіонів чи представників етнічних груп, так і на суб'єктів, які відіграють важливу роль у забезпеченні національної безпеки: політиків, чиновників владних інституцій, військовослужбовців та представників інших силових структур, а також на світову громадськість, керівництво зарубіжних держав і міжнародних організацій.

Деструктивна інформаційна діяльність в Інтернеті має переважно прихований характер, щоб зберегти у таємниці зацікавленість і причетність суб'єкта-ініціатора до їх проведення. Заходи інформаційно-психологічного впливу можуть бути:

– пропагандистськими (просування певних ідей з метою формування їх підтримки обраними цільовими групами),

– дезінформаційними (введення в оману, надання неправдивої, упередженої інформації);

– маніпулятивними (здійснення прихованого інформаційно-психологічного впливу на аудиторію з метою зміни його ставлення до певних проблем та програмування поведінки на підтримку чи на сприйняття ідей вигідних ініціатору інформаційного впливу);

– компрометуючими (об'єктами є органи державної влади та посадові особи, окремі дії чи загалом політика уряду, які виставляються у негативному, невигідному для них світлі);

– дестабілізуючими (з метою розхитування суспільно-політичної чи економічної ситуації в державі-жертві, загострення міжнаціональних, міжетнічних, міжконфесійних конфліктів тощо).

Сьогодні інформаційні дії в мережі Інтернет найчастіше є частиною спеціальних інформаційних операцій, які є комплексом інформаційних зусиль з використанням як традиційних каналів комунікації (телебачення, радіо, друкові видання, наочні засоби тощо), так і електронних (від новинних та розважальних до наукових і вузькопрофесійних Інтернет-ресурсів, соцмереж).

Сутність заходів інформаційно-психологічного впливу в мережі Інтернет полягає в організованому навмисному поширенні неправдивих чи упереджених повідомлень у масових масштабах з метою досягнення політичних цілей держав, що здійснюють інформаційну експансію. Незважаючи на те, що такі заходи відбуваються фактично у віртуальному просторі, вони мають цілком реальні наслідки: втручання в процеси державного управління, дестабілізацію об'єктів критичної інфраструктури, підвищення соціальної напруги, загострення міжетнічних, міжконфесійних конфліктів, диверсифікацію громадської думки тощо.

Тому, навіть потужним державам і наддержавним утворенням життєво необхідно захищати власний інформаційний простір шляхом запобігання та протидії деструктивним інформаційним діям опонентів у мережі Інтернет.

Значних успіхів у цьому напрямку досяг Європейський Союз, який упродовж останніх років впровадив комплекс заходів щодо здійснення стратегічних комунікацій, які мають забезпечити вирішення проблеми поширення в мережі Інтернет небезпечного для ЄС інформаційно-психологічного впливу.

Відповідно до нормативних документів Євросоюзу загальними цілями стратегічних комунікацій є: ефективне спілкування та просування політики та цінностей ЄС, зокрема у рамках Східного партнерства; зміцнення загального медіасередовища, включаючи підтримку незалежних ЗМІ; підвищення поінформованості громадськості про дезінформаційну діяльність з боку зовнішніх суб'єктів; покращення спроможності ЄС передбачати та реагувати на деструктивні інформаційні заходи [2].

Загалом діяльність інституцій Європейського Союзу щодо запобігання та протидії деструктивній інформаційній діяльності в мережі Інтернет (2015-2019 рр.) можна подати у вигляді схеми (Рис.1.).

З метою інституційного забезпечення стратегічних комунікацій як на рівні ЄС, так і окремих його країн-членів сформовані спеціальні підрозділи. Так, у 2015 році при Європейській службі зовнішніх справ (European External Action Service, EEAS) створено Оперативну робочу групу ЄС зі стратегічних комунікацій (East StratCom Task Force), діяльність якої спрямована на роз'яснення ключових аспектів політики ЄС, формування його позитивного іміджу та протидію дезінформації; сприяння свободі ЗМІ; вдосконалення механізмів прогнозування, оцінки та реагування ЄС на дезінформацію з боку зовнішніх акторів тощо. До речі, у складі Європейської служби зовнішніх справ вже діяв Центр аналізу гібридних загроз (Hybrid Fusion Cell), який займався стратегічними комунікаціями як складовою протидії гібридним загрозам.

Подібні органи функціонують також і в країнах-членах ЄС: у Польщі діють два відділи стратегічних комунікацій - у Міністерстві національної оборони і в Міністерстві внутрішніх

справ; у Чехії такий підрозділ функціонує на базі Міністерства внутрішніх справ; у Нідерландах - Міністерства закордонних справ; у Словаччині створена окрема урядова установа зі стратегічних комунікацій. Відповідно, такі структури складаються з представників міністерств і відомств безпекового спрямування: внутрішніх та закордонних справ, оборони та безпеки, і залежно від ситуації до груп залучаються інші міністерства (освіти, культури тощо), а також представники громадськості.

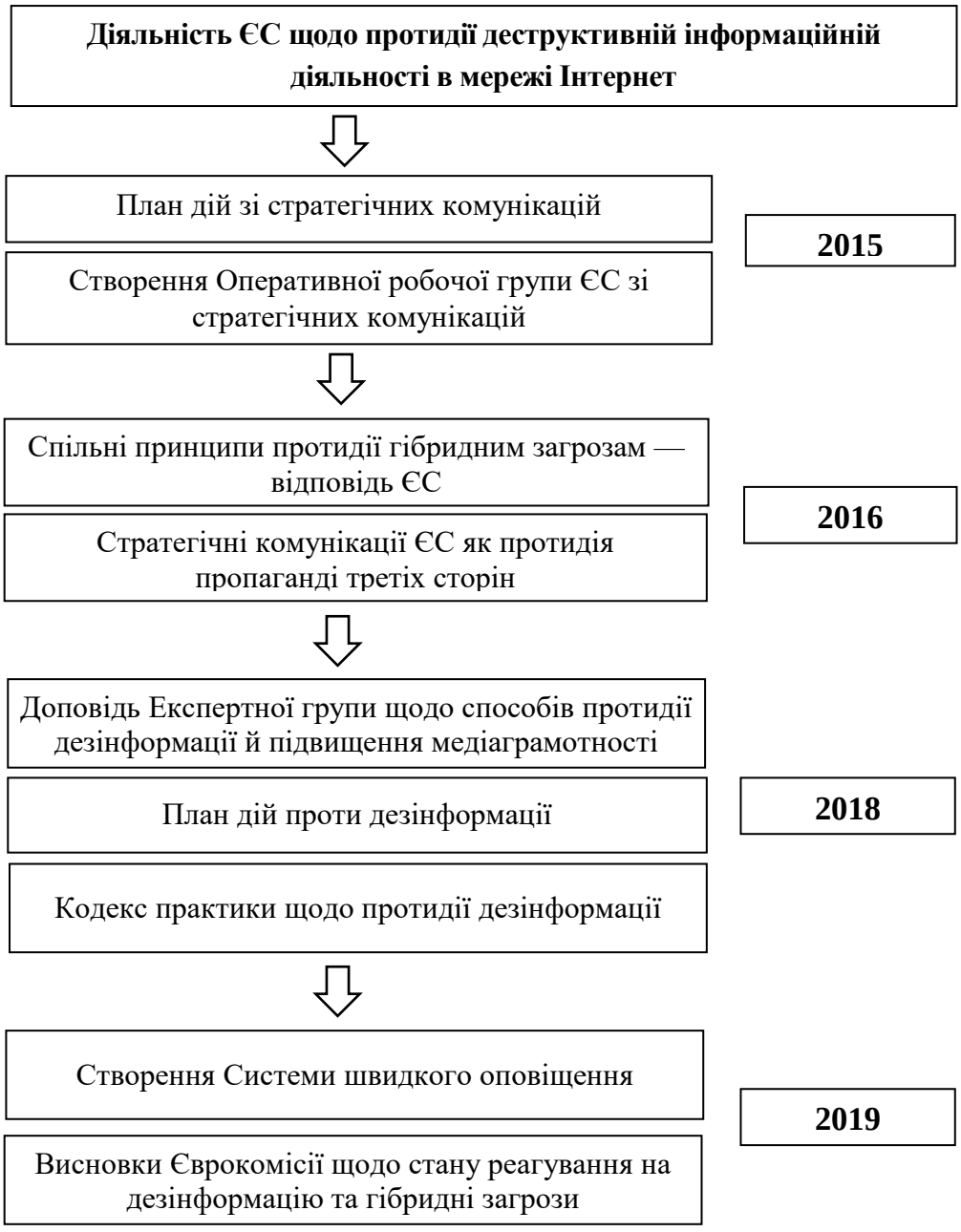

Рис.1. Діяльність ЄС з протидії деструктивній інформаційній діяльності в мережі Інтернет (2015-2019 рр.)

Також у деяких європейських державах створені регуляторні органи у сфері телекомунікацій, наприклад, у Великобританії з 2001 року діє державний медіарегулятор Ofcom (Управління з комунікацій), а у Франції з 1989 року – CSA (Вища аудіовізуальна рада). Ці органи регулюють діяльність телекомунікаційних компаній і мають повноваження виносити попередження і накладати санкції за порушення норм законодавства.

У 2019 році створено Систему швидкого оповіщення (Rapid Alert System) серед інституцій та держав-членів ЄС для сприяння обміну інформацією й обговоренню проблем, пов'язаних з дезінформаційними кампаніями в Інтернеті, поширення кращих практик щодо протидії дезінформації та координації дій з реагування на деструктивні інформаційні дії. RAS базується на інформації з відкритим вихідним кодом, а також спирається на ідеї науковців, фахівців з перевірки фактів, представників онлайн-платформ та міжнародних партнерів. Координатором діяльності 28-ми національних контактних пунктів у рамках Системи швидкого оповіщення визначено Європейську службу зовнішніх справ.

Основоположну роль для здійснення ефективних стратегічних комунікацій в Євросоюзі відіграє законодавча база. Особливістю європейської практики є те, що нормативно-правове регламентування зазначених питань здійснено у багатьох країнах-членах Європи, водночас деякі стратегічно важливі питання, серед яких міжнародне право, просування демократії, захист прав людини, засади Східного партнерства, а також протидія пропаганді, розробляються на рівні ЄС.

Розглянемо детальніше основні положення нормативних документів Євросоюзу з питань стратегічних комунікацій, протидії пропаганді й дезінформації. Системну нормотворчу діяльність за цим напрямом розпочато у 2015 році. План дій зі стратегічних комунікацій ЄС (Action Plan on Strategic Communication) був розроблений у співпраці з наднаціональними інституціями ЄС та державами-членами і представлений у червні 2015 року. У документі окреслено координаційні та моніторингові заходи щодо питань, пов'язаних зі Східним партнерством та діяльністю поза його межами, а також зусиллями ЄС щодо підтримки свободи ЗМІ та зміцнення спільного медіасередовища [2].

У 2016 році Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам - відповідь Європейського Союзу» (Joint Framework on countering hybrid threats a European Union response) [7], де наголошено на необхідності вироблення державами-членами ЄС узгоджених механізмів реалізації стратегічних комунікацій для протидії дезінформації та публічного викриття гібридних загроз через Інтернет-ЗМІ та соціальні мережі.

У Резолюції Європейського парламенту «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін» (EU strategic communication to counteract propaganda against it by third parties) [5] зазначається, зокрема, що в умовах ведення гібридної війни дезінформація та пропаганда є важливими її складниками і для їх протидії необхідним є здійснення проактивної політики інформування із залученням інституцій і країн-членів ЄС, різноманітних органів НАТО й ООН, неурядових організацій.

У березні 2018 р. Єврокомісія опублікувала доповідь Експертної групи щодо способів протидії дезінформації й підвищення медіаграмотності. Автори доповіді рекомендували, зокрема, збільшити допомогу й фінансування незалежних організацій, які займаються перевіркою істинності фактів (фактчекінгом), медіакритикою і медіаосвітою; сприяти взаємодії ЗМІ з соціальними мережами і фактчекінговими організаціями з метою здійснення швидкої перевірки інформації та її джерел і, як наслідок, вчасному запобіганню дезінформації; ввести курси медіаосвіти в школах.

У результаті подальшої роботи у грудні 2018 року представлено План дій проти дезінформації (Action Plan against Disinformation) [1], в якому виділено чотири сфери, які є ключовими для розвитку потенціалу Євросоюзу та зміцнення співпраці між державами-членами та ЄС у справі протидії дезінформації: удосконалення механізмів виявлення дезінформації, забезпечення скоординованого реагування, визначення зобов'язань у цій сфері онлайн-платформ та Інтернет-індустрії, сприяння медіаосвіті. У Плані дій зазначено, що видатки ЄС на стратегічні комунікації у 2019 році зростуть більше ніж удвічі у порівнянні з попереднім роком: з 1,9 до 5 млн. євро.

Важливим кроком у протидії деструктивним інформаційним впливам в мережі Інтернет стало підписання Інтернет-платформами Facebook, Google і Twitter, Mozilla, а також рекламодавцями і представниками рекламної індустрії Кодексу практики щодо протидії дезінформації (Code of Practice on Disinformation) [3] у жовтні 2018 р. У травні 2019 року

Кодекс практики підписала компанія Microsoft, а також представила свою дорожню карту. Відповідно до Кодексу підписанти погодилися об'єднувати свої зусилля з протидії дезінформуванню за такими напрямами: нагляд за рекламними майданчиками, політична і тематична реклама, повнота послуг, розширення прав і можливостей споживачів та наукової спільноти.

На неформальній зустрічі лідерів ЄС в Сібіу (Informal EU27 Leaders' Meeting) у травні 2019 року були представлені висновки Європейської Комісії щодо стану реагування на дезінформацію та гібридні загрози, де, зокрема, відзначено потребу в підтриманні стабільних зусиль для підвищення обізнаності, підвищення готовності та зміцнення стійкості європейської демократії до дезінформації, а також у проведенні поглибленої оцінки виконання зобов'язань, прийнятих онлайн-платформами та іншими підписантами згідно з Кодексом практики. Наголошено, що зростаючий ризик шкідливого втручання та онлайнових маніпуляцій, пов'язаних з розробкою методів штучного інтелекту та збору даних, вимагають постійної оцінки та відповідного реагування [4].

Висновки

Як показало дослідження, з метою запобігання та протидії деструктивним інформаційним діям в мережі Інтернет Європейський Союз проводить проактивну й ефективну політику стратегічних комунікацій, яка поєднує ведення постійної інформаційно-просвітницької діяльності для пропагування засад і демократичних цінностей ЄС, здійснення перевірки і спростування фейкових повідомлень, підтримку діяльності незалежних ЗМІ, моніторинг і оцінку інформаційних загроз, скоординоване реагування на негативні інформаційні дії. Позитивною рисою європейської політики стратегічних комунікацій є забезпечення активної співпраці інституцій ЄС та країн-членів, онлайн-платформ, міжнародних та неурядових організацій, ЗМІ для вирішення поставлених завдань.

Водночас варто звернути увагу на зростаючу потребу у виробленні й нормативному закріпленні критеріїв для розмежування деструктивної та конструктивної інформаційної діяльності, спрямованої, наприклад, на захист національних інтересів. Крім того, важливим є забезпечення балансу між введенням санкцій за пропаганду і дезінформування та дотриманням демократичних прав і свобод громадян.

Список використаної літератури

1. Action Plan against Disinformation [Електронний ресурс]. – Режим доступу: https://eeas.europa.eu/headquarters/headquarters-homepage/54866/action-plan-against-disinformation_en (дата звернення 28.07.2019)

2. Action Plan on Strategic Communication // European External Action Service. – June 2015 – 5 p. [Електронний ресурс]. – Режим доступу: http://archive.eapcsf.eu/assets/files/ Action%20PLan.pdf (дата звернення 28.07.2019)

3. Code of Practice on Disinformation [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (дата звернення 28.07.2019)

4. European Council conclusions on the MFF, climate change, disinformation and hybrid threats, external relations, enlargement and the European Semester, Press release, 20 June 2019 [Електронний ресурс]. – Режим доступу: https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/european-council-conclusions-20-june-2019/ (дата звернення 28.07.2019)

5. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties [Електронний ресурс]. – Режим доступу: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0441+0+DOC+XML+V0//EN (дата звернення 28.07.2019)

6. Global Digital Report 2018 [Електронний ресурс]. – Режим доступу: https://digitalreport.wearesocial.com/ (дата звернення 28.07.2019)

Joint Framework on countering hybrid threats. A European Union response [Електронний ресурс]. Режим доступу: http://bit.ly/2t0ywSh (дата звернення 28.07.2019).

Надійшла: 15.06.2019 Рецензент: к.т.н., с.н.с. Щебланін Ю.М.