УДК 327.7 (4)
DOI https://doi.org/10.32782/2305-9389/2023.29.27

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Фурсай Олександра,
аспірант
Навчально-наукового інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка
ORCID ID: 0000-0003-1318-4550

Сьогодні особливої ролі набуває інформаційна сфера як поле взаємодії та протистояння суб'єктів міжнародних відносин. Інформація та масові комунікації дедалі більше стають інструментом впливу. Для акторів у міжнародних відносинах стало очевидним, що комунікації можуть бути самостійним засобом для досягнення мети. Інформаційний простір дав розширені можливості взаємодії людям, державним та недержавним установам, комерційним та некомерційним організаціям. У зв'язку із цим гостро постає питання інформаційної безпеки та розроблення й упровадження інструменту, який дасть змогу ефективно підтримувати рівень захисту та безпеки в інформаційному просторі і не тільки.

Наочним прикладом ефективного розвитку інформаційної політики є Європейський Союз. Загальна політика в галузі комунікації та інформації ЄС утілюється через Європейську Комісію, Європейську Раду, Форум інформаційного суспільства ЄС, Генеральний Директорат з інформаційного суспільства, Генеральний Директорат з освіти і культури, а також через інформаційні центри у країнах – членах організації та поза її межами [1].

Слід зазначити, що інформаційна політика Європейського Союзу постійно вдосконалюється. Значна увага приділяється правовим засадам інформаційної безпеки, що передбачає розроблення нормативно-правових актів, активно ведеться робота в напрямі поліпшення законодавства щодо попередження та боротьби з дезінформацією. Держави ЄС спрямовують зусилля на захист інформаційних систем від зовнішнього негативного впливу та створення всіх необхідних умов для належного, безпечного функціонування держави та суспільства. Для України досвід ефективної реалізації політики інформаційної безпеки є особливо важливим, ураховуючи повномасштабне вторгнення Росії, а також як один з інтегруючих факторів України у Європу.

Ключові слова: *інформаційна безпека, кібербезпека, Європейський Союз, Європейська Комісія, НАТО, інформаційний простір, дезінформація, інформаційне суспільство.*

Fursai Oleksandra. Information security policy of the European Union

Today, the information sphere plays a major role as a field of interaction and confrontation between subjects of international relations. Information and mass communications are increasingly becoming a tool of influence. For actors in international relations, it has become obvious that communications can be an independent means to achieve a goal. The information space provided enhanced opportunities for interaction among people, state and non-state institutions, commercial and non-commercial organisations. In this regard, the issue of information security and the development and implementation of a tool that will allow us to effectively maintain the level of protection and security in the information space and behind its limits is an acute problem.

A clear example of the effective development of information policy is the European Union. The general EU communication and information policy is implemented through the European Commission, the European Council, the EU Information Society Forum, the General Directorate for the Information Society, the General Directorate for Education and Culture, as well as through information centres in member countries of the organisation and outside its borders [1]. It should be noted that the information policy of the European Union is constantly being improved. Considerable attention is paid to the legal principles of information security suggesting the development of normative legal acts, EU experts are actively engaged in work aimed at improving legislation on the prevention of disinformation.

The EU states direct all their efforts to protect information systems from external negative influence and create all the necessary conditions for the proper and safe functioning of the state and society. For Ukraine, the experience of effective implementation of the information security policy is particularly important, taking into account the full-scale invasion of Ukraine by Russia, and also as one of the integrating factors of Ukraine into Europe.

Key words: *information security, cyber security, European Union, European Commission, NATO, information space, disinformation, information society.*

Свій початок інформаційна політика ЄС бере з опублікованого у 1994 р. звіту «Європа і глобальне інформаційне суспільство. Рекомендації Європейській Раді», який був підготовлений на замовлення Європейської Ради Мартіном Бангеманом [2, с. 5–22]. У тому ж році Європейська Комісія прийняла ще один не менш важливий програмний документ «Шлях Європи до інформаційного суспільства». Зазначені в документі основні положення передбачали: забезпечення вільного доступу до інформаційних систем, формування національної думки європейської спільноти щодо становлення інформаційного

суспільства, розроблення концепції інформаційної політики ЄС та популяризацію національної ідентичності [3, с. 45–54].

Уже сьогодні Європейський Союз має власний чітко регульований інформаційний простір. Наповнення інформаційного простору ЄС здебільшого складається з контенту національних ЗМІ, які працюють у тому числі у загальноєвропейських масштабах, а також матеріалів у соціальних мережах. Однак окрім регулювання інформаційного простору в рамках єдиної аудіовізуальної політики, Європейський Союз здійснює заходи в інформаційному просторі з метою підтримки безпеки своїх громадян та ліберально-демократичних цінностей. Це стосується як діяльності терористичних організацій, так і третіх країн та внутрішніх суб'єктів.

Найбільший інтерес для дослідження становлять політика кібербезпеки та боротьба з дезінформацією. За останні декілька років саме цей сегмент інформаційної політики ЄС розвивався найбільш інтенсивно, що значною мірою пов'язане з настороженим сприйняттям зовнішньої інформаційної політики Росії та зростанням міжнародної напруженості навколо повномасштабного військового вторгнення Росії в Україну.

На порядку денному ще довго залишалося питання можливого втручання у європейські вибори 2019 р. [4]. Зокрема, до заходів, покликаних захистити вибори, було включено захист персональних даних, прозорість передвиборчих онлайн-кампаній, кібербезпеку, зміцнення європейської співпраці та забезпечення належних санкційних заходів для політичних партій. Ці положення спираються на основні сьогодні регулюючі документи у сфері онлайн-безпеки, що набрали чинності у 2018 р., серед яких – «Загальний регламент про захист персональних даних» та «Звід правил» [5]. Варто зазначити, що Європейська Комісія значною мірою спирається на громадянське суспільство у питаннях контролю за інформаційною сферою, що проявляється в опитуваннях, регулярному інформуванні та підтримці недержавних наглядових центрів.

Для захисту виборів Європейське агентство з кібербезпеки (ENISA) видало керівництво для країн-членів щодо забезпечення належного рівня технічної безпеки [6]. Таку політику спровокували, зокрема, повідомлення про втручання у президентські вибори у США 2016 р. з боку Росії, а також у вибори у Франції у 2017 р. Під «утручанням» Європейська Комісія передбачає низку дій – від злому поштових скриньок та обвалення вебсайтів за допомогою DDoS-атак до втручання в електоральні системи та фінансування політичних сил [7]. ENISA є основним відомством у Європейському Союзі, що займається питаннями кібербезпеки, як у технічній частині, так і в питаннях координації сил та засобів та інформування населення [8]. Воно було засновано Регламентом від 10 березня 2004 р. [9, с. 128–137]. Агентство було створено з метою підвищення здатності ЄС запобігати загрозам інформаційної безпеки та відповідати на випадки нападу в цифровому середовищі. Нині позиціонує себе як центр забезпечення кібербезпеки в усій Європі. Установчий Регламент від 2004 р. було доповнено Регламентом 2013 р. [10]. Відповідно до нього, перед агентством стоять такі цілі:

1) підтримка високого експертного рівня;

2) сприяння органам ЄС у формуванні політики щодо мережевої та інформаційної безпеки;

3) сприяння органам та країнам – членам ЄС у проведенні політики, необхідної для відповідності вимогам до мережевої та інформаційної безпеки в рамках європейського законодавства;

4) сприяння ЄС та країнам-членам у підвищенні здатності та готовності до запобігання, розпізнавання та відповіді на проблеми та інциденти, пов'язані з інформаційною безпекою;

5) широка взаємодія з представниками громадського і приватного секторів.

East StratCom є основною організацією у структурі інститутів Європейського Союзу, що протидіє російській зовнішній інформаційній політиці та взагалі дезінформації як такій. Група згадується у різних документах, зокрема у резолюції щодо протидії пропаганді від третіх сторін [11]. У тій самій резолюції серед основних джерел пропаганди та дезінформації відзначені російські установи та ЗМІ: «Спутник», «Россотрудничество», «Русский мир» та проурядові ЗМІ.

StratCom став організацією, що просуває комунікації Європейського Союзу у країнах Східного партнерства та підтримує незалежні ЗМІ. Східна політика, урегулювання питання військової агресії Росії на території України та фінансова підтримка українських реформ у 2015 р. вже входили до пріоритетних зовнішньополітичних завдань Європейської Комісії. Із цим пов'язаний і початок активної боротьби з російською дезінформацією [12]. Серед основних інструментів – взаємодія з пресою, комунікації у мережі, статті, аудіовізуальні матеріали [13]. StratCom також здійснює моніторинг російських проурядових ЗМІ та видає за необхідності спростування. Підготовлена ними інформація часто цитується. Так, серед тих, хто посилається на них, – ЗМІ, такі як The Guardian, Welt, Zeit, Independent, USA Today та ін. [14].

У березні 2015 р. Європейська Комісія доручила представництву ЄС підготувати план дій зі стратегічних комунікацій. Створення такого документу мало стати першим кроком у боротьбі з російською дезінформацією [15]. План було підготовлено та оприлюднено у червні 2015 р. Він визначив основні напрями діяльності для StratCom:

1. Підвищення потенціалу ЄС у стратегічних комунікаціях.
2. Робота з партнерами та розширення шляхів взаємодії.
3. Комунікаційна діяльність за програмами ЄС, проєкти та діяльність у напрямі країн Східного партнерства.
4. Підтримка свободи ЗМІ та свободи вираження думок.
5. Ініціативи громадської дипломатії.
6. Розвиток потенціалу журналістів та медіааторів.
7. Підтримка плюралізму в російськомовному медіапросторі.
8. Робота з громадянським суспільством.
9. Підвищення обізнаності, розвиток критичного мислення та просування медіаграмотності.
10. Зміцнення взаємодії між країнами-членами щодо законодавчого регулювання медіапростору [16].

У жовтні 2019 р. було підведено проміжні підсумки ефективності відомства. Відповідно до підрахунків, StratCom видав понад 6 500 випадків спростування новин більше ніж на 20 мовах [17].

Наступним кроком в оновленні системи інформаційної безпеки стала підготовка та публікація Європейською Комісією у квітні 2016 р. «Спільного плану попередження гібридних атак» [18]. Як наголошується у документі, ситуація у країнах Східного та Південного партнерства створила нові загрози, у вирішенні яких Європейський Союз має виступити посередником. План спирається на видану ще в 2013 р., до кризи, «Стратегію кібербезпеки», яка визначила такі пріоритети, як підвищення рівня стійкості кіберсфери, усунення кіберзлочинності, розроблення стратегії цифрової безпеки з опорою на загальну безпекову та оборонну політику, поліпшення цифрової інфраструктури, просування європейських цінностей [19]. Сучасні стратегії роблять більший акцент на онлайн-сфері та соціальних мережах. Так, у плані 2016 р. щодо протидії гібридним загрозам у розділі стратегічних комунікацій згадуються таргетовані кампанії, спрямовані на соціальну дестабілізацію [20]. У документі є й інший важливий наратив – створення системи контролю за повідомленнями в мережі. У частині кібербезпеки план рекомендує поглибити співпрацю у роботі груп протидії загрозам комп'ютерної безпеки (Computer security incident response team; CSIRTs), які були створені відповідно до Директиви 2016 р. щодо заходів підвищення рівня мережевої та інформаційної безпеки у ЄС [21]. Відповідно до тієї ж Директиви, було створено «Групу взаємодії з безпеки мережі та інформації», яка була покликана координувати дії в кіберсфері між країнами, у тому числі роботу CSIRTs, сприяти обміну інформацією, яка складається з представників відповідних міністерств [22].

Відповідно до плану, згодом було створено «Центр передових технологій боротьби з гібридними загрозами», який тісно співпрацює з НАТО. Необхідність такої співпраці навіть зазначена у плані окремо.

Загалом, вивчивши документ, можна відзначити два основні напрями діяльності Європейського Союзу у сучасній інформаційній політиці: стратегічні комунікації та боротьба з дезінформацією, з одного боку, з іншого – кібербезпека.

Через два роки, у квітні, було опубліковано «Повідомлення про боротьбу з дезінформацією в Інтернеті» [23]. Документ був підготовлений, базуючись на власних громадських опитуваннях та дослідженнях від Євробарометра. У цьому документі наголошується, що європейське населення зіткнулося з великою кількістю випадків дезінформації. У документі стверджується, що Інтернет стає дедалі важливішим джерелом новин і водночас у ньому зростає кількість дезінформації від внутрішніх та зовнішніх акторів, що суперечить демократичним підвалинам та позбавляє населення можливості робити свідомий вибір. Дезінформація визнається частиною гібридної війни, згадується можливість використання засобів інформаційної війни в російській військовій доктрині, а російські кампанії в інформаційному середовищі розглядаються як основна загроза. Серед інших можливих наслідків дезінформації – зниження довіри до науки та емпіричних доказів.

Одразу після президентських виборів у Франції було прийнято інший значущий документ – «Зведення правил боротьби з дезінформацією» [24]. Це перший випадок, коли представники бізнесу добровільно погодилися ухвалити стандарти саморегуляції для боротьби з дезінформацією. Цей документ був покликаний здійснити завдання, поставлені у повідомленні 2018 р. Серед методів було прийнято забезпечення прозорості рекламних політичних кампаній, закриття фейкових облікових записів, а також демонетизація для розповсюджувачів дезінформації. До ініціативи приєдналися Facebook, Google,

Twitter, Mozilla та інші платформи. Згодом учасники подавали Європейській Комісії звіти з виявлених випадків дезінформації та заблокованих акаунтів.

На виконання положень «Повідомлення 2018 року» за сприяння Європейської Комісії було створено Наглядовий центр за соціальними мережами (SOMA), який є платформою для спостереження за ЗМІ та виявлення дезінформації на допомогу Європейській Комісії. Учасником може стати будь-яка людина чи організація у ЄС, залучені до перевірки фактів на достовірність. Платформа надає різні технологічні інструменти та можливість обмінюватися даними з випадків дезінформації. Організація ставить перед собою завдання моніторингу, освіти, експертних рекомендацій, оцінки результатів та координації зусиль [25].

Наступний крок, який зробила Європейська Комісія, став найважливішим із погляду стратегії боротьби з дезінформацією. Цим кроком стало ухвалення «Плану дій проти дезінформації» у грудні 2018 р. [26]. План визначає дезінформацію як достовірно неправдиву чи спотворену інформацію, що створюється і поширюється з метою економічної вигоди чи навмисного введення в оману громадськості, здатну завдати шкоди суспільству. До загрозливих об'єктів включено, насамперед, демократичні процеси. План знову відзначає як пріоритет у забезпеченні безпеки боротьбу з гібридними загрозами, частиною якої є стратегічні комунікації. У цьому ж пункті з питання гібридної загрози є посилання на хімічну атаку в Солсбері, що дає підстави стверджувати про багаторівневу безпекову політику проти російської загрози, ураховуючи й те, що «План дій проти дезінформації» робить акцент на роботі StratCom і Європейської служби зовнішньої дії у східному напрямку. У контексті гібридної війни дезінформаційні кампанії пов'язані з кібератаками та зломом комп'ютерних мереж.

У «Плані дій проти дезінформації» зазначається, що вперше загроза дезінформації з російського боку в онлайн-середовищі виникла у 2015 р. Європейська Комісія визнає також, що хоча кампанії дезінформації проводять понад тридцять країн, Росія лідирує у цьому напрямі, дозволяючи всім іншим переймати успішний досвід.

Згідно з «Планом дій проти дезінформації», країни-члени та інститути ЄС мають бути залучені до роботи на різних рівнях: боротьба з гібридними загрозами, кіберзагрозами, здійснення розвідки та стратегічних комунікацій, захист даних, безпека виборів та робота зі ЗМІ. Загалом запропоновані Планом дії ґрунтуються на чотирьох опорах: підвищення здатності Європейського Союзу у виявленні та спростуванні дезінформації; зміцнення можливості спільного реагування на небезпеки; мобілізація приватного сектору; інформування громадян та підвищення стійкості населення до загроз. План передбачає проведення всіх необхідних заходів перед травневими виборами 2019 р.

У лютому 2019 р. Рада Європейського Союзу опублікувала рішення, де наголосила на важливості запобігання кіберзагрозам для забезпечення чесних та прозорих виборів [27]. Серед іншого, документ звертає увагу на важливість проведення перед виборами тижня медіаграмотності. G7 і NATO були визначені організаціями-партнерами. У червні 2019 р., уже після виборів, було опубліковано звіт щодо здійснення Плану дій [28]. Документ став підсумковим для всього процесу розбудови системи стратегічних комунікацій та боротьби з дезінформацією в умовах європейських виборів. У ньому наголошується, що вжиті перед європейськими виборами дії у боротьбі з дезінформацією виявилися успішними. Із січня до червня StratCom виявив та спростував 1 000 випадків дезінформації, що понад удвічі більше порівняно з аналогічним періодом попереднього року. Бюджет, виділений Європейській службі зовнішньої дії на стратегічні комунікації, збільшили вдвічі, а штат розширюється. Хоча StratCom не виявив закордонних дезінформаційних кампаній, націлених на європейські вибори, у звіті вказується на дезінформаційну активність із боку Росії.

У звіті згадується створена у березні 2019 р. «Система швидкого реагування». Вона покликана забезпечити оперативну взаємодію з G7, НАТО та онлайн-платформами з випадків дезінформації. На даний момент вона використовується для виявлення неправдивих відомостей на тему коронавірусу, поширених в Інтернеті, серед яких – неправильні способи лікування, які можуть спричинити важкі наслідки для здоров'я [29].

Особлива увага надається боротьбі з дезінформацією та поширенням фейкових матеріалів, ціллю яких є дискредитація європейських інституцій та загалом стратегій Європейського Союзу та його держав-членів щодо протидії COVID-19. Зокрема, за оцінкою Європейської служби зовнішніх справ, такі міжнародні актори, як Росія та Китай, використовують для такої шкідливої діяльності державні ЗМІ й соціальні мережі, такі як Twitter, Facebook та ін. Слід зазначити, що результатом таких дій є не тільки інформаційна дезорієнтація громадян держав – членів ЄС, а й створення глобального образу колективного Заходу (зокрема, тандему ЄС – НАТО) як «розділеного» та «хаотичного». Тобто боротьба ЄС у цьому напрямі є

не тільки частиною комплексної роботи з підтримки інформаційної гігієни в європейському інформаційному просторі, а й зосереджена на захисті західних ліберально-демократичних цінностей та стратегічної привабливості Європейського Союзу як успішної моделі колективної співпраці [30].

Згідно зі звітом, Google вжив заходи щодо більше ніж 130 тис європейських облікових записів, які порушили правила розміщення реклами. Facebook повідомив про 1,2 млн випадків порушення правил розміщення реклами та контенту і заблокував 2,2 млрд фейкових акаунтів, а також перешкоджав роботі півтори тисячі неєвропейських та 658 європейських сторінок, груп та акаунтів, націлених на європейських громадян, та вжив заходів щодо підвищення прозорості рекламних кампаній. Twitter відхилив понад 16 тис рекламних оголошень, націлених на громадян Європейського Союзу.

Серед інших організацій, яким Європейський Союз надає підтримку у боротьбі з дезінформацією, – SOMA та Міжнародна мережа перевірки фактів (International Fact-Checking Network), яка нещодавно запустила європейське відділення.

Європейському Союзу вдалося побудувати великий та доволі потужний апарат інформаційної діяльності. Деякі документи останніх років навіть мають стратегічне значення: «План дій проти дезінформації», «Зведення правил боротьби з дезінформацією», «План боротьби з гібридними загрозами». Було створено нові установи міжурядового та неурядового характеру, здатні проводити заходи щодо інформаційного захисту саме за змістовною частиною: SOMA, Центр передових технологій боротьби з гібридними загрозами та ін. StratCom удалося виявити величезну кількість фактів дезінформації. Європейський Союз досяг головної мети – створив систему захисту європейських громадян та демократії від дезінформації. Інформаційна політика ЄС є позитивним чинником для зміцнення своїх позицій у світі, оскільки Європа підтримує дотримання миру, свобод, права націй на самовизначення, реалізацію спільної зовнішньої безпекової політики та формування єдиної системи європейського інформаційного простору.

Література:

1. Балицька Ю.А. Формування нової стратегії публічності в інформаційній діяльності ЄС. URL: http://en.chnu.edu.ua/wp- content/uploads/2018/03/Balytska.pdf.
2. Bruggemann M. Information policy and the public sphere: EU communications and the promises of dialogue and transparency. *Javnost – The Public, Journal of the European Institute for Communication and Culture*. 2010. Vol. 17. № 1. P. 5–22.
3. Бєлоусова Н.Б. Особливості реалізації стратегії інформаційного суспільства в Європейському Союзі. *Проблеми міжнародних відносин*. Вип. 6. С. 45–54.
4. European Commission. 10 ways the EU is fighting disinformation. European Commission. Medium. 2019. URL: https://europeancommission.medium.com/10-ways-the-eu-is-fighting-disinformation-f07fca60e918.
5. State of the Union 2018: European Commission proposes measures for securing free and fair European elections. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681.
6. Compendium on Cyber Security of Election Technology. European Union. 2018. URL: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf.
7. European Cyber Security Journal. The Kosciuzko Institute. 2017. URL: https://cybersecforum.eu/wp-content/uploads/2021/06/ECJ-VOLUME-3-2017-ISSUE-3.pdf.
8. About ENISA – The European Union Agency for Cybersecurity. European Union Agency. URL: https://www.enisa.europa.eu/about-enisa.
9. Evaluation of the EU decentralised agencies in 2009. Evaluation for the European Commission. 2009. URL: https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/evaluation_eu_agencies_vol_iii_/evaluation_eu_agencies_vol_iii_en.pdf.
10. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance. EUR-Lex, Access to European Union Law. 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0526.
11. EU strategic communication to counteract anti-EU propaganda by third parties. European Parliament. 2016. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html.
12. European Council meeting (19 and 20 March 2015) – Conclusions. European Council. 2015. URL: https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf.
13. STRATEGIC COMMUNICATIONS. The Diplomatic Service of the European Union. URL: https://www.eeas.europa.eu/taxonomy/term/400164_en.
14. About EUvsDisinfo. EUvsDisinfo. https://euvsdisinfo.eu/.
15. European Council meeting (19 and 20 March 2015) – Conclusions. European Council. 2015. URL: https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf.
16. ACTION PLAN ON STRATEGIC COMMUNICATION. URL: https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf.
17. EUvsDisinfo: how to debunk over 6,500 disinformation cases in four years? The Diplomatic Service of the European Union. 2019. URL: https://www.eeas.europa.eu/eeas/euvsdisinfo-how-debunk-over-6500-disinformation-cases-four-years_en.

18. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response. EUR-Lex, Acces to European Union Law. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.
19. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. EUR-Lex, Access to European Union Law. 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001.
20. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response. EUR-Lex, Acces to European Union Law. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.
21. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Office Journal of the European Union. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.
22. NIS Cooperation Group. European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.
23. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling online disinformation: a European Approach. EUR-Lex, Access to European Union Law. 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236.
24. The 2022 Code of Practice on Disinformation. European Commission. 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.
25. WHO LEADS THIS EFFORT? SOMA. URL: https://www.disinfobservatory.org/about-us/.
26. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Report on the implementation of the Action Plan Against Disinformation. EUR-Lex, Access to European Union Law. 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=comnat:JOIN_2019_0012_FIN.
27. Securing free and fair European elections: Council adopts conclusions. European Council. 2019. URL: https://www.consilium.europa.eu/en/press/press-releases/2019/02/19/securing-free-and-fair-european-elections-council-adopts-conclusions/.
28. Report on the implementation of the Action Plan Against Disinformation. European Commission. 2019. URL: https://www.eeas.europa.eu/sites/default/files/joint_report_on_disinformation.pdf.
29. EU Rapid Alert System used amid coronavirus disinformation campaign. EURACTIV. 2020. URL: https://www.euractiv.com/section/media/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/.
30. Danylenko S., Fursai O. «Vaccinodemic» as a component of the global hybrid conflict between democracy and autocracy: the case of Ukraine. Rocznik Instytutu Europy Środkowo-Wschodniej. 2022. URL: https://ies.lublin.pl/wp-content/uploads/2022/11/riesw_2022-02-02.pdf.