УДК 323(450):001.92
Єлизавета Радзивилюк,
студентка факультету міжнародних відносин,
спеціальність «Консолідована інформація»,
Східноєвропейський національний університет
liza20009@gmail.com
https://doi.org/10.29038/2524-2679-2020-01-112-122

ОСОБЛИВОСТІ УБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ ІТАЛІЇ В КОНТЕКСТІ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ ТЕХНОЛОГІЙ

У статті досліджено особливості убезпечення інформаційного простору Італії в контексті розвитку інформаційно-комунікативних технологій. У роботі наведено нове розв'язання актуальної наукової проблеми, що полягає в розробленні концептуальних та правових засад забезпечення інформаційної безпеки, а також практичних рекомендацій щодо вдосконалення механізмів її забезпечення.

Отримані в процесі дослідження результати дають підстави стверджувати, що реалізація національних інтересів в інформаційній сфері буде дієвою в разі законодавчого визначення національних цінностей і зумовлених ними національних інтересів. Виходячи з розробленої моделі взаємодії національних цінностей, інтересів цілей та надбань в інформаційній сфері, ми запропонували основними критеріями оцінки негативного впливу на інформаційну безпеку держави вважати деструктивні трансформації національних цінностей в інформаційній сфері, які можливо встановлювати шляхом соціологічних опитувань і вивчення громадської думки. Такі критерії доцільно акумулювати в методологічній базі й на її підставі моніторити стан і динаміку вітчизняної інформаційної сфери, виявляти найбільш вразливі сфери.

Запропоновано та обґрунтовано включити до об'єктів забезпечення інформаційної безпеки національні інтереси, цінності, цілі й надбання в інформаційній сфері; розроблено критерії оцінки негативного впливу загроз на стан інформаційної безпеки, якими запропоновано вважати деструктивні трансформації національних цінностей в інформаційній сфері, що дає змогу створити правове підґрунтя відповідної методологічної бази; виділено у вітчизняній системі інформаційного права нову складову частину – забезпечення інформаційної безпеки, а також проаналізовано причини й передумови її виникнення; у системі інформаційно-психологічного складника інформаційної безпеки виокремлено такі елементи, як духовна, воєнна, соціальна, економічна, екологічна та глобальна безпека й змістовно схарактеризовано взаємозв'язки між ними, що дало змогу врахувати сучасні загрози та розробити пріоритетні напрями державної політики забезпечення інформаційної безпеки.

Ключові слова: *інформаційна безпека; держава; Італія; Україна; медіа-простір; інформаційна війна; маніпуляція; свідомість.*

1. ВСТУП

Постановка проблеми. Італія відіграє вагому роль у процесах європейської інтеграції з огляду на заявлену пріоритетну соціальну спрямованість інформаційної політики. Політика уряду Італійської Республіки має на меті впровадження електронної демократії, ефективну лібералізацію

телекомунікацій, створення необхідних умов для розвитку електронної торгівлі, забезпечення загального й рівного доступу до інформаційних ресурсів, упровадження електронної освіти на загальнонаціональному рівні (особливо під час розв'язання проблеми «цифрового розриву» між Півднем та Північчю Італії). Європейський Союз як політична, економічна, соціальна структура намагається поглибити й консолідувати політику інтеграційного співробітництва за допомогою оптимізації спільної зовнішньої політики та політики безпеки, а також координації інформаційного законодавства та інформаційної політики держав-членів, зокрема підкреслено, що Італія виробила свої власні механізми прийняття й упровадження політичних рішень та визначила ієрархію інститутів й обов‟язки органів влади стосовно взаємодії з Євросоюзом щодо формування інформаційного суспільства.

Аналіз останніх досліджень і публікацій. Дослідження інформаційної безпеки Італії з правничого погляду пов‟язане з формуванням якісної системи інформаційної безпеки, що відповідатиме сучасним вимогам і нагальним потребам Італії як повноправного члена й надійного партнера європейської спільноти. Цю проблематику досліджували Ю. Бабенко, О. Барабанов, М. Дмитренко, Н. Карпова, А. Манойло, Е. Маслова та ін. Проблема захисту від нових видів небезпек і загроз, породжених інформатизацією, що проявилися в третьому тисячолітті, турбує дослідників сучасного суспільства. Кількості робіт стосовно проблем інформаційної безпеки стає дедалі більше. Водночас аналіз наукової літератури доводить, що методологічні аспекти вивчення інформаційної безпеки вимагають подальшого опрацювання.

Мета дослідження – проаналізувати особливості убезпечення інформаційного простору Італії в контексті розвитку інформаційно-комунікативних технологій.

Методика дослідження. У ході дослідження використано такі методи дослідження, як порівняння, класифікація, теоретичне моделювання, з‟ясування причинно-наслідкових зв‟язків, систематизація, абстрагування та конкретизація, аналіз документації й результатів діяльності дослідників із проблеми проведеного дослідження.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Державний інформаційний простір – надзвичайно важливе політичне поняття, яке у вартісній шкалі соціальних цінностей можна поставити на друге місце після державної незалежності. Країна зобов‟язана забезпечити використання свого інформаційного поля в інтересах саме держави та її громадян. Якщо вона цього не зробить, то цей інформаційний простір буде використано проти неї самої. Основним принципом безпеки інформації є те, що інформація повинна зберігати свій ступінь захисту при всіх її передачах, починаючи з джерела, а контроль за розподілом і поширенням інформації повинен забезпечити відсутність її витоку, а також і те, що правила доступу до інформації повинні дозволяти використання інформації лише особам, яким

вона потрібна для виконання службових обов‟язків. Присвоєння інформації того або іншого грифа таємності виробляється відповідно до правил систем безпеки країн-учасниць.

У зв‟язку з цим НАТО виокремлює такі цілі й вимоги для всіх країн, зацікавлених у збереженні цілісності, непорушності та конфіденційності їхнього державного інформаційного простору. Інформаційна структура повинна постійно вдосконалюватися, темпи розвитку нових інформаційних технологій та їх поширення повинні прискорюватися. Важливими є розвиток систем електронної сертифікації та криптографії, належна підготовка персоналу. Формування й реалізація єдиної державної політики в контексті забезпечення безпеки національних інтересів від загроз в інформаційній сфері має стати одним із пріоритетних напрямів розвитку держави. Розвиток індустрії інформаційних та телекомунікаційних засобів, їх поширення на внутрішньому медіа-ринку держави, модернізація систем теле- й радіомовлення, оновлення технічної бази для забезпечення захисту інформації в цій сфері є також важливими заходами на шляху до формування державної інформаційної безпеки. Якщо до цього буде приєднана ефектна протидія інформаційній експансії та спробам використання національного інформаційного простору, можна буде сказати, що держава обрала правильний шлях боротьби з кіберзлочинністю. На сьогодні Європейський Союз як політична, економічна, соціальна структура намагається поглибити й консолідувати політику інтеграційного співробітництва через оптимізацію спільної зовнішньої політики та політики безпеки, а також через координацію інформаційного законодавства й інформаційної політики держав-членів, зокрема підкреслено, що Італія виробила власні механізми прийняття та впровадження політичних рішень і визначила ієрархію інститутів та обов‟язки органів влади стосовно взаємодії з Євросоюзом щодо формування інформаційного суспільства.

У зв‟язку зі збільшенням кількості скандалів щодо зміни результатів виборів та референдумів третіми країнами, Італія, як і решта членів Європейського Союзу, намагається усунути від себе проблему втручання третіх країн у вибори на різних рівнях. Вибори в Італії до сенату 2018 р. відбулися за неприємних інцидентів, пов‟язаних із втручанням у діяльність інформаційних засобів, які належать урядовим органам держав ЄС та крадіжку цінної інформації й персональних даних. У січні в мережі Facebook з‟явилась інформація про те, що окремий портал цієї мережі сприятиме об‟єктивному висвітленню виборів 2018 р. до сенату Італії та протидії фейковим новинам, а також зменшенню рівня втручання іноземних країн до італійських виборів. Фейкові новини, зокрема ті, що направлені на маніпулювання настроями виборців (на зміну настроїв, активність/пасивність виборців, підтримку), формуючись на основі дезінформації соціальних медіа й стрічки міжнародних новин, сприяють непрозорій політичній кампанії та завдають шкоду тій державі, проти якої були задіяні, на користь країни, яка створює, фінансує, підтримує таку компанію.

В Італії найбільш неоднозначні партії: «Рух 5 зірок» та «Ліга Півночі» зустрічаються відкрито й неофіційно з представниками інших країн, також

представники цих партій активно діють у соціальних мережах, поширюючи популістські заклики. Перша була створена нещодавно (2009 р.), але дуже швидко набула популярності та підтримки серед населення. Вибори в Італії у 2018 р. відбулися й наразі немає повідомлень про викрадення або псування електронної інформації, пов‟язаної з результатами виборів, хоча деякі видання наголошують на тому, що атака на державні установи не припинялася. Результати виборів підтвердили, що вплив соціальних медіа та засобів масової інформації в Інтернеті суттєво зріс і продовжує бути одним із найголовніших факторів, який може вплинути на незалежні результати виборів [8].

Розрив між індустріально розвиненою Північчю й аграрним Півднем є значно більшим, ніж у Бельгії. До того ж ситуація в південних регіонах обтяжена діяльністю мафії. Ліга Півночі (Lega Nord), що виступила з гаслами федералізації країни та перегляду розподілу доходів на користь промислово розвиненої Півночі і його подальшого дистанціювання від слабшого Півдня, отримала на виборах 1992 р. 8,6 %, а в 1996 р. вже 10,1 % голосів. На виборах до Європарламенту 2009 р. Ліга Півночі отримала 10,2 % голосів виборців [6]. Найрадикальніші представники Ліги Півночі обґрунтовують необхідність створення незалежної держави Паданія зі столицею в Мілані. В останні роки Ліга Півночі позиціонує себе як консервативна політична сила. Для привернення уваги до своє діяльності партія створила збірну Паданії з футболу, яка проводить матчі переважно з командами інших невизнаних держав і регіонів. В Італії з 1991 р. діє партія «Північна ліга» (або «Ліга Півдня»), яка виступає за посилення автономії північної частини Італії. У прибічників Ліги склалася національна ідеологія, у рамках якої вони відмовляються від спорідненості з іншими італійцями, а їх походження ведеться від цизальпинських галів.

Під час вироблення основних положень інформаційної політики уряд Республіки Італія визначив пріоритетами трансформацію органів державного урядування на основі ІКТ, вільний доступ он-лайн для громадян і підприємців, реалізацію програми комп‟ютеризації та електронної освіти для державних службовців, прозорість державного документообігу за допомогою Інтернету, забезпечення якості інформаційних продуктів і послуг. Виконання поставлених цілей контролюється Національним центром із питань інформатики при Державній адміністрації (Centro Nazionale per I‟Informatica nella PA, CNIPA). Питанням інформаційного суспільства в Республіці Італія займається Комітет з інформаційного суспільства, який створено 2001 р., і Міністерство з інновацій та технологій. Головна роль комітету полягає в координації дій між усіма адміністраціями, розробці спеціальних проектів і планах дій у сфері новітніх технологій, підтриманні зв‟язку з громадянами, у розвитку економічної, культурної та соціальної сфер держави.

Основні документи Італії у сфері інформаційного суспільства, такі як План дій із питань побудови інформаційного суспільства, План дій із питань побудови електронного уряду, Адміністративний цифровий кодекс та ін. доводять, що урядова політика у сфері інформації й комунікації спрямована на

подолання цифрової нерівності між Північчю та Півднем Італії, а також на оптимізацію інформаційної індустрії й упровадження моделі інформаційного суспільства, яка ґрунтується на інноваціях технологій і знань. Урядові стратегії висвітлюють такі основні цілі інформаційної політики, як моніторинг сфери онлайн-послуг, підвищення внутрішньомережевої якості, оцінювання інтелектуальних ресурсів, упровадження електронного урядування на базі програми «Електронний уряд для ефективного федералізму: одне бачення – спільна реалізація», розвиток культури електронної комунікації в співробітництві Державної адміністрації з громадянами та безпосередньо в діяльності регіональних і місцевих органів управління. На сьогодні цифрова реформа виконується завдяки повному поділу локальної мережі, поширенню близько 50 % усієї інформації он-лайн, підвищенню рівня розвитку ІКТ, упровадженню системи сертифікованої електронної пошти. Одним із головних документів національної інформаційної політики Італії є Національний план дій щодо наукових розробок, загального розвитку та зайнятості (2005 р.), в основу якого покладено принципи розвитку й постійного зростання послуг ІКТ, зміцнення інтелектуального капіталу нації, адаптація матеріальної й нематеріальної інфраструктур [4, с. 364–365].

Основним принципом безпеки інформації є те, що інформація повинна зберігати свій ступінь захисту при всіх її передачах, починаючи з джерела, а контроль за розподілом і поширенням інформації повинен забезпечити відсутність її витоку, а також те, що правила доступу до інформації повинні дозволяти використання інформації лише особам, котрим вона потрібна для виконання службових обов‟язків. Присвоєння інформації того або іншого грифа таємності здійснюється відповідно до правил систем безпеки країн-учасниць. У зв‟язку з цим НАТО виокремлює такі цілі й вимоги для всіх країн, зацікавлених у збереженні цілісності, непорушності та конфіденційності їхнього державного інформаційного простору. Інформаційна структура повинна постійно вдосконалюватися, темпи розвитку нових інформаційних технологій та їх поширення мають прискорюватися. Важливими є розвиток систем електронної сертифікації й криптографії, належна підготовка персоналу. Формування та реалізація єдиної державної політики в контексті забезпечення безпеки національних інтересів від загроз в інформаційній сфері має стати одним із пріоритетних напрямів розвитку держави. Розвиток індустрії інформаційних і телекомунікаційних засобів, поширення їх на внутрішньому медіа-ринку держави, модернізація систем теле- та радіомовлення, оновлення технічної бази для забезпечення захисту інформації в цій сфері є важливими заходами на шляху до формування державної інформаційної безпеки. Якщо до цього буде приєднана також ефектна протидія інформаційній експансії й спробам використання національного інформаційного простору, то можна буде сказати, що держава обрала правильний шлях боротьби з кіберзлочинністю.

Для забезпечення участі європейських урядів, громадян і підприємств в інформаційному суспільстві ЄС послідовно працює над розвитком інформаційних і телекомунікаційних технологій. Після виходу білої книги

«Зростання, конкурентоспроможність і зайнятість» у 1993 р. сформовано єдину стратегію інформаційного суспільства, яка вже наступного року була закріплена в плані заходів «Шлях Європи до інформаційного суспільства» [5]. 1999 р. інформаційне суспільство стало реальністю, але залишилася необхідність подальшої координації між учасниками. Це враховано в декларації «Eeurope – інформаційне суспільство для всіх» [7], а 2000 р. розроблено й ухвалено відповідний план заходів «Eeurope». Цей документ сконцентровано на виконанні трьох основних завдань – забезпечення дешевого, швидкого й безпечного доступу до Інтернету; інвестиції в трудові ресурси та їх кваліфікацію; заохочення до користування Інтернетом. План заходів «Eeurope» ґрунтується на низці найважливіших концепцій, програм і дій, що стосуються таких сфер, як eresearch, e-security, e-working, e-accessibility, e-commerce, e-government, elearning, e-health, e-transport, e-content. E-government – основний напрям роботи майбутніх європейських концепцій у регіональному масштабі. Як констатується в документі BISER (Benchmarking for Information Society: Europe Indicators for European Regions), основними рушійними силами для проникнення інформаційного суспільства у сферу держави й публічної адміністрації є e-government (в установах G2C, G2B, уключаючи інтерактивну комунікацію з громадськістю), мережі/комунікації всередині й між адміністраціями, розміщення замовлень у режимі он-лайн і менеджмент знань. Головною метою європейської політики в документі визначено створення Інтернет-порталів державних установ, запровадження інтерактивних комунікацій, послуг на основі транзакцій, нових інформаційних послуг, а також зниження рівня бюрократизму.

Формування інформаційного суспільства є закономірним етапом еволюції сучасного соціуму, що характеризується, насамперед, масштабним упровадженням інформаційних технологій і розвитком глобального інформаційного простору. Процес становлення нового суспільства, зумовлений упровадженням інформаційних технологій, вимагає правильного усвідомлення його інформаційної специфіки й конструктивного розвитку закладеного в ньому потенціалу.

Відповідно, життєдіяльність інформаційного суспільства потребує чіткого законодавчого врегулювання багатоманітних відносин, що виникають у зв‟язку зі створенням, функціонуванням, використанням інформаційних систем і ресурсів, каналів комунікацій, відповідних технологій тощо. Досліджене раніше формування в системі інформаційного права такої підгалузі, як правове забезпечення інформаційної безпеки, зумовлює потребу виокремлення законодавчих актів, положень, норм, котрі регламентують різні аспекти забезпечення інформаційної безпеки, їх аналізу на предмет наявності системних вад, а також систематизації, консолідації на цій основі загальних правових норм у єдиний базовий закон, позбавлений відомих на сьогодні суперечностей, колізій і прогалин. Це, зі свого боку, має створити передумови для якісної комплексної трансформації законодавства, яке регулює інформаційні відносини в різних сферах життєдіяльності суспільства. Отже, транспарентність органів

державного управління потрібно розглядати як багатогранну характеристику ефективного функціонування влади, що ґрунтується на трьох головних елементах: відкритості, прозорості й доступності, котрі у взаємозв‟язку визначають інтегративний зміст досліджуваного поняття.

Особливістю оптимізації інформаційного простору є так звана медіатизація – посилення інформаційного супроводу всіх інших мілітарних і немілітарних способів ведення війни. При цьому дії в інформаційній сфері та кіберпросторі не повинні розглядатися як окремі, відірвані від інших форм агресії, вони є додатковим супроводжувальним елементом. Це чітко можна простежити в т. зв. доктрині Герасимова, керівника Генштабу Росії, який описує нові конфлікти та відповідну тактику їх ведення. Італія перебувала під посиленим інформаційним впливом із боку Росії задовго до початку відкритої агресії в Україні 2014 р. Можна відзначити активізацію інформаційно-психологічної роботи 2008–2009 рр. (після операції Росії з окупації грузинських територій). За словами директора Національного інституту стратегічних досліджень В. Горбуліна, це була нещадна до українців експлуатація можливостей відкритого інформаційного простору [3]. У підготовчий до агресії період основна інформаційна робота з боку Росії фокусувалася на східних індустріальних районах України й Криму, але також досягала окремих цільових груп в інших частинах – державних службовців, інтелектуальних і культурних середовищ, людей похилого віку. Утім, така активність РФ не викликала захисної реакції з боку органів влади та правоохоронних органів і не сприймалася як складова частина інформаційно-психологічної операції.

Окрім відкритості, яку нині можна вважати ознакою вразливості, активній інформаційній агресії сприяли хронічні проблеми з формуванням українського медіа-ландшафту. Наприклад, негативно позначилася залежність національного інформаційного простору від іноземних медіа-корпорацій переважно російського походження. Це особливо проявилося в запрошенні російського топ-менеджменту на телеканали, засиллі російських телепродуктів у кабельних мережах.

Державні медіа перебували під відвертою цензурою з боку центральної та місцевої влади. Відбувалась інформаційна регіоналізація, за якої через регіональні або російські медіа населення окремих регіонів отримувало спотворений образ суспільно-політичної ситуації в Україні [1]. Це давало змогу легко маніпулювати населенням, коли була потрібна мобілізація електорату на загальнонаціональних виборах, а також сприяло посиленню російського інформаційного впливу, у якому порушувалися питання національної ідентичності, етнонаціональної й мовної політики, міжконфесійних відносин, внутрішньо- та зовнішньополітичних відмінностей. Саме інформаційна регіоналізація сприяла успішній окупації Росією Криму й ОРДЛО, де десятиліттями створювався сприятливий ґрунт для формування розмитої ідентичності громадян України. Така ситуація також підживлювалася провідною роллю олігархічних груп і російських медіа, які замінили державу в системі комунікацій на центральному та регіональному рівнях. Велика популярність серед українських користувачів російських соціальних мереж

«Одноклассники» й «ВКонтакте» давала змогу використовувати ці інструменти для розробки та впровадження спеціальних інформаційних акцій.

У цілому особливістю інформаційно-психологічних операцій під час ведення гібридної війни є використання сфер життєдіяльності держави й суспільних відносин, які у звичайній мирній обстановці не співвідносяться з інформаційними загрозами. Слабкість української політики в інформаційній сфері зробила нашу державу ще більш уразливою на момент російської агресії. Національне законодавство, що регулювало на той час інформаційно-безпекові питання, ґрунтувалося на неефективних і декларативних принципах, які не давали змоги побудувати дієву систему інформаційної безпеки. Використання кіберпростору як виміру асиметричної агресії є явищем порівняно новим і менш опрацьованим із погляду розуміння рівня загроз та можливої протидії. Як відзначає Д. Дубов, начальник відділу інформаційної безпеки й розвитку інформаційного суспільства Національного інституту стратегічних досліджень, дискусія щодо сприйняття природи кібератак і відповідей на них почалася у 2010–2011 рр. У 2011 р. прийнято документ «Талліннське керівництво із застосування міжнародного законодавства в кіберсфері», а у 2012 р. НАТО визнало кіберпростір новим театром воєнних дій. Однак у практичній площині реагування є досить проблематичним, оскільки важко довести причетність конкретних країни чи груп до здійснення атак [2].

Відповідно, державна система безпеки в умовах гібридної війни потребує застосування негайних загальнонаціональних заходів для підвищення здатності України гарантувати безпеку суспільства, першочерговими з-поміж яких є вжиття дієвих заходів із викорінення агентури з державної системи; схвалення окремим документом (стратегією) комплексу заходів із протидії гібридним загрозам за зразком Спільного рамкового документа ЄС із протидії гібридним загрозам; розвиток державно-приватного партнерства в сприянні розгортанню повноцінного мовлення на окупованій території; посилення контррозвідувальних спроможностей держави й проведення активних заходів; нейтралізація діяльності італійських представництв за кордоном та проведення роботи з недопущення їх появи; протидія італійському впливу на українське суспільство через релігійні організації; ліквідація наявних і нейтралізація нових спроб установлення прихованих контурів зовнішнього управління секторами безпеки, економіки, медіа з боку агресора. Протягом багатьох років у рамках допомоги Італії підтримувала проросійські організації й політичні рухи, які зіграли одну з провідних ролей під час окупації Криму та вторгнення на Донбас. Використовувалася системна пропаганда. Та й сьогодні жителям тимчасово окупованих територій подається викривлена інформація про «загострення кризи в Україні». Нині італійські засоби комунікації широко інтегровані у світові, використовують множинні можливості впливу на інформаційний простір через соціальні мережі, створюють проксі-вплив у різних країнах, зокрема й через підтримку різних організацій, які потім ретранслюють потрібні Росії меседжі. Виправлення ситуації доцільно здійснювати на основі аналізу прогалин у системі з гарантування безпеки суспільства, зокрема й аналізу, виконаного в цій публікації, та з урахуванням

досвіду окремих країн ЄС і Східного партнерства, напрацьованого ними в протистоянні російським гібридним загрозам.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, інформаційне сьогодення війни стало основою пропаганди та маніпулювання свідомістю задля досягнення певного статусу на політичних аренах. Інформаційно-психологічні операції спрямовуються на населення тієї чи іншої країни для того, щоб змінити розуміння або поведінку, ставлення людей до тієї чи іншої події. Основними цілями таких війн є формування правових поглядів і переконань та навіть ідеологій, спроможних направити їхню енергію й сили на виконання певних завдань.

Відтак політика уряду Італійської Республіки має на меті впровадження електронної демократії, ефективну лібералізацію телекомунікацій, створення необхідних умов для розвитку електронної торгівлі, забезпечення загального й рівного доступу до інформаційних ресурсів, упровадження електронної освіти на загальнонаціональному рівні (особливо під час розв‟язання проблеми «цифрового розриву» між Півднем і Північчю Італії). Дезінформація не є ані винятковим для Італії феноменом, ані пов‟язаним суто із Росією в самій Італії, радше – навпаки. В італійській мові навіть існує спеціальний термін на позначення фейків – «bufale». На тлі того, що в Італії про Україну відомо критично мало, а проросійське бізнес-лобі поширює переконливі для італійського вуха твердження на кшталт шкоди санкцій для італійської економіки, викривлена інформація про Україну в італійських ЗМІ є нормою. Під час вироблення основних положень інформаційної політики уряд Республіки Італія визначив пріоритетами трансформацію органів державного урядування на основі ІКТ, вільний доступ он-лайн для громадян і підприємців, реалізацію програми комп‟ютеризації та електронної освіти для державних службовців, прозорість державного документообігу за допомогою Інтернету, забезпечення якості інформаційних продуктів і послуг. Досягнення поставлених цілей контролюється Національним центром із питань інформатики при Державній адміністрації (Centro Nazionale per I‟Informatica nella PA, CNIPA).

У подальших дослідженнях доцільно розглядати процес забезпечення інформаційної безпеки як цілісну систему регулювання суспільних відносин, що виникають у процесі протидії загрозам національній безпеці в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Negri, G. Facebook to monitor Italian election as EU debates Russian fake news. *The European Security Journal.* <https: // www. esjnews. com / facebook-italy-russia-fake-news> (2018, березень, 29).

2. *Сепаратизм по-итальянски.* URL: http://www.germaniaplus.de/2009 /09/separatizm-po-italyanski/

3. *Європейські комунікації:* монографія/Макаренко Є. А., Ожеван М. А., Рижков М. М. [та ін.]. Київ: Центр вільної преси, 2008, 536 с.

4. *Програма «Шлях Європи до Інформаційного Суспільства. План Дій»* (Europe‟s Way to the Information Society. An Action Plan)» URL: http: // i. lekciya. com. ua / doc / 3177 / index. html? page=17; Europe‟s Way to the Information Society. An Action Plan: URL: https: // publications. europa. eu / en / publication-detail/-/publication / deed9eb9–0b6e – 11e4-a7d0–01aa75ed71a1 / language-en (дата звернення: 08.12.2018).

5. *eEurope – An information society for all.* URL: https: // ec. europa. eu / digital- single-market / en / news / eeurope-information-societyall (дата звернення: 08.12.2018).

6. Горбулін, В. Україна стала ключовою державою протистояння Заходу і Росії. *Укрінформ.* URL: https: // www. ukrinform. ua / rubric-polytics / 2170805-volodimirgorbulin-direktor-nacionalnogo-institutu-strategicnih-doslidzen. html

7. *Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2015 році».* Київ: НІСД, 2015, 684 с.

8. Військова відповідь на кібератаки Кремля? І так, і ні. *Укрінформ.* URL: https: // www. ukrinform. ua / rubric-technology / 2251563-vijskova-vidpovid-nakiberataki-kremla-i-tak-i-ni. html

PECULIARITIES OF PROVIDING THE INFORMATION SPACE OF ITALY IN THE CONTEXT OF THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The article is a study of features of securing the information space of Italy in the context of the development of information and communication technologies. The paper presents a new solution to the current scientific problem, which consists in the development of conceptual and legal bases for ensuring information security, as well as practical recommendations for improving the mechanisms for its provision.

The results obtained in the course of the study give reason to claim that the realization of national interests in the information sphere will be effective in the case of legislative definition of national values and the prevailing national interests. Based on the developed model of interaction of national values, interests of goals and gains in the information sphere, it is suggested that the main criteria for assessing the negative impact on the information security of the state should be considered as destructive transformations of national values in the information sphere, which can be established through sociological surveys and surveys. Such criteria should be accumulated in the methodological base and on its basis to monitor the state and dynamics of the domestic information sphere, to identify the most vulnerable areas.

It is proposed and justified to include national interests, values, goals and values in the information sphere in the objects of information security; criteria for assessing the negative impact of threats on the state of information security have been developed, which are proposed to consider destructive transformations of national values in the information sphere, which makes it possible to create a legal basis for an appropriate methodological base; a new component – providing information security – was identified in the domestic system of information law, and the reasons and prerequisites for its occurrence were analyzed; elements such as spiritual, military, social, economic, environmental and global security have been identified in the system of information and psychological component of information security, which substantially characterizes the interconnections between them, which made it possible to take into account modern threats and to develop priority directions of the state policy of providing information security.

Key words: information security, state, Italy, Ukraine, media space, the information war, manipulation, consciousness.

REFERENCES

1. Negri, G. Facebook to monitor Italian election as EU debates Russian fake news. *The European Security Journal.* https: // www. esjnews. com / facebook-italy-russia-fake-news (accessed 12 January 2020) (in English).

2. *Separatism in Italian.* http: // www. germaniaplus. de/2009/09/separatizm-po-italyanski/ (accessed 12 January 2020) (in Russian).

3. Makarenko, Ye. A., Ozhevan, M. A., Ryzhkov, M. M. (2008). *Yevropeys'ki komunikatsiyi:* monohrafiya. [European communications: a monograph]. Kyiv: Free Press Center, pp. 212–215 (in Ukrainian).

4. *Europe's Way to the Information Society. An Action Plan.* http://i.lekciya. com.ua/doc/3177/index.html?page=17 (accessed 12 January 2020) (in Ukrainian).

5. *eEurope – An information society for all.* https://ec.europa.eu/digital-single-market/en/ news/eeurope-information-societyall (accessed 12 January 2020) (in English).

6. Gorbulin, V. *Ukraine has become a key state of confrontation between the West and Russia.* https://www.ukrinform.ua/rubric-polytics/2170805-volodimirgorbulin-direktor-nacionalno-go- institutu-strategicnih-doslidzen.html (accessed 12 January 2020) (in Ukrainian).

7. *Analitychna dopovid' do Shchorichnoho Poslannya Prezydenta Ukrayiny do Verkhovnoyi Rady Ukrayiny «Pro vnutrishnye ta zovnishnye stanovyshche Ukrayiny v 2015 rotsi»* [Analytical Report to the Annual Message of the President of Ukraine to the Verkhovna Rada of Ukraine «On the Internal and External Situation of Ukraine in 2015»]. (2015). K.yiv: NISD, pp. 512–533 (in Ukrainian).

8. *The military response to the Kremlin's cyberattacks? Yes and no.* https://www. ukrinform.ua/rubric-technology/2251563-vijskova-vidpovid-nakiberataki-kremla-i-tak-i-ni.html (accessed 12 January 2020) (in Ukrainian).

Матеріал надійшов до редакції 22.01.2020 р.

UDK 316.472.4/.47:[616.89-008:004

Żaneta Zając,
absolwentka studiów I stopnia na kierunku Bezpieczeństwo Narodowe,
studentka II roku studiów II stopnia na kierunku Bezpieczeństwo Państwa
na Uniwersytecie Pedagogicznym im. Komisji Edukacji Narodowej w Krakowie
https://orcid.org/0000-0002-4080-7541
Aleksandra Zamojska,
absolwentka studiów I stopnia na kierunku Bezpieczeństwo Narodowe,
studentka II roku studiów II stopnia na kierunku Bezpieczeństwo Państwa
na Uniwersytecie Pedagogicznym im. Komisji Edukacji Narodowej w Krakowie
https://orcid.org/0000-0002-9733-5151
https://doi.org/10.29038/2524-2679-2020-01-122-131

WPŁYW MEDIÓW SPOŁECZNOŚCIOWYCH NA BEZPIECZEŃSTWO ZDROWOTNE NA PRZYKŁADZIE FACEBOOKA, INSTAGRAMA ORAZ YOUTUBE

Przedmiotem tego artykułu jest analiza wpływu mediów społecznościowych na bezpieczeństwo zdrowotne jednostki. Rozważono następujące platformy: Facebook, Instagram i YouTube, czyli trzy rodzaje mediów społecznościowych o największej liczbie odbiorców. Użytkownicy tych portali to przede wszystkim młodzi ludzie - we wczesnej dorosłości i młodości. Ten przedział wiekowy jest najbardziej podatny na nierefleksyjną akceptację prezentowanych treści i włączenie ich do własnego życia, dlatego wybrane zagrożenia i skutki wynikające z nieefektywnego wykorzystania powyższe platformy zostały